International Journal of Latest Trends in Computing
E-ISSN: 2045-5364

Volume 2, Issue 2, June 2011

IJLTC Board Members

TABLE OF CONTENTS

X2ORtrans: A Schema Driven Mapping for IS-A Relationship

Kodituwakku S. R[1] and Kanagasabapathy P.[2]

[1]Department of Statistics & Computer Science, University of Peradeniya

[2]Postgraduate Institute of Science, University of Peradeniya

(salukak@pdn.ac.lk, prithak@yahoo.com)

Abstract: With the introduction of XML vast amount of XML data is manipulated in Web applications. As a result there is a growing interest in storing XML data in relational databases. There are many proposed heuristic techniques to store complex XML documents in relational databases. These techniques typically define fixed mappings and do not take application characteristics into account. Some other approaches have also been proposed to store XML data in relational databases. These approaches do not take the structural semantics into consideration. Due to this lack of consideration they fail to map XML schema into a better relational or object-relational database schema.

This paper proposes a flexible algorithm to map the IS-A relationship in XML schema to object-relational database schema. This method is based on the rich properties of XML schema and object-relational database schema. The salient feature of the proposed method is that it maps the IS-A relationship by preserving the semantics of the data. Additionally it facilitates the efficient storage of valid XML data into relations of the object-relational database schema. The proposed methodology is validated by comparing it against two widely used mapping techniques: XMLSchemaStore and LegoDB.

Keywords: eXtensible Markup Language (XML); object-relational databases; XML schema; IS-A relationship, inheritance, Structured Query Language (SQL).

1. Introduction

The emergence of the Internet as a mainstream technology facilitates access to a vast repository of information invaluable to establishment of the world-wide-web. Organizations collect enormous amounts of data on many topics of interest from this repository. This collected data or information is critical to the smooth, daily functions of any modern organization.

XML [1] is fast becoming a key format for representing and exchanging information. Perhaps, this is due to the fact that XML is not only a language for describing the data itself, but is especially helpful in describing its structure. This feature simplifies processing XML data considerably. The growing usage of XML technologies essentially demands effective storage and management of XML documents as well as for exchanging data. A number of approaches have been proposed and used. The most general and usual classification of XML data is based on their content, structure, and usage. Accordingly XML data is classified into two groups: native XML databases and XML-enabled databases.

Native XML database [2] is a special kind of database, specifically designed to store, query and manipulate XML documents in its native hierarchical form. This Native XML database is generic as it accepts any well-formed XML data, irrespective of the actual structure of data, and does not rely on schema existence. Developing new techniques for storage and retrieval of XML data is required for this purpose. While several researchers have focused on developing native XML databases [3], [4] still there is a room for further researching. XML not only models structured document, but also has the capabilities to model semi-structured and unstructured schema [5], [6]. It is observed that both structured and unstructured approaches are useful in storing and accessing XML data.

With the introduction of the Internet it is possible to store XML data in object-relational databases. This idea results from the way of describing the structure of XML documents, which resembles object-relational features in many ways and from other database features XML technologies include. Object-relational database (ORDB) allows a more expressive type system that coincides with the purpose of XML. Hence, the object-relational database management system is perfect to manage XML data in native form and to store XML data in database management systems. Nowadays, many object-relational database management systems allow users to define data types to handle XML data [7].

Database technology has developed increasingly over the past three decades and is presently the ideal choice to store and access data. The XML-enabled databases try to influence existing

database technology to store and retrieve XML data and are built on top of relational or object-relational systems. The use of present database management systems requires a mapping from the data model of XML [8] to the database system and from XML query languages [9], [10] to database query languages.

This paper proposes a method to map XML data to object-relational database. It mainly focuses on mapping the 'IS-A' relationship exist in XML schema10 into object-relational database schema. The method is presented in form of an algorithm. The proposed mapping algorithm is a schema driven mapping approach.

3 2. Related Work

Various techniques have been proposed for the XML processing based on relational and object-relational databases [11] – [26]. This section presents two such methods [12], [13] closely related to the technique proposed in this paper. These two techniques are summarized as they are compared against the proposed technique. The key aim of the XMLSchemaStore [12] is to exploit object-oriented features in XML document, analyzing XML schema in it and storing XML data. A document object model tree has been used to analyze the XML schema. The suggested mapping rules provide a clear picture for most of the elements of XML schema but the semantic of the data is not considered. The LegoDB system [13] aims at providing XML developers with an efficient storage solution tuned for a given application. The study presented in LegoDB system is a cost-based XML-to-relational mapping engine. It explores a space of possible mappings and selects the best mapping for a given application defined by an XML schema, XML data statistics, and an XML query workload. LegoDB influences existing XML and relational technologies. It represents the target application using XML standards and constructs the space of configurations using XML-specific operations. It also uses a traditional relational optimizer to obtain accurate cost estimates of the derived configurations. Both of these methods do not take the semantics of the data and the efficiency of data management into consideration. Due to this lack of consideration on structural semantics they fail to produce a better object-relational database schema that facilitates an efficient database access.

3. Materials

In modeling a database, it is often useful to identify a collection of similar entities. Such collection is called an entity set [27]. Sometimes it is natural to classify those in an entity set into 'IS-A' hierarchies. This relationship is often referred to as parent-child inheritance relationship [28]. 'IS-A' relationship models the notion of child class and parent class type of relationship. This kind of relationship can be identified in XML schema as well. Therefore, 'IS-A' relationship in XML schema can successfully be mapped into object-relational schema. An instance of a 'IS-A' relationship in shown in Figure 1.

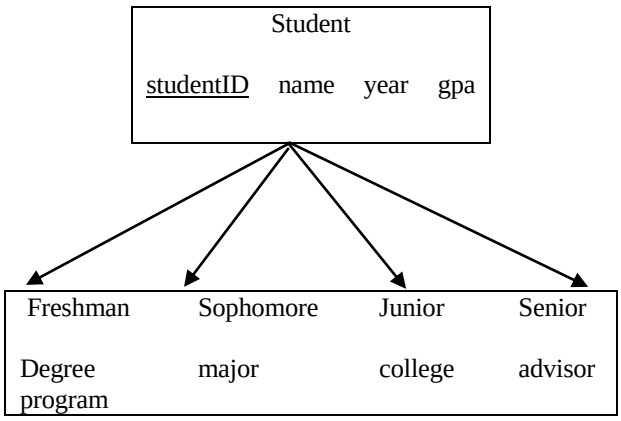


Figure 1 - Instances of a 'IS-A' relationship

3.1 'IS-A' Relationship Cases

A sub-class S is a class whose entities must always be a subset of the entities in another class, called the super-class C of the 'IS-A' relationship. Such a relationship is denoted by C/S and satisfies the $S \subseteq C$ property.

A specialization Z = {S1, S2, . . . , Sn} is a set of subclasses that have the same super-class G; that is, G/Si is a class-subclass relationship for i = 1, 2, . . . , n. G is called a generalized entity type.

Z is said to be total if we always have: $\bigcup_{i=1}^{n} S_i = G$
Otherwise, Z is said to be partial.

Z is said to be disjoint if we always have: $Si \cap Sj = \varnothing$ (empty set) for $i \neq j$
Otherwise, Z is said to be overlapping.
The disjointness and completeness constraints are independent. Accordingly four possible constraints on 'IS-A' relationship [28] can be identified: {Disjoint, total}, {Disjoint, partial}, {Overlapping, total} and {Overlapping, partial}.

3.2 'IS-A' Relationship Hierarchies and Lattices

A subtype itself may have further subclasses specified on it, structuring a hierarchy or a lattice and is also known as a single inheritance or a multiple inheritance respectively. A single inheritance has the constraint that every child class participates as a subclass in only one 'IS-A' relationship; that is, each child class has only one parent and basically results in a tree structure. In contrast, for a multiple inheritance, a child class can be a subtype in more than one inheritance relationship resulting in a lattice.

3.3 'IS-A' Relationship in XML Schema

The focus of our work is on how to represent 'IS-A' relationship constraints in XML schema. The 'IS-A' relationship is a relationship that defines an entity/class in terms of another. The storage of parent-child entities in entity types specifies 'IS-A' relationship. The completeness (total or full/partial) constraints and disjointness (disjoint/overlap) constraints need to be emphasized in 'IS-A' relationship. This section highlights techniques used to specify each of the constraints in XML schema.

3.3.1 Completeness Constraint

A total participation specifies that every entity in the parent class must be a member of at least in one child class. In set terminology, it represents FACULTY ∪ STUDENT = PERSON. To represent this constraint in XML schema, the schema element can be enumerated – choice content model in the element construct of the parent class. It allows only the entities of child class to reside in it, executing a total participation. In partial participation, it allows an entity not to belong to any of the child classes. Instead FACULTY ∪ STUDENT ≠ PERSON is presented. So, by imposing in the element construct, using schema element – choice content model, objects of both parent class and child classes can be modeled.

3.3.2 Disjointness Constraint

The disjointness constraint states that the child classes must be disjoint. In set terminology, it reads that FACULTY ∩ STUDENT = {}. In order to determine that child classes are disjoint, an existence of a key field unique across child types makes sure that the child classes are disjoint. This will impose the disjoint constraint. If the child classes are not to be disjoint, their sets of entity types may overlap. That is, the same entity may fall into multiple subtypes in the 'IS-A' hierarchy. In set terminology this allows the possibility that the intersection of FACULTY and STUDENT could not be non-empty, and can represent as FACULTY ∩ STUDENT ≠ {}. A unique identification is to be enumerated to define an overlapped entity. So, an overlapped instance is determined by comparing the values in key attributes from different child classes. Here the key is unique only to its particular child type. Hence, the non-existence of a key field is general to child classes.

***3.3.3** Hierarchies and Lattices in XML Schema*

In a single inheritance (hierarchy) every subtype associates as a child in only one 'IS-A' relationship having only one parent. On the other hand, when a child class directly inherits all properties from more than one parent class this leads to a lattice. Multiple inheritance hierarchies are more complex and are harder to design, implement, and understand than single inheritance hierarchies. Unfortunately, there is no way to structure multiple- inheritance in XML schema.

3.7 'IS-A' Relationship in ORDB Schema

The object-relational database [29]-][33] is composed of enriched SQL. Object-relational databases have evolved and incorporated various object features such as user-defined structured types, methods and inheritance. These concepts have been incorporated in the SQL: 1999 standard [34], which enables database designers to define new data types and complex object structures. By implementing the language enhancement introduced in SQL: 1999, ORDB inherits the SQL interface and, therefore, achieves access transparency. 'IS-A' hierarchy technique is captured in SQL: 1999 standard as Type Inheritance.

3.7.1 'IS-A' using Type Inheritance

Type Inheritance permits to create abstract data types, which inherits properties from another abstract data type (ADT) known as parent type. Type Inheritance describes the structure of parent class and child class entity types. The entity types are defined by creating object tables that stores instances of the ADT. If an object table is defined on a parent type and it can hold objects of the parent type and child type. SQL: 1999 does not support multiple-inheritance as it may cause ambiguity. The type inheritance improves the usefulness of objects by enabling creation of type hierarchies. Child classes not only inherit the features of the parent object type but also extend the parent type definition.

4. Methodology

This section proposes an algorithm for mapping the 'IS-A' relationship in XML schema into ORDB schema. This is done with a set of simple, consistent, easy-to-implement mapping rules.

XML to Object relational transformation (X2ORtrans) for 'IS-A' relationship

In order to store an XML schema in an object-relational database, the tree structure of the XML document must be mapped to a corresponding object-relational schema. The XML documents are then shredded and loaded into the mapped tables in the object-relational database system.

Design methodology named X2ORtrans (XML to ORDB transform) takes an XML schema as an input and maps all the class hierarchy constraints in the XML schema to generate the object-relational schema. The algorithm handles the all four cases of the IS-A relationship between the parent class and child classes. The methodology is given in the following algorithm.

4.1. Algorithm

```
Process: Mapping the 'IS-A' Relationship in the XML Schema to Object-Relational Schema
Input: An XML schema
Output: An object-relational database schema

CASE 1: partial participation and disjoint constraint
if (parent p be partial) then
if (child d be disjoint) then
   declare 'CREATE TYPE' object as Parent _T for parent class in create body type
   state type inheritance 'NOT FINAL' for Parent _T
   for every child class create 'CREATE TYPE' as Child_T
   state type inheritance 'UNDER' for Child_T
   mark the property to Parent _T and Child_T as 'INSTANTIABLE'
   CREATE an object TABLE as TabMain with reference to Parent_T and Child_T
else
CASE 2: partial participation and overlap constraint
if (child d be overlap) then
   declare 'CREATE TYPE' object as Parent_T for parent class in create body type
   state type inheritance 'NOT FINAL' for Parent _T
   for every child class create 'CREATE TYPE' as Child_T
   do not denote type inheritance 'UNDER' for Child_T
   store the unique 'ID' attribute to Parent_T and Child_T
   mark the property to Parent _T and Child_T as 'INSTANTIABLE'
   CREATE an object TABLE as MainTab which refers to Parent_T
   for every Child_T CREATE separate object TABLE as SubTab
end if
end if
CASE 3: total participation and disjoint constraint
if (parent p be total) then
if (child d be disjoint) then
   declare 'CREATE TYPE' object as Parent_T for parent class in create body type
   state type inheritance as 'NOT FINAL' for Parent_T
   for every child class create 'CREATE TYPE' as Child_T
   state type inheritance 'UNDER' for Child_T
   mark the property to Parent_T as 'NOT INSTANTIABLE'
   mark the property to Child_T as 'INSTANTIABLE'
   CREATE an object TABLE as MainTab which references to each and every Child_T or for each Child_T
   CREATE separate object TABLE as SubTab
else
CASE 4: total participant and overlap constraint
if (child d be overlap) then
   declare 'CREATE TYPE' object as Parent_T for parent class in create body type
   state type inheritance as 'NOT FINAL' for Parent_T
   for every child class create 'CREATE TYPE' as Child_T
   do not denote type inheritance 'UNDER' for Child_T
   store the unique 'ID' attribute to Parent_T and Child_T
   mark the property to Parent_T and Child_T as 'INSTANTIABLE'
   CREATE an object TABLE as MainTab which refers to Parent_T
   for each Child_T CREATE separate object TABLE as SubTab
end if
end if
```

4.2. Description of the Algorithm

CASE 1: partial participation and disjoint constraint

A partial participation permits the instances of parent class and child class to be existent, and parent type Parent_T and child types Child_T

encompass 'instantiable' constraint. It is adequate to create only one object table MainTab to store the instances of Parent_T and Child_T. It is also possible to create individual instance tables for each child type. However, repeated storage of the parent table and child table may lead to data redundancy and wastage of storage.

CASE 2: partial participation and overlap constraint
Parent type Parent_T and child type Child_T classes are created respectively. Due to the restriction in object type, an instance cannot belong to separate types unless existence of an 'IS-A' hierarchy. Therefore, type inheritance 'under' cannot be specified. This requires an overlapped entity to have two separate objects for each child class. If the type inheritance is stated, parent class attributes get stored redundantly. Such a situation opens up room for inconsistency. To avoid this, when there is an overlapping constraint it is advisable to avoid specifying inheritance using 'under'. The unique 'id' is specified to join the parent-child tables to get the values of child class instances and each child table to identity the overlapped instances. Since a partial participant 'instantiable' is stated to Parent_T and Child_T separate object tables as MainTab and SubTab for parent and each child class are created.

CASE 3: total participation and disjoint constraint
As mentioned in pervious cases, types Parent_T and Child_T are created for structure of parent-child relationship using type inheritance. Since it is a total participation, the instances of the parent class is not allowed to exist. As a result, Parent_T is stated with 'not instantiable' constraint. Two alternate can be considered in creating the object tables. One way, is to create a single object table MainTab holding all objects of child classes. The other is an object table to be created for each child class holding instances of each child type. The choice of the alternate may depends on the amount of data sets for a better query execution performance.

CASE 4: total participation and overlap constraint
As mentioned in case 2, type inheritance is not stated and separate object tables MainTab and SubTab for parent and each child class are created respectively.

5. Results and Discussion

This section evaluates the X2ORtrans mapping algorithm by describing its completeness and soundness. Then a demonstrative example is presented. Finally it is compared against two well-known mapping algorithms: XMLSchemaStore and LegoDB.

5.1 Completeness and Soundness

Completeness of X2ORtrans: The algorithm is complete with respect to the given subset of the W3C XML schema specification1. By analyzing the schema given in the W3C XML schema, it can be seen that schema is built from the basic elements of XML in capturing class hierarchy. The X2ORtrans is well-defined on all the base elements. These basic elements are mapped into ORDB schema.

Soundness of X2ORtrans: Any given XML document is valid with respect to a particular schema because X2ORtrans maps schema elements, attributes or inheritance relationship to a class, child class or as inheritance between two instances of the ORDB schema. In other words the XML schema can be represented as instances of the object-relational database schema so that the structural semantics are preserved as much as possible.

5.2 Motivating Example

The motivation, here, was to capture the 'IS-A' relationship from XML schema and to model it as a class hierarchy. The motivation is highlighted with an illustrative example depicted in Figure 2.

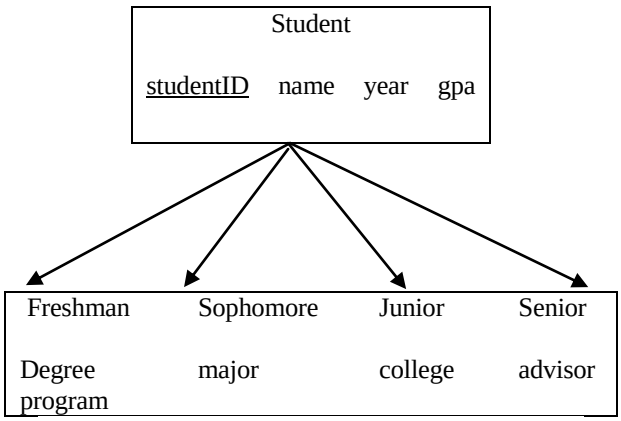


Figure 2 - Example of 'IS-A' relationship

Assume that the 'IS-A' relationship depicted in Figure 3 has been captured from a XML schema and needs to be mapped to an object-relational database schema. For comparison and illustration purposes it is assumed that total and disjoint constraints are maintained in the above example.

The proposed method is compared against XMLSchemaStore and LegoDB methods with respect to efficient access and efficient storage. Consider the following transactions, which are used to demonstrate the above aspects.

T1: create the tables for the parent entity and all the child classes
T2: find the student id, student name, year, gpa of all common values in child entities of freshman, sophomore, junior and senior
T3: select the student id for all students who are either seniors or juniors but not freshman or sophomore
XML query language – Xquery8 or XPath7 provides the transactions. It needs to be translated to a query on the underlying database. In his study, semantics which have been revealed throughout the transformation process for the efficient access of data.

T1: create the tables for the parent entity and all the child classes in Figure 2.
LegoDB results:
FRESHMAN (studentID, name, year, gpa, degree_program)
SOPHOMORE (studentID, name, year, gpa, major)
JUNIOR (studentID, name, year, gpa, college)
SENIOR (studentID, name, year, gpa, advisor)

XMLSchemaStore results:
First the user-defined types will be created:
STUDENT_type (studentID, name, year, gpa)
FRESHMAN_type UNDER STUDENT_type (degree_program)
SOPHOMORE_type UNDER STUDENT_type (major)
JUNIOR_type UNDER STUDENT_type (college)
SENIOR_type UNDER STUDENT_type (advisor)

Now the tables will be created and for simplicity the primary key is underlined:
FRESHMAN of FRESHMAN_type (studentID)
SOPHOMORE of SOPHOMORE_ type (studentID)
JUNIOR of JUNIOR_type (studentID)
SENIOR of SENIOR_type (studentID)

X2ORtrans results:
First the user-defined types will be created:
STUDENT_type (studentID, name, year, gpa) NOT FINAL NOT INSTANTIABLE
FRESHMAN_type UNDER STUDENT_type (degree_program)
SOPHOMORE_ type UNDER STUDENT_type (major)
JUNIOR_ type UNDER STUDENT_type (college)
SENIOR_ type UNDER STUDENT_type (advisor)
Now that the tables will be created and for simplicity the primary key is underlined:
Solution 1: creating a single table for the parent class
STUDENT OF STUDENT_type (studentID) or can
Solution 2: creating separate tables for each child classes
FRESHMAN of FRESHMAN_type (studentID)
SOPHOMORE of SOPHOMORE_ type (studentID)
JUNIOR of JUNIOR_type (studentID)
SENIOR of SENIOR_type (studentID)

According to the above results the LegoDB approach creates a set of relations for each child class along with the properties of the parent class and its child classes. In XMLSchemaStore, the object types are created for all classes (parent class and child classes). Then the object tables are created for every child type. Similar to XMLSchemaStore approach X2ORtrans creates the object types first. In creating the object tables the X2ORtrans approach provides two optimal solutions. That is, either to create a single object table to the parent type, representing all entity types in the class hierarchy or an option is similar to XMLSchemaStore approach.

T2: find the student id, student name, year, gpa of all common values in child entities of freshman, sophomore, junior and senior

LegoDB and XMLSchemaStore results:

SELECT S.studentID, S.name, S.year, S.gpa FROM STUDENT AS S WHERE S.studentID IN (SELECT studentID FROM FRESHMAN WHERE studentID IN (SELECT studentID FROM SOPHOMORE WHERE studentID IN (SELECT studentID FROM JUNIOR WHERE studentID IN (SELECT studentID FROM SENIOR WHERE studentID))))

X2ORtrans results:
An empty result will be generated by looking at the semantic of the TOTAL participation constraints. Thereby, it is believed that no necessity arises in assessing the database schema.

In LegoDB and XMLSchemaStore, a complex query is generated to find the common entities in child classes. Whereas in X2ORtrans method, due to the DISJOINT semantics of child classes are being known, it is possible to retrieve the result without querying the database schema. It affords an advantage to this study method with a saving on time and an efficient performance to the users.

T3: select the student id for all students who are either seniors or juniors but not freshman or sophomore

LegoDB and XMLSchemaStore results:
SELECT studentID FROM JUNIOR WHERE studentID NOT IN (SELECT studentID FROM FRESHMAN UNION SELECT studentID FROM SOPHOMORE) UNION SELECT studentID FROM SENIOR WHERE studentID NOT IN (SELECT studentID FROM FRESHMAN UNION SELECT studentID FROM SOPHOMORE)

X2ORtrans results:
SELECT studentID FROM JUNIOR UNION ALL SELECT studentID FROM SENIOR

LegoDB and XMLSchemaStore generate a list of select statements for each of child class with the union construct. In X2ORtrans, two select statements are required for child class tables with union all construct. In assessing the query this study method is more competent than LegoDB and XMLSchemaStore and has been used as the constructor union all, avoiding duplicates unlike union. By exploiting the DISJOINT and TOTAL semantics in the class hierarchy, it is possible to use the construct union all. These useful semantics are missed in the other approaches, resulting in an expensive transaction.

The above mentioned features are summarized in Table 1.

Table 1 - Summary of comparison results

Comparison Approaches			
Attempted Features	**LegoDB**	**XMLSchemaStore**	**X2ORtrans**
Source Schema	XML Schema	XML Schema	XML Schema
Target Schema	Relational Schema	Object-Relational Schema	Object-Relational Schema
Mapping Methods	User-Defined	Schema Driven	Schema Driven
Class Hierarchy Mechanism	Considered	Considered	Considered
Semantics of Data	Not Supported	Not Considered	Supported
Data Management Efficiency	Not Considered	Not Considered	Limited Consideration

5. Conclusion

The primary goal in developing a possible schema mapping is to provide efficient data access and efficient data storage by preserving the schema semantics. The proposed method attempts to achieve this up to some extend. The proposed methodology characterizes the nature of class hierarchy by exploiting the completeness and disjointness constraints, and shows how they correspond to the structure in XML schema. In addition, an algorithm is proposed in managing the 'IS-A' relationship in XML schema into ORDB schema.

The proposed X2ORtrans algorithm is simple and understandable. Therefore, this is a useful transformation for both experts and novices. According to the comparison results the proposed method maps the IS-A relationship in the XML schema into the RDBMS schema by preserving the structural semantics.

References

[1]. D. C. Fallside and P. Walmsley (2004), "XML Schema Part 0: Primer Second Edition, W3C Recommendation", http://www.w3.org/TR/xmlschema-0/.
[2]. R. Bourret (2009), "Native XML Databases", http://www.rpbourret.com/xml/ProdsNative.htm/.
[3]. S. Kimbro (2001), "Introduction to Native XML Databases", http://www.xml.com/pub/a/2001/10/31/nativexmldb.html/
[4]. R. Murthy, and S. Banerjee (2003), "XML Schema in Oracle XML DB", In Proceedings of the International Conference on Very Large Data Base (VLDB), p:1009–1018.
[5]. S. J., Tufte, K., He, G., Zhang, C., DeWitt, D., and Naughton, J. (1999), "Relational Databases for Querying XML Documents: Limitations and Opportunities", In Proceedings of the International Conference on Very Large Data Base (VLDB, p: 8-19.
[6]. S. Pal, I. Cseri, O. Seeliger, G. Schaller, L. Giakoumakis and V. Zolotov (2004), "Indexing XML Data Stored in a Relational Databases", In Proceedings of the International Conference on Very Large Data Base (VLDB), p: 1134 – 1142.
[7]. Scott Boag et. al. (2007). XML Query Language (XQuery): 1.0, W3C Recommendation http://www.w3.org/TR/xquery/
[8]. Bert Bos (2005), The XML Data Model, W3C Recommendation http://www.w3.org/XML/Datamodel.html
[9]. Anders Berglund et. al (2007). XML Path Language (XPath): 2.0, W3C Recommendation, http://www.w3.org/TR/xpath20/
[10]. L. JongSeon, J. KyungSoo, K. KyungSoo and C. MunYoung (2007), "Design of Automatic Database Schema Generator based on XML Schema", In Proceedings of IEEE, p: 1039 - 1043.

[11]. E. Pardede, J. W. Rahayu and D. Taniar (2004), "On Using Collection for Aggregation and Association Relationships in XML Object-Relational Storage", In Proceedings of ACM SAC, p: 703 – 710.

[12]. Mlynkova and J. Pokomy (2004), "From XML Schema to Object-Relational Database – An XML Schema-Driven Mapping Algorithm", In Proceedings of IADIS, International Conference WWW/Internet, p: 115—122.

[13]. P. Bohannon, J. Freire, J. Haritsa, M. Ramanath, P. Roy and J. Simeon (2000), "LegoDB: Customizing Relational Storage for XML Documents", In Proceedings of the International Conference on Very Large Data Base (VLDB), p: 1091 – 1094.

[14]. M. F. Fernandez, W.C. Tan and D. Sucin (2000), "SilkRoute Trading between Relational and XML", In Proceedings of International Conference on World Wide Web, (33), p: 723 – 745.

[15]. S. Amer-Yahia, F. Du and J. Freire (2004), "A Comprehensive Solutions to the XML to Relational Mapping Problems", In Proceedings of ACM WIDM, p: 31-38.

[16]. D. Beech, A. Malhotra and M. Rys (1999), "Formal Data Model and Algebra for XML", W3C Group Note.

[17]. D. Florescu and D. Kossmann (1999), "Storing and Querying XML Data using an RDBMS", In Proceedings of IEEE Data Engineering Bulletin, 22(3):27-34.

[18]. D. Draper (2004), "InformIT: Mapping between XML and Relational Data", Addison Wesley.

[19]. S. Hongwei, Z. Jingtao, W. Jing and Z. Shusheng (2000), "An Algorithm Mapping XML-Schema to Relational Schema", National Specialty Laboratory of CAD/CAM.

[20]. G. D. Penna, A.. Di Marco, B. Intrigila, I. Melatti and A. Pierantonio (2003), "Xere: Towards a Natural Interoperability between XML and ER Diagrams", Technical Report TRCS/GO102, Department of Computer Science, University of L'Aquila.

[21]. Tatarinov, S. Viglas, K. S. Beyer, J. Shanmugasundaram, E. J. Shekita and C. Zhang (2002), "Storing and Querying Ordered XML using a Relational Database Systems", In Proceedings of ACM SIGMOD, p: 204 – 215.

[22]. Deutsch, M. Fernandez and D. Suciu (1999), "Storing Semistructured Data with STORED", In Proceedings of ACM SIGMOD, p: 432 – 441.

[23]. S. Amer-Yahia and D. Srivastava (2002), "Mapping Schema and Interface for XML Stores", In Proceedings of ACM WIDM, p: 23 – 30.

[24]. Moller and M. I. Schwartzbach (2006), "An Introduction to XML and Web Technologies", Addison-Wesley.

[25]. N. D. Widjaya, D. Taniar, J. W. Rahayu and E. Pardede (2002), "Association Relationship Transformation of XML Schema to Object-Relational Databases", In Proceedings of iiWAS, p: 135-142.

[26]. T. Shimura, M. Yoshikawa and S. Uemura (1999), "Storage and Retrieval of XML Documents Using Object-Relational Databases", In Proceedings of DEXA (99), p: 206 – 217.

[27]. R. Ramakrishnan and J. Gehrke (2003), "Database Management Systems", 3rd edition, McGraw-Hill.

[28]. R. Elmasri and S. B. Navathe (2007), "Fundamentals of Database Systems", 5th edition, Addison-Wesley.

[29]. T. S. Dillon and P. L. Tan (1993), "Object-Oriented Conceptual Model", Prentice Hall.

[30]. G. Booch (1994), "Object-Oriented Analysis and Design with Applications", 2nd edition, Benjamin / Cummings.

[31]. J. Rumbaugh, W. Blaha, W. Premerlani, F. Eddy and W. Lorensen (1991), "Object-Oriented Modeling and Design", 2nd edition, Prentice-Hall.

[32]. W. Kim (1995), "Modern Database Systems", ACM Press and Addison Wesley.

[33]. W. S. Han, K. H. Lee and B. S. Lee (2003), "An XML Storage System for Object Oriented / Object-Relational DBMSs", Journal of Object Technology, 2(1), p: 113 – 126.

[34]. Eisenberg and J. Melton (1999), "SQL: 1999, formerly known as SQL3", In Proceedings of ACM SIGMOD Record 28(1), p: 895.

Fuzzy Linguistic for Measuring Customer Satisfaction

Lazim Abdullah[1], and Solihah Khadiah[2]

[1&2]University Malaysia Terengganu, Department of Mathematics,
lazim_m@umt.edu.my

***Abstract*:** Customers' satisfaction is one of the very important keys in ever challenging market. There are many approaches that have been used to evaluate customers satisfaction. This paper proposes an evaluation of customer satisfaction from the perceived service quality using fuzzy linguistic. A twenty three-item questionnaire was distributed to thirty four judges who being asked about the services provided by a hypermarket in Kuala Terengganu, Malaysia. Data collected were analyzed using a fuzzy linguistic evaluation model. The judges give their current state of perception about service quality in linguistic terms. Data in form of linguistic terms were quantified into fuzzy triangular numbers with their respective weight for each criterion. The level of customer satisfactions was determined by considering the minimum value of a difference between total integral value and integral value for each linguistic term. The judges agree that the level of satisfaction was at the 'middle' with degree of optimism at 0.5. The findings suggest that linguistic evaluation is practical and meaningful in measuring customer satisfaction.

***Keyword*:** Fuzzy logic; customer satisfaction; fuzzy numbers; linguistic evaluation

1. Introduction

In the new global market, customer service oriented industry has become a central issue for in-depth discussion. Customer service providers face stiff competition for survival, since customers have become increasingly sensitive to service quality. Customers know what they deserved to get when they are receiving service from any service oriented industry. Customers are free to make choices and an opportunity to choose which companies to deal with. Hence, service provided by companies must embark new measures to find ways to enhance quality of service and eventually satisfying their customers. Customer satisfaction becomes the focal point in attracting new customers and retains the existing one. According to many authors, customer satisfaction means the emotional reaction of consumers to the gap between the expected service and the actually perceived service [1]-[4]. About a similar definition, customer satisfaction proposes satisfaction based on a customer's estimated experience of the extent to which a provider's services fulfil his or her expectations [5].Through customer satisfaction, companies retain their customers and gain new market shares [6],[7].

Even though new customers are welcomed almost in every line of business, the main objective of companies is to maintain customers for a long-time period. The total value of a lifetime customer is almost unquantifiable, and allows firms to achieve a competitive advantage against competitors [8]. The emotion of satisfaction among customers derived from service quality offered by companies. This action is affected by elements such as time, location, and situation. For example, 'the service provided is better than what I expected', 'the gap between the expected and perceived service is not big', 'generally speaking, I am satisfied with the service'. These entire examples show satisfaction levels that commonly stated. In this sense, many methods has been formulate to measure satisfaction. It has been a normal practice to collect data through surveys with questionnaires prior to data analysing. The ordinal level scale used most frequently applied in questionnaires is the Likert scale, with rankings of the form: 1 strongly agree; 2 agree; 3 unsure, 4 disagree, and 5 strongly disagree. Clearly, someone who circles 5 disagrees with the statement more than someone who circles 4 does. However, the degree of difference is unclear, since an ordinal scale indicates relative position, not the magnitude of the difference between the choices. Therefore, the available arithmetic operations include median and mode, but not the mean. Thus, results of survey based on the ordinal scale cannot usually be statistically analyzed by traditional statistical methods [9]-[11].

Moreover, measuring satisfaction level and service quality is not merely statistical matters because of the concept of these words are inherently intangible in nature and difficult to defined [12]. Consumers' judgment toward a service depends basically on the strength of their beliefs or expectations about various features associated with the service and the weight of attribute [13]. Consumers' beliefs or expectations typically involved perceptions over the service and its attributes stemming from their experience with the service. Thus, perceptions depend greatly on the linguistic judgment and decisions usually employ subjective knowledge and linguistic information. The linguistic values are difficult to measure throughout a classical mathematical function. One of the mathematical theories that developed to deal with linguistics judgment is fuzzy set theory. Fuzzy set theory was initially used to manage the vagueness of human thought, since it can represent vague expressions such as 'usually', 'fair' and 'satisfied', which are regarded as the natural representation of customers' preference and judgment [14]. Fuzzy sets theory offers an alternative mean to accommodate with the unclear boundaries and subjective nature. Indeed, it was very fortunate that the fuzzy sets theory provides a

framework that cope with uncertainty in language, that is, subjective uncertainty [15].

Linguistic judgement has been widely used in many real life applications in various decision making domains with different mathematical formulations. For instance, [16] present a fuzzy linguistic scale, which is characterized by trapezoidal fuzzy numbers, for the comparison between two alternatives. Possibility degree formula was employed for comparing trapezoidal fuzzy numbers. Reference [17] present a multi person decision-making method using fuzzy logic with a linguistic quantifier when each group member specifies incomplete judgment possibly both in terms of the evaluation of the performance of different alternatives with respect to multiple criteria and on the criteria themselves. Reference [18] use fuzzy linguistic approach to assess the maintenance strategies and practices in a company. Thus, the present study attempts to express all the perceived statements into a linguistic value such as 'very low', 'low', 'middle', 'high' and 'very high'. Rather than employ statistical methods to analyse customer satisfaction, this research uses the fuzzy set theory that has been applied in the field of management science [19]-[23]. Since customer satisfaction is subjective in nature, this study applies a fuzzy approach in analyzing the perceived service quality. Specifically the objective of this research is to determine level of customer satisfaction from the perceived service quality in a hypermarket using fuzzy linguistic evaluation.

2. Linguistic Judgement and Integral Fuzzy Number

One of the most powerful uses of fuzzy set theory is to represent the linguistic variables. Linguistic variables are descriptions employed by people. A linguistic variable also can be defined as a variable, whose values are not numbers, but are words or sentences in natural or artificial language. The relative importance weights in the decision making process can be evaluated by linguistics terms such as 'very low', 'low', 'middle', 'high' and 'very high' and so on. These linguistics terms can be quantified and expressed as Triangular Fuzzy Numbers (TFNs) using fuzzy set theory [24]. TFN is a special type of fuzzy number with three parameters, each representing the linguistic variable associated with a degree of membership of 0 or 1. Since it is shown to be very convenient and easily implemented in arithmetic operations, the TFN is also used very common in practice [28]. The membership function of a fuzzy number $\tilde{A}$ is defined as follows:

$$f_{\tilde{A}}(x)=\begin{cases}\dfrac{x-a}{b-a}, a\le x\le b, a\ne b\\ \dfrac{x-c}{b-c}, b\le x\le c, b\ne c\\ 0, otherelse\end{cases} \quad (1)$$

Then $\tilde{A}$ is called a TFN and denoted as $\tilde{A}$ = (a, b, c).

Since TFNs are flexible in nature, thus it opens to making comparison. A comparison between TFNs is indeed very important in decision making. Integral values for TFNs are proposed to compare and subsequently rank more than two fuzzy numbers simultaneously [26].

The definition of integral values for the TFN $\tilde{A}$ is shown in equation (2) as follows:

$$I(\tilde{A})=(1-\alpha)\int_0^1 g_{\tilde{A}}^{L}(\tilde{u})du+\alpha\int_0^1 g_{\tilde{A}}^{R}(\tilde{u})du,$$

where $0\le\alpha\le 1$,

and $\alpha=\dfrac{1-\alpha}{2}a+\dfrac{1}{2}b+\dfrac{\alpha}{2}c$ (2)

The index of optimism (α is representing the degree of optimism for a person). A larger α indicates a higher degree of optimism. The index of optimism is used to reflect the decision maker's optimistic attitude. For a person of neutral or moderate objective personality, his or her value of α equals 0.5. When α = 0.5, the total integral value of the TFN $\tilde{A}$ becomes:

$$I(\tilde{A})=(1-\frac{1}{2})\int_0^1 g_{\tilde{A}}^{L}(\tilde{u})du+\frac{1}{2}\int_0^1 g_{\tilde{A}}^{R}(\tilde{u})du=\frac{a+2b+c}{4} \quad (3)$$

The three equations are directly employed in the customer satisfaction experiment.

3. Experiment

Data were collected using a Likert Scale questionnaire constructed by the researchers. The questionnaire was designed based on related studies and tailored to the purpose of the research. Thirty four judges were selected from different genders, ages and occupations. The questionnaire comprised two parts in which the first part contains the basic information of the judges with three simple statements. The second part was designed based on the focus of this study that comprises 10 criteria of quality service measurement. The perceived criteria used in this experiment are presented in Table 1. The criteria for evaluation of service quality are denoted as $C_i, i=1,2,\ldots,n$ where n is the number of service attributes contained in the questionnaire.

Table 1. Measurement Criterions Used For Customer Service Evaluation

i	Criteria, c_i
1	Good's quality
2	Good's price
3	Display clarity prices of goods
4	Good's arrangement
5	External conditions
6	Entrance and exit
7	Waiting time
8	Cleanliness
9	Staff's ability and capability
10	Facility for parking space

Total of twenty three statements that reflect the criteria need to be responded by judges. Judges need to select at the space provided for a given value from 'very low' (1) to 'very high' (5) to represent the service quality provided by a Hypermarket at Kuala Terengganu, Malaysia. Scales of 5 and its linguistic values are presented in Table 2.

Table 2 Linguistic Variable and Scale

Number	Linguistic Variable
1	Very Low (VL)
2	Low (L)
3	Middle (M)
4	High (H)
5	Very High (VH)

The TFN used by [27] is used to the evaluation of hypermarket in this experiment. In the first step of experiment, customers use the linguistic terms to record their perception over ten criteria of service quality, and transformed into pre-defined fuzzy numbers. Then, the weight for the service quality evaluation criteria is determined from the questionnaire. The fuzzy perceived quality score is calculated by combining the fuzzy numbers of criteria and their corresponding weight. Finally, the fuzzy service quality score is converted to linguistic terms to reflect the customer satisfaction level of overall service quality. In short, the computational procedures are written in four steps and given as follows.

3.1 Computational Procedures

In order to make the computational procedures self-explained and systematic, the following steps are proposed.

Step 1: Define TFNs of linguistic variables.

Measurement criteria of service quality and corresponding linguistic values are defined in Table 3

Table 3 Linguistic Variables And TFN

Linguistic Variables	Symbol	TFN
Very Low	VL	(0, 0, 3)
Low	L	(0, 3, 5)
Middle	M	(2, 5, 8)
High	H	(5, 7,10)
Very High	VH	(7,10,10)

Step 2: Define Weights of linguistic variables

Each linguistic variable comes with different weight. Let C_i denote the evaluation criteria of service quality, and let W_i denote the corresponding C_i, i=1, 2,..., n. The weights of C_I are defined as the peak, (a_p, 1) of central triangular fuzzy number (a_1, a_p a_2) for each linguistic value. These are shown in Table 4.

Table 4. Weight of Importance for Each Criterion

Linguistic variable	Weight, W_i
Very Low	(3, 3, 8)
Low	(3, 8, 13)
Middle	(8, 13, 18)
High	(13, 18, 23)
Very High	(18, 23, 23)

Step 3: Combine weighs and TFNs.

Combine the criteria that measured in TFNs with corresponding weights to obtain the overall service quality.

Let the set of linguistic terms be $A_c = \{VL, L, M, H, VH\}$. In accessing the service quality, c_i is the evaluation result of each quality criterion C_i, and $c_i \in A_c$. The corresponding TFN of c_i is denoted as $\tilde{c}_i$. To simplify the service quality calculation, the linguistic terms in accessing the service quality perceived are represented by the TFNs $\tilde{A}$.

Based on the criteria measured and the corresponding weights in Step 1 and Step 2 respectively, the overall service quality $\tilde{A}$ can be obtained using the following equation.

$$\tilde{A} = \left(\frac{1}{\sum_{i=1}^{n} W_i}\right) \otimes (W_1 \otimes \tilde{c}_1 \oplus W_2 \otimes \tilde{c}_2 \oplus \ldots \oplus W_n \otimes \tilde{c}_n) \quad (4)$$

Step 4: Convert $\tilde{A}$ into linguistic terms.

To help the customers understand better the meaning of the total service quality level, rather than simply a score or scale, the TFN of the service quality $\tilde{A}$ should be transformed into linguistic terms, which is the original form. Only a few methods have been proposed to convert the fuzzy numbers to the corresponding linguistic terms, including shortest distance method [29]. This study applies the same method as [27] where ranking fuzzy numbers are incorporated with integral value to convert fuzzy numbers to their corresponding linguistic term.

Let $\tilde{u}_1 = VL, \tilde{u}_2 = L, \tilde{u}_3 = M, \tilde{u}_4 = H, \tilde{u}_5 = VH$

Based on equation (3) with α =0.5, the integral value of $\tilde{u}_i, i = 1,2,...,5$, can be obtained and subsequently used as a preference comparison standard.

Find j, which can lead to $I(\tilde{u}_j) \le I(\tilde{A}) \le I(\tilde{u}_{j+1})$

Let $P = \min\left\{ I(\tilde{A}) - I(\tilde{u}_j), \left| I(\tilde{A}) - \frac{I(\tilde{u}_j) + I(\tilde{u}_{j+1})}{2} \right|, I(\tilde{u}_{j+1}) - I(\tilde{A}) \right\}$ (5)

The conversion steps need to comply one of the following rules.

If $P = I(\tilde{A}) - I(\tilde{u}_j)$, then the service quality level is given by $\tilde{u}_j$.

If $P = I(\tilde{u}_{j+1}) - I(\tilde{A})$, then, the service quality level is given by $\tilde{u}_{j+1}$.

If $P = I(\tilde{A}) - \frac{I(\tilde{u}_j) + I(\tilde{u}_{j+1})}{2}$, then, the service quality level is between $\tilde{u}_j$ and $\tilde{u}_{j+1}$.

Prior to decision, the integral value of $\tilde{u}_i, i = 1,2,...,5$ are calculated (Equation (3)) with $\alpha = 0.5$. The integral values for each linguistic term are presented in Table 5.

Table 5 Integral Values for $\tilde{u}_i$.

Linguistic term	*VL*	*L*	*M*	*H*	*VH*
Corresponding TFN	$\tilde{u}_1$	$\tilde{u}_2$	$\tilde{u}_3$	$\tilde{u}_4$	$\tilde{u}_5$
$I(\tilde{u}_i)$	0.75	2.75	5.0	7.25	9.25

The integral values use as a guidance in making linguistic decision. These computational procedures are employed in obtaining results of the experiment.

3.2 Computations and Results

Responses for each criterion from the questionnaire are analyzed by taking arithmetic mean from the scale. The round off to nearest whole number of the scale is done in ensuring smooth conversion from linguistic variable to the defined TFN. The weight of importance for each criterion is determined based on the defined TFN (see Step 2).

For the purpose of clarity, an example of computation from one judge is presented.

Summation of weight for all criteria is obtained as

$$\sum_{i=1}^{n} w_i = 130$$

The TFNs of criteria and corresponding weights are combined to calculate the service quality (Equation (4)).

Thus,

$$\tilde{A} = \left(\frac{470}{130}, \frac{843}{130}, \frac{1071}{130} \right)$$

To obtain the integral value for $\tilde{A}$, equation (3) is used. Now, the integral value for $\tilde{A}$ is obtained at 6.204808. Therefore the linguistic term to represent the customer satisfaction is between 'medium'(u_3) and 'high' (u_4).

With the similar fashion, calculations for all 34 judges are executed using a computer algebra system. The averaged integral value for all judges is 5.0354282. At this point, the level of customer satisfaction is between u_3 and u_4 which is between 'middle' and 'high' in linguistic terms. To determine one out of three situations in decision rules, calculations in Step 4 are executed. When j=3, the Equation (5) gives the minimum value of P as 0.0354282. Therefore, based on the rules, service quality level is u_3. Of the five ordered linguistic terms, the present judges evaluated customer satisfaction at the 'middle' with degree of optimism at 0.5.

4. Concluding Remarks

This paper has shown the significance of linguistic judgment in evaluating customer satisfaction based on the ten selected criteria of service quality. Judges expressed their perception of service quality in linguistic terms by choosing the number from the scale provided. The scale converted to linguistic terms where the weights were determined prior to combining with the fuzzy numbers according to the linguistic terms. Finally, the fuzzy service quality score was transformed into linguistic terms by ranking fuzzy numbers and locate position using integral value to reflect the overall service quality level. Then, the overall level of customer satisfaction was determined. The level of customer satisfaction in linguistic term is successfully reflected the perceptions of customers. Fuzzy numbers and linguistic terms effectively used as a method in to measure service quality. The identification of consumers' perceptions of service quality may help management to improve the service and in return would elevate their business standings.

References

[1] M. K. Brady, J. R. Christopher and J. J. Cronin, ' Managing behavioural intentions in diverse cultural environments- an investigation of service value and

satisfaction for American and Ecuadorian fast-food customers', Journal of International Management, Vol. 7, 2001, pp. 129–149.

[2] J. J. Cronin, J. Brady, K. Michael, G. Tomas, and M. Hult, 'Assessing the effects of quality, value and customer satisfaction on consumer behavioural intentions in service environments', Journal of Retailing, Vol.76, no. 2, 2000, pp. 193–218.

[3] R. Hallowell, 'The relationship of customer satisfaction, customer loyalty and profitability: an empirical study', *The* International Journal of Service Industry Management, Vol.7, no. 4, 1996, pp. 27–42.

[4] A Parasuraman, V.A., Zeithaml,. and L.L. Berry, 'SERVQUAL: a multiple-item scale for measuring consumer perceptions of service quality', Journal of Retailing, Vol. 64, no. 1, 1988, pp. 12–40.

[5] T. J. Gerpott, W. Rams, and A. Schindler, 'Customer retention, loyalty, and satisfaction in the German mobile cellular telecommunications market', Telecommunications Policy, Vol. 25, no. 4, 2001, pp. 249-269.

[6] V. A. Zeithaml, 'Consumer perception of price, quality and value: A means-end model and synthesis of evidence', Journal of Marketing, Vol. 52, no.3, 1988, pp. 2–22.

[7] M. Christopher, 'Logistics and Supply Chain Management', London : Pitman Publishing, 1998.

[8] G. Bailey, 'Customer care- Making it works', Managing Service Quality, Vol. 6, no. 3, 1996, pp. 36–38.

[9] N. K. Malhotra, 'Marketing Research: An Applied Orientation', 3rd ed., NJ: Prentice-Hall, Upper Saddle River, 1999.

[10] R. D. Mason, D.A. Lind, and W. G. Marchal, 'Statistical Techniques in Business and Economics', 10th ed., New York.: McGraw-Hill, 1999.

[11] V. Kumar, D. A. Aaker, and G.S. Day,. 'Essentials of Marketing Research', New York: Wiley, 1999.

[12] J. Kandampully, 'Firm should give loyalty before they can expect it from customers', Managing Service Quality, Vol. 7, No. 2, 1999, pp. 92-104.

[13] J. F. Engel, R. D. Blackwell and P.W. Miniard, 'Consumer behaviour' Forth Worth, TX: The Dryden Press. 1995.

[14] L.A. Zadeh, 'Fuzzy Sets', Information and Control. Vol. 8, no.5, 1965, pp. 338-353.

[15] M. Mukaidono, 'Fuzzy Logic for Beginners'. Singapore: World Scientific Publishing. 2001.

[16] Y.J Xu,. and Z.J Cai,. 'Method based on fuzzy linguistic judgment matrix and trapezoidal induced ordered weighted geometric operator for multi attributes decision making problem'. International Conference on Wireless Communications, Networking and Mobile Computing, 2007. pp. 5757 – 5760.

[17] D.H. Choi, B.K., Ahn, and S.H. Kim, 'Multicriteria Group Decision Making Under Incomplete Preference Judgments: Using Fuzzy Logic With A Linguistic Quantifier', International Journal of Intelligent Systems, Vol 22, no.6 ,2007, pp.641-660.

[18] C. Mechefske and Z. Wang, 'Using Fuzzy Linguistics To Select Optimum Maintenance And Condition Monitoring Strategies', Mechanical Systems and Signaling Processing, Vol 15, no 6, 2001 , pp. 1129-1140.

[19] M. O. Hutchinson, 'The use of fuzzy logic in business decision making', Derivatives Quarterly, Vol. 4, no. 4, 1998, pp. 53-67.

[20] M. Viswanathan, 'Understanding how poroduct attributes influence product categorisation; development and validation of fuzzy-set based measures of gradeness in product categories', Journal of Marketing Research, Vol. 36, no. 1, 1999, pp. 75-95.

[21] X. Xia, Z. Wang, , and Y. Goa, 'Estimation of non-statistical uncertainty using fuzzy-set theory', Measurement Science and Technology, Vol. 11, no. 4, 2000, pp. 430-435.

[22] H. T. Lee, and S. H. Cheng, 'Use C_{pk} index with fuzzy number to evaluate service quality', International Federation of Operational Research Societies. Vol. 9, 2002, pp. 719-730.

[23] J. C. Chein, and H. H. Tsai, 'Using Fuzzy Number to Evaluate Perceived Service Quality', Fuzzy Sets and Systems, Vol. 116, 2000, pp. 289-300.

[24] H. Y. Lin, P. Y. Hsu, and G. J. Sheen. 'A fuzzy based decision making procedure for data warehouse system selection', Expert Systems with applications, Vol. 32, no. 3, 2007, pp. 939-953.

[25] Liou, T.S. and Wang, M.J. (1992) 'Ranking fuzzy numbers with integral value', Fuzzy Sets and System, Vol.50, pp.247-255.

[26] T.S. Liou, and M.J. Wang, 'Subjective assessment of mental workload- a fuzzy linguistic multi-criteria approach', Fuzzy Sets and System, Vol.62. 1994, pp. 155-165.

[27] T.S. Liou, and C. W. Chen, 'Subjective appraisal of service quality using fuzzy linguistic evaluation', International Journal of Quality and Reliability Management, Vol. 23, no. 8, 2006, pp. 928-943.

[28] J. J. Cronin, and S. A. Taylor, 'Measuring service quality: a re-examination and extension', Journal of Marketing, Vol. 56, no. 7, 1992, pp. 55–68.

[29] K.J. Schmucker, 'Fuzzy Sets, Natural Language Computations, and Risk Analysis', New York: Computer Science Press, Inc. 1985.

Author Biographies

Lazim Abdullah holds Undergraduate B Sc (Hons) in Mathematics and at University of Malaya in Jun 1984. He obtained masters degree in Mathematics Education at University of Science Malaysia, Penang in 1999 and Ph.D degree at University of Malaysia Terengganu, in Information Technology Development, September 2004. He is currently an Associate Professor at Faculty of Science and Technology, University of Malaysia Terengganu, Ministry of Higher Education Malaysia. His researches are dealt with fuzzy sets theory and its application to social ecology, health sciences, environmental sciences and education. He is interested about measurement of social, health and education indicators by inserting computational intelligence of fuzzy knowledge. His interest also lies towards profiling social and educational constructs using statistical software. He is an editor of books, conferences proceedings and also a reviewer and editorial board of International Journals. He is a member of IEEE Computational Intelligent Society and Malaysian Mathematical Society.

Solihah Khadiah holds B.Sc (Hons)in Mathematics at University of Malaysia Terengganu. Currently she is a research student at the same university.

IT-supported Interaction Creates Discursive Spaces

Gilbert Ahamer[1]

[1] Austrian Academy of Science, Institute for GIScience,
gilbert.ahamer@oeaw.ac.at

***Abstract*:** How to establish an online space of discourse that lives on interaction organized into a dialogue? This text provides an analysis of the social dynamics of several modes of interaction between students of "Technology Assessment" in a University of Applied Science. The web-based negotiation game "Surfing Global Change" SGC (© with the author) delivers a set of rules for guided online discussion that opens into the generation of a consensus on complex interdisciplinary matters. This analysis shows that "quality" can be measured by many combinations of parameters but that finally any such metrics must be accepted by the affected stakeholders. This paper suggests public participation as a tool.

***Keywords*:** Surfing Global Change, role game, debate, discourse, mutual assessment, social dynamics, GIS.

1. Introduction

The target of this paper is to assess web-supported communication procedures during a competitive discussion. IT structures such as *web platforms* are able open up a meeting space for interdisciplinary understandings.

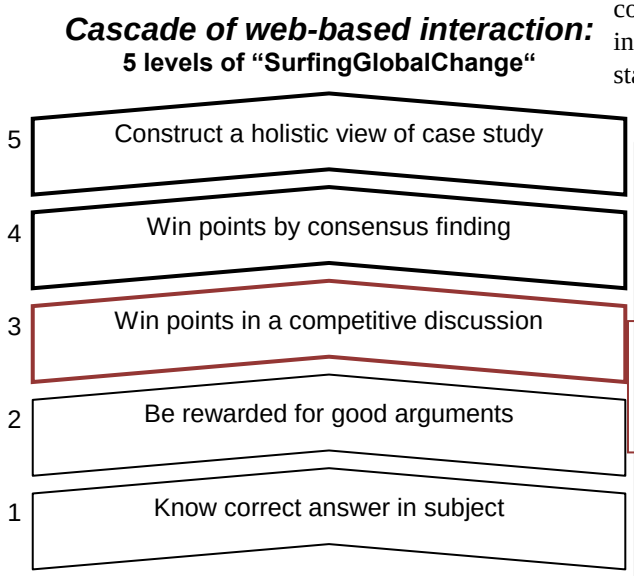


Figure 1: The five level structure of the web-based negotiation game "*Surfing Global Change*" copyrighted by the author and described in Ahamer (2004, 2006).

On a theoretical level, "*communicative spaces*" have been described by Ahamer & Strobl (2010), Castells (2010), Healey et al. (2008), Heiskala (1990). This concept builds on Pierre Bourdieu's notions of social spaces and social capital (Wikipedia, 2011): "For Bourdieu each individual occupies a position in a *multidimensional social space*" which is created by "social practice".

In this case, such *constitutive social practice* is *mediated through IT*, more specifically through interactive learning platforms, a key *emerging pedagogic technology* (Mukerji & Tripathi, 2010, Pavan & Diani, 2010).

On a practical level, communicative or discursive spaces are often built in more elaborate architectures of web-based learning (Ahamer, 2010), especially by the five-level web-supported negotiation game "*Surfing Global Change*" (SGC, Figure 1, the most important level 3 is in brown), the rules of which were published earlier (Ahamer 2004: 36ff, 2006: 387-389) and were elected finalist in the highest rewarded European prize on media didactics (MP, 2007).

This paper uses mainly the experiences of the competitive discussion in level 3 of SGC (brown box in Figure 2) and of other levels and interprets its statistical analysis.

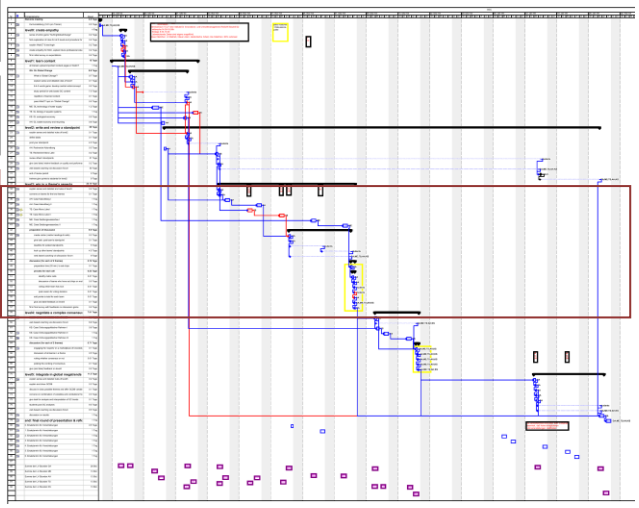


Figure 2: Typical time plan for an interdisciplinary implementation of "Surfing Global Change" (SGC) for students of "environmental systems studies" (USW, 2011) including five lecturers in "team teaching".

2. Facts and statistics for level 3

Given the key role of level 3 within the entire architecture of SGC, four independent professional reviews (Rauch, 2003, Gierlinger-Czerny, 2003) on the basis of these experts' earlier experiences (Rauch, 2000, Gierlinger-Czerny & Peuerböck, 2002) have been commanded by the author in order to diagnose the social dynamics of this original web-supported negotiation game.

Level 3 emulates an Environmental Impact Assessment negotiation and allocates roles to *four teams of students sitting in a discussion* while other students watch from behind and *assess the quality of their performance* (see Figure 4 and Figure 7). This procedure is prepared by various discursive actions on the web platform (Figure 3) preparing the sense and quality of the peer review procedures.

Students analyzed in this paper came from two disciplines: "construction management" and "industrial electronics", both from the University of Applied Science at Joanneum (FHJ, 2011) at Graz in Austria.

According to the SGC rules, students have first to *agree on* their "game board", i.e. on *a thematic matrix* (Table 1, see chapter 2.1) with which they are *performing the discussion* afterwards (chapter 2.2), the *statistical details* of which are analyzed (chapter 2.3) and compared with results from other SGC levels (chapter 2.4).

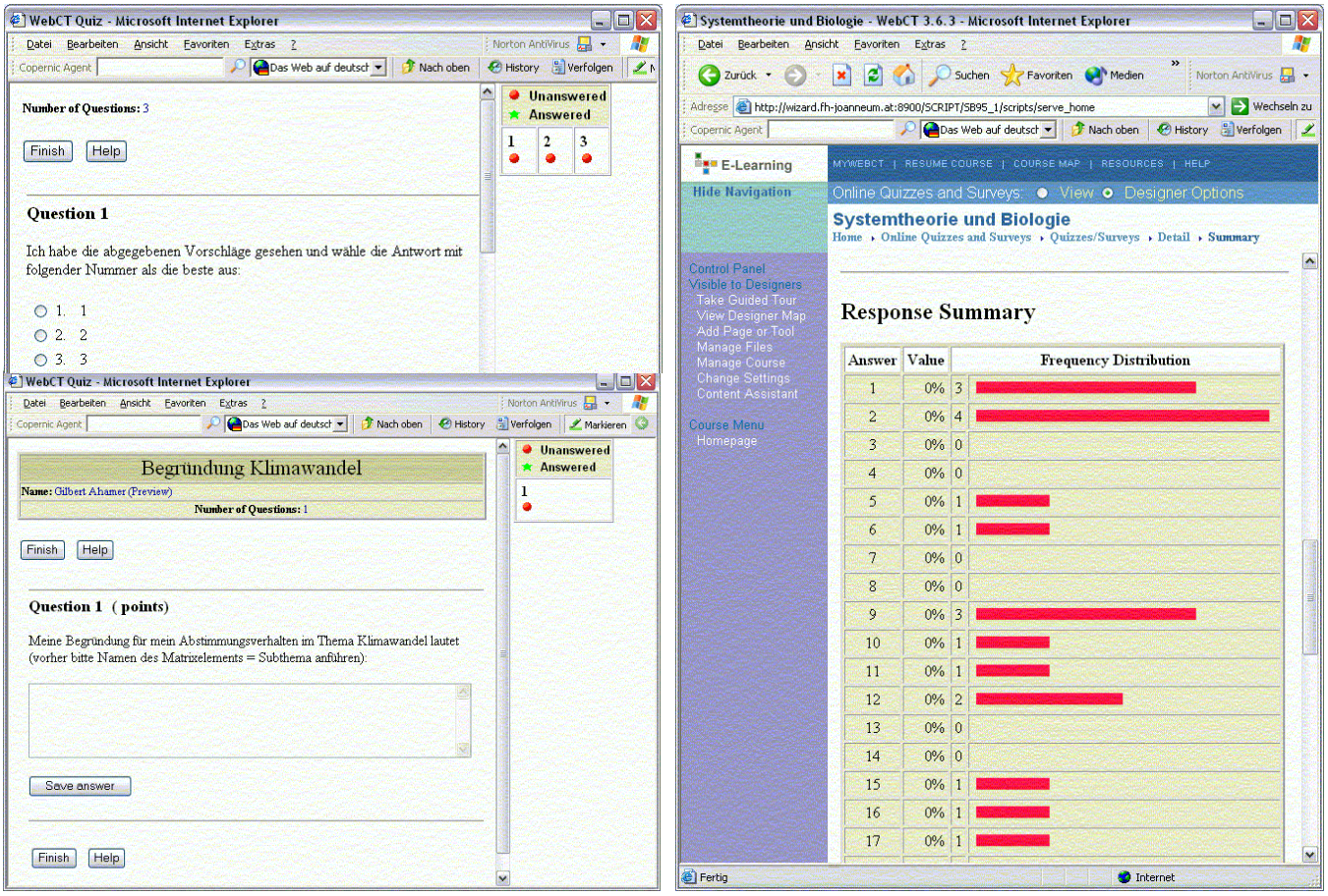


Figure 3: Web based voting procedure to select a matrix for each of the two themes to be used for level 3 with students in construction implemented as an anonymous WebCT survey. Upper left: multiple choice question, lower left: text box for giving the reason explaining the choice, right: result of the voting procedure, the documentation of the reasons given is then delivered to the students in an anonymized manner.

New university campus sum = 100 points (usually: 60 points)	Economic	Environmental	Infrastructure	Landscape	Social
City population & neighbors		10			
Students			5		5
Business people	5				
The university operators	15				5
The city council			10	5	

Table 1: An example for a matrix filled in by a team (text describing the meaning of the single matrix elements concretely is left out in this grid)

2.1 The process of agreeing on a thematic matrix

(a) Students of "construction engineering and construction management"

The names of the two themes were agreed on by the students after they had been given about one week to ponder on their classes' first proposals and to informally approximate to a common solution during their daily life with compulsory presence in the lectures. After final fixation of the *two themes* ("new FH university campus" that was just in a state of planning nearby and "erection of antennas for mobile phones" which was in continuous public interest in Austria due to the alleged effects on human health) randomly organized groups of six were asked during their lessons of advanced English to invent the titles for the rows and columns of the matrix. No restrictions were imposed but the suggestion was made by the trainer to use a 5x5 matrix.

As a result, 14 matrices (10 for "campus", 4 for "antennas") were posted and additionally hung up in the classroom for a *web based anonymous voting procedure* (Figure 3) which was enriched by asking for the reasons for their decisions and the question for the optimal choice of concept for the two matrix dimensions (e.g. categories of potential effects horizontally versus affected societal actors vertically). 34 students (74%) took part in finding an "optimal" matrix for each one of the two themes and the posted arguments were fairly reasonable (example: matrix for "campus" see in Table 1).

In both cases, the matrix identified by "number 1" was selected by a very clear majority and consequently the discussion was held with these matrices. At this time of test implementation, the trainer did not yet fill in concrete text for the meaning of every single cell as the logical combination was considered sufficient.

Only by a closer analysis of correlations in voting behavior it could be revealed by the trainer that nine out of 34 votes (26%) had chosen matrix "number 1" in both cases, this was posted on the platform. In sharp contrast to statistically expectable probability distributions, "number 1" peaked out of the other votes drastically, interestingly by the amount of about nine votes. This gave rise to the hypothesis that without any deliberation (or by strategy) some students could have voted just formally but without any deeper motivation for their choice.

Consequently the trainer decided to *guide* more in this process of matrix generation in the second implementation.

(b) Students of "electronic engineering"

Here again the two themes have been agreed on after a one week deliberation phase. In this case, the 26 students were divided into the groups that correspond to their level 3 teams and asked in a first step to define the heads of rows and columns of their matrix (3x3 recommended this time); this meant 8 working teams for about 20 minutes. In a second step, all four teams belonging to the same theme had to convene on one new matrix starting from the four proposals. In a third step, these four teams had to find consensus on titles for the grid elements; this was meant as a first act of accommodation and deeper insight into the theme's structure in the tradition of "technology assessment".

2.2 Discussing with the matrix

(a) Students of "construction engineering and construction management"

Due to the experimental situation of the first implementation of a completely new game, *discussions were held* three times for construction students (BBM), for a typical situation in class see Figure 4:

(1) The first round occurred without prior written preparation and included 38 students (out of 46 = 82%) on only one subject "new FH campus" in four teams (construction business, administration, environmental lobby, economic lobby, see first third of Table 2); it was decided to be counted not at all for the final marks and hence does not appear in the statistics of the present study.
   (i) During this first round the 5x5 matrix on "FH campus" with 100 chips set by the teams resulted in 7 events of discussions that were really held lasting 20, 4, 4, 9, 9, 5 and 8 minutes. Students have decided to set the 100 chips in 8 to 25 parcels which is a strategy to strongly disperse the chips compared to later games and hence very high number of discussion events. As a result of the unexpected high number of discussion events and effects of tiring among the students the game was cancelled after about half of the potential length and the consequence of smaller matrices planned for the future.

(2) The second round included 44 students (out of 46 = 96%) on only one subject "antennas for mobile phones" in four teams with the same role names as above (names of the team leaders have been fixed with subsequent free gathering of the teams comprising 7, 14, 11, 12 students); it was decided to be counted as "level 3" for the mark and hence for the present report. The result was an outstanding success for the team "administration" as a result of their members' high engagement during discussion and pronounced knowledge of details. As a consequence, students suggested a more equilibrated distribution of rewards.
   (ii) During this second round the 3x3 matrix on "antennas" with 40 chips set by the teams resulted in five events of discussions (out of 8 possible = 63% with one ending in a consensus) lasting 9, 13, 4, 1 and 13 minutes and three occurrence of "bonus points" (i.e. if

only one team hat set chips on a matrix cell). Students have decided to set the 40 chips in three to eight parcels which was a comparatively dispersing strategy resulting in a relatively high number of discussion events. The size of the matrix (3x3) could be considered as the lower limit for good practicability of the game.

Figure 4: Typical situation in a SGC level 3 discussion.

These above first two rounds served additionally as a preparation for the visit of the mentioned external assessors in order to gain a first insight into the social dynamics created by the set of rules.

(3) The third round where three external assessors were present was held during the morning and the afternoon of the same day with all students distributed into two main groups using the same theme (FH campus) and therefore obeyed to the rule of SGC to split the entire class into two halves. For the sake of consistency, this round was taken as "level 4" for the students' marks. It should be noted here that at least one of the afternoon teams did not show up as planned due to a possible effect of tiring with too many discussion rounds in the experimental situation; therefore another group of students quickly decided on the spot to fill the vacant role (which could distort some statistical results as a consequence because they played two times which is perfectly in line with SGC vision "engagement pays off"). As a result of student feedback after the morning session which called for inclusion of "fact based expert opinions", one of the external experts and the trainer were decided to distribute additional points during the afternoon round.

(i) During the morning discussion the 3x4 matrix on "FH campus" with 60 chips set by the teams resulted in 3 events of discussions (= 25%) lasting 5, 5 and 8 minutes and several occurrences of rounds with "bonus points". Students have decided to set the 60 chips in three or four parcels which was a more aggregated strategy compared to earlier games and hence fewer discussion events.

(ii) During the afternoon discussion the same matrix resulted in 5 events of discussions (= 42%) lasting 10, 11, 11, 10 and 23 minutes and consequently a lower amount of "bonus events".

The *number of chips* to be distributed was used to *control the length* of the entire discussion event and therefore varied in the three rounds (100, 40, 60 chips). The *trainer has assessed the written standpoints* from the second and third rounds (rightmost column in Table 2) and given short feedback (positive and negative, two short items each) via the web platform after the discussion event.

Table 2: Overview of all rounds of discussion games during the first implementation held for construction students (BBM). The number of chips was varied in order to test resulting game lengths.

First round on "FH campus" with only one group (100 chips)				
Team name	**Number of students**	**Points P for team**	**Points p for student**	**Assessment by the trainer**
Construction firm	5	154	25.7	-
Administration	6	152	30.4	-
Environmental lobby	18	187	10.4	-
Economic lobby	9	123	13.7	-

Second round on "antennas for mobile phones", one group (40 chips)				
Team name	**Number of students**	**Points P for team**	**Points p for student**	**Assessment by the trainer**
Construction firm	7	93	13.3	24
Administration	14	27	1.9	16
Environmental lobby	11	15	1.4	32
Economic lobby	12	16	1.3	32

Third round on "FH campus" with two groups (60 chips)				
Team - morning	**Number of**	**Points P for team**	**Points p for**	**Assessment by the trainer**

	students		student	
Neighbors	7	95	13.6	32
Students	5	85	17.0	8
FH management	6	100	16.7	8
Municipality	5	95	19.0	0
Team - afternoon	**Number of students**	**Points P for team**	**Points p for student**	**Assessment by the trainer**
Neighbors	6	101.5	16.9	24
Students	8	166.5	20.8	0
FH management	7	98	14.0	24
Municipality	2	172	86.0	0

(b) Students of "electronic engineering"

Students had roughly one week time to gather as a team (after during the lecture only the name of the team speaker was nominated) and to write up and post a coordinated team's standpoint (Figure 5). For about three days they had the opportunity to look into their adversaries' argumentation.

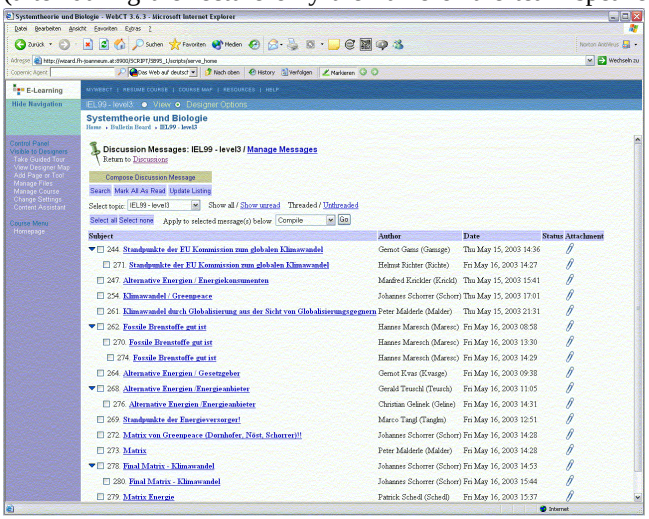


Figure 5: Via the bulletin board (folder level 3) the common standpoint of the team was communicated to the other colleagues before the level 3 discussion: each team starts one thread. The deadline for posting is one day before the discussion.

According to the rules and in a classroom setting like in Figure 7, the discussion process (2-3 hours per theme) was managed by the trainer and (in the very first implementations) an additional person assisting. Time for the discussions on the single cells was *measured* by an alarm clock as shown in the diagram of Figure 6. The discussion matrix visually documented to all participants via video projector (Figure 4, above right) where details were entered as seen in Figure 8 and Figure 9 in the case of students in electronics.

In the following paragraphs, the procedures of level 3 are documented for students in electronics. Discussion occurred for 4 out of 9 grid cells (= 44%), discussion length ranged from 10 minutes to 23 minutes (see italic text in the grid cells of Figure 8 and Figure 9).

Students belonging to the other theme were watching the entire discussion and had the possibility to use for their feedbacks the PCs standing along the wall of the class. This occurred 49 times which is 31% and delivered satisfying arguments. For these explanations and substantiations of voting behavior students collected points (on an average roughly one tenth of all level 3 points, see Figure 12 below right) that correlated slightly with level 2 reviewer rewards.

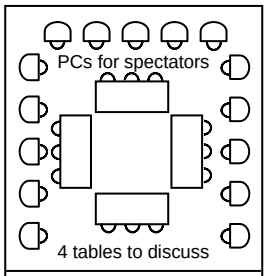


Figure 7: Suitable classroom

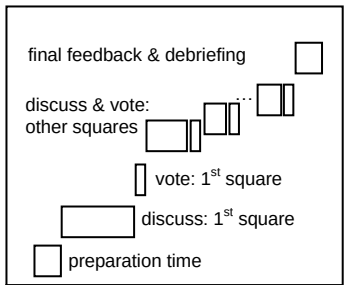


Figure 6: time plan for level 3 discussions

The matrices in Figure 8 and Figure 9 represent the thematic distribution of sub-themes that was held most suitable by the students after having performed the online decision shown in Figure 3 – performed with a more realistic sense and less pragmatic approach than the students in construction.

CLIMATE CHANGE	Environment	Humans	Economy
Traffic	*15 min., FEL , G, EU, OG* Effects of increased traffic volume on global temperature rise	*0 min., no team* Comfort by mobility	*22 min., FEL, EU, OG* *no winner* Transit
Laws	*20 min., G. u. EU* *consensus* Eco-tax	*0 min., no team* Restriction or enhancement of quality of life by environmental legislation	*23 min., G. u. OG* *consensus* Environmental obligations
Transformation of energy	*only FEL* Emissions of power plants	*only EU* Use of energy	*0 min., no team* Efficiency of energy transformation

Fossil Energy Lobby	FEL
Greenpeace	G
EU Comission	EU
Opponents of Globalization	OG

Figure 8: Matrix for the theme "*climate change*" used for level 3 with students in electronics (IEL).

ALTERNATIVE ENERGY	Energy price	Environment	Quality of life
Subsidies	*11 min.,G, AL , RP , C* Distortion of competition	*10 min., G. & AL* *no one wins* Weighing of distribution of subsidies	*only G* Promotion of quality of life
Legislation	*only RP* Regulation?	*only C* Targets	*10 min., G, AL, RP* *consensus* sustainable guaranteeing
Feasibility	*only AL* Rentability	*only C* Environmental Impact Assessment (EIA)	*13 min., AL u. C* *consensus* Consensus with neighbors

Government	G
Alternate Energy Lobby	AL
Reg. Energy Provider	RP
Consumer of Energy	C

Figure 9: Matrix for the theme "*alternative energy*" used for level 3 with students in electronics (IEL).

2.3 Statistical results concerning the discussion process

(a) Students of "construction engineering and construction management" (BBM)

Similar to level 2, one interesting question is whether or not the traditional assessment of paper quality *by the teacher is in line with the result of the game rules*. Again, there appears no positive correlation as shown in the four parts in Figure 10 for construction students. There could even be seen a negative correlation suggesting an inverse relationship of "points from trainer" and "points resulting from the discussion rules". This would mean that "the better the academic quality of the standpoints, the weaker the ability to reach victory in a controversy": a hint towards the principal *difference of academic and social skills* that both should be trained within Surfing Global Change!

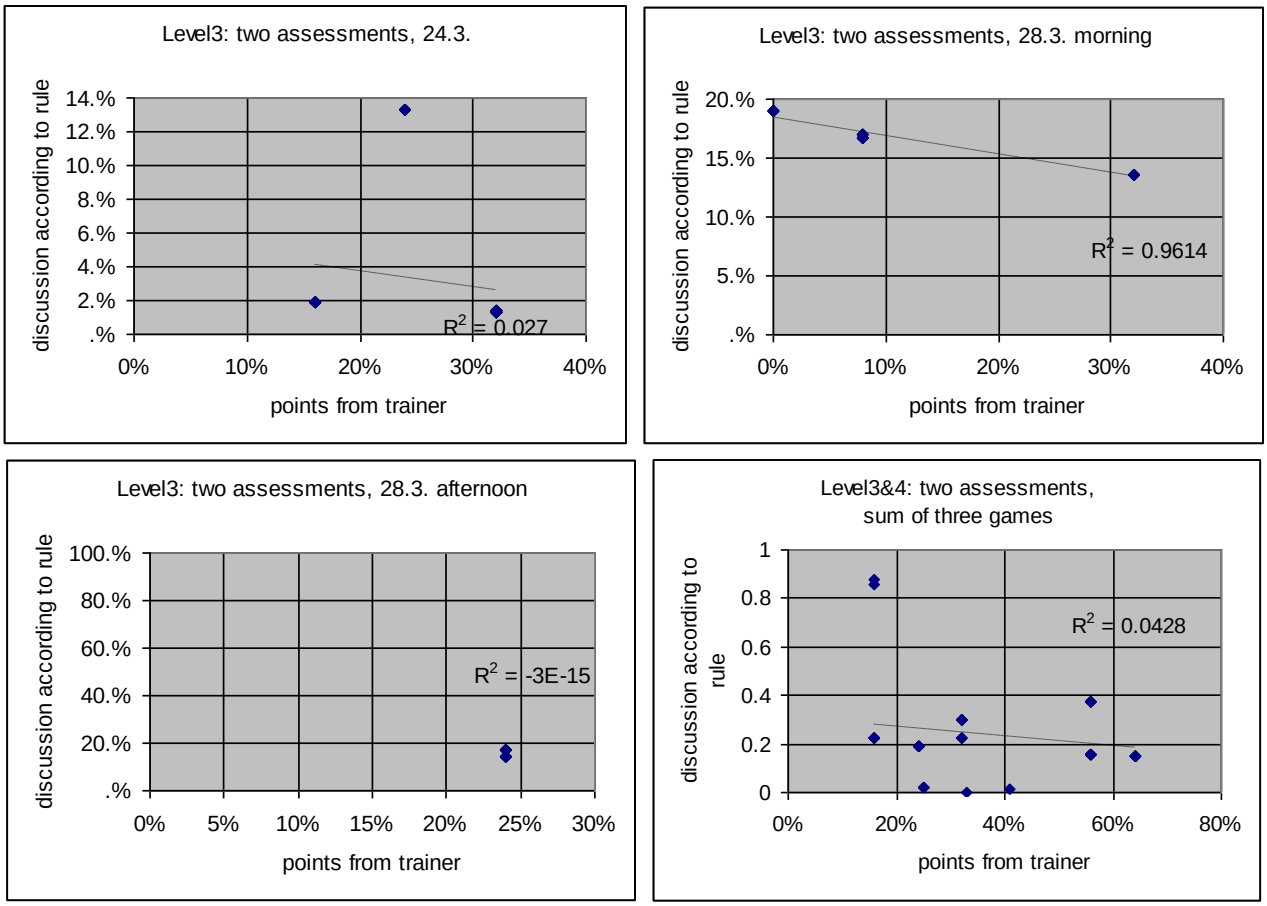


Figure 10: Four correlations of level 3 team points (P from Table 2) given by the trainer for the written standpoints with points resulting from the discussion rules, valid for construction students (BBM).

Given the *seemingly structural deviation between success in discussion versus in paper writing* and in order to exclude alleged "unjust voting by colleagues" in the class of construction students, it was decided to shift the relative importance decisively towards "trainer's assessment" which is shown by the large blue share of almost 90% in Figure 11 (left). This large share was reduced for the subsequent level 4 (Figure 11 right).

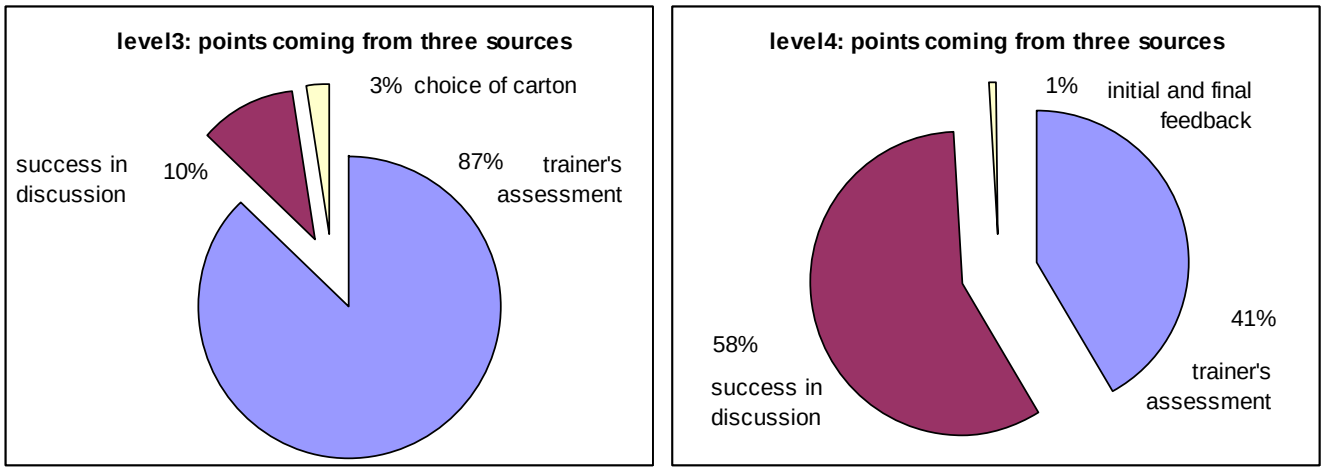


Figure 11: Composition of the average final level 3 and level 4 scores as a result of three components, valid for construction students (BBM), for comparison with electronics students (IEL) see Figure 12 below right.

(b) Students of "electronic engineering" (IEL)

The *same diagnosis* of "no correlation" (or rather inverse correlation) is valid for students in electronics (IEL) as shown in Figure 12 (above left).

An additional procedure was applied for the students in electronics: right after voting, the students not participating in the discussion could substantiate their voting decision via the web platform which brought them additional points. The incidence of these points, however, is not at all correlated with the level 3 points resulting from the discussion rule (Figure 12 above right), neither with the trainer's points (below left).

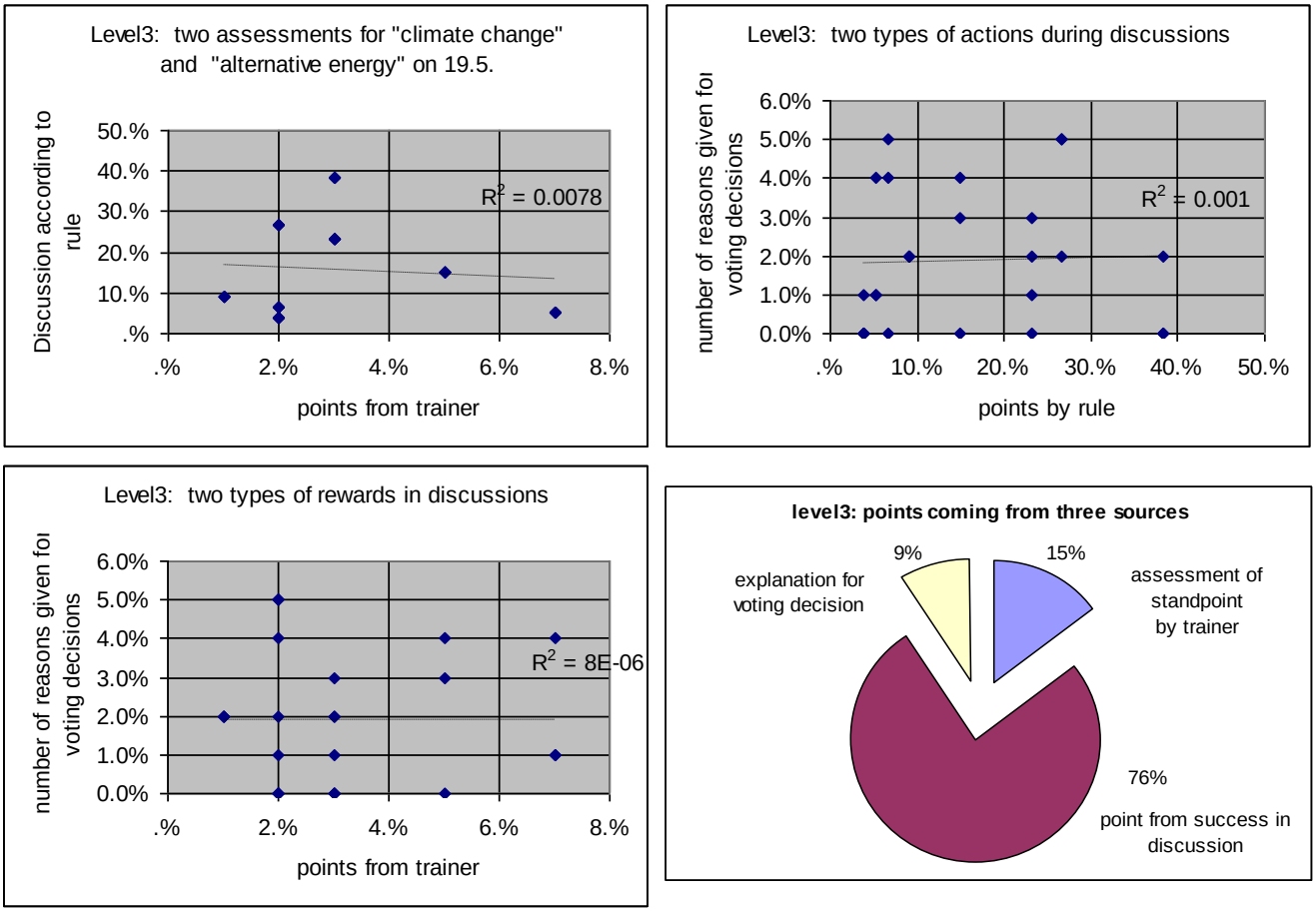


Figure 12: Three (*weak*) correlations of level 3 points resulting from the discussion rules with points from the trainer (above left) and rewards for declaring the reasons for voting decisions (above right) and the two latter with each other (below left). Composition of the average final level 3 score as a result of the three components mentioned above; for electronics students.

These results show that the trainer's assessment is quite independent of the assessment resulting from the rules, thus underlining the importance of taking into account *all divergent social and academic skills into the final mark* of the course. Because for students of electronics "unjust effects" when voting for the winning discussant seemed comparatively rare, the share of the trainer's assessment to the level 3 mark for electronics students (blue in Figure 12 below right) was deliberately kept much smaller than for construction students (Figure 11 left).

Especially for construction students the atmosphere during the discussion was a very vivid and even controversial one which might be partly due to the experimental situation in the first game implementation; for students in electronics the atmosphere was calmer.

2.4 Comparison of level 3 with other skills

(a) Students of "electronic engineering"

A possible hypothesis would be that the skills in level 3 are similar to the skills in level 2, namely both focused on stating and defending an own opinion in front of others. Out of such correlations for students in electronics in Figure 13 with generally no or at least very weak R^2, the rewards for reviewing in both levels are correlated slightly ($R^2 = 0.14$, Figure 13 center left). This would point to the fact that if students are inclined to reviewing activities they would act this way in both levels, which is quite plausible.

But the other five figures show NO connection between success in level 2 & level 3! Hence there seem to exist *two distinct social capabilities*, one being review of a text in *silence* and without an atmosphere of confrontation (level 2) and more fact-oriented, the other being a *struggle* for the external impression and a positive appearance of one's team in front of colleagues in a strongly controversial atmosphere under time constraints (level 3) with more orientation to the effect. Basically, this not really close similarity between the social skills demanded in these two levels is confirmed by the astonishingly weak correlations in Figure 15 below.

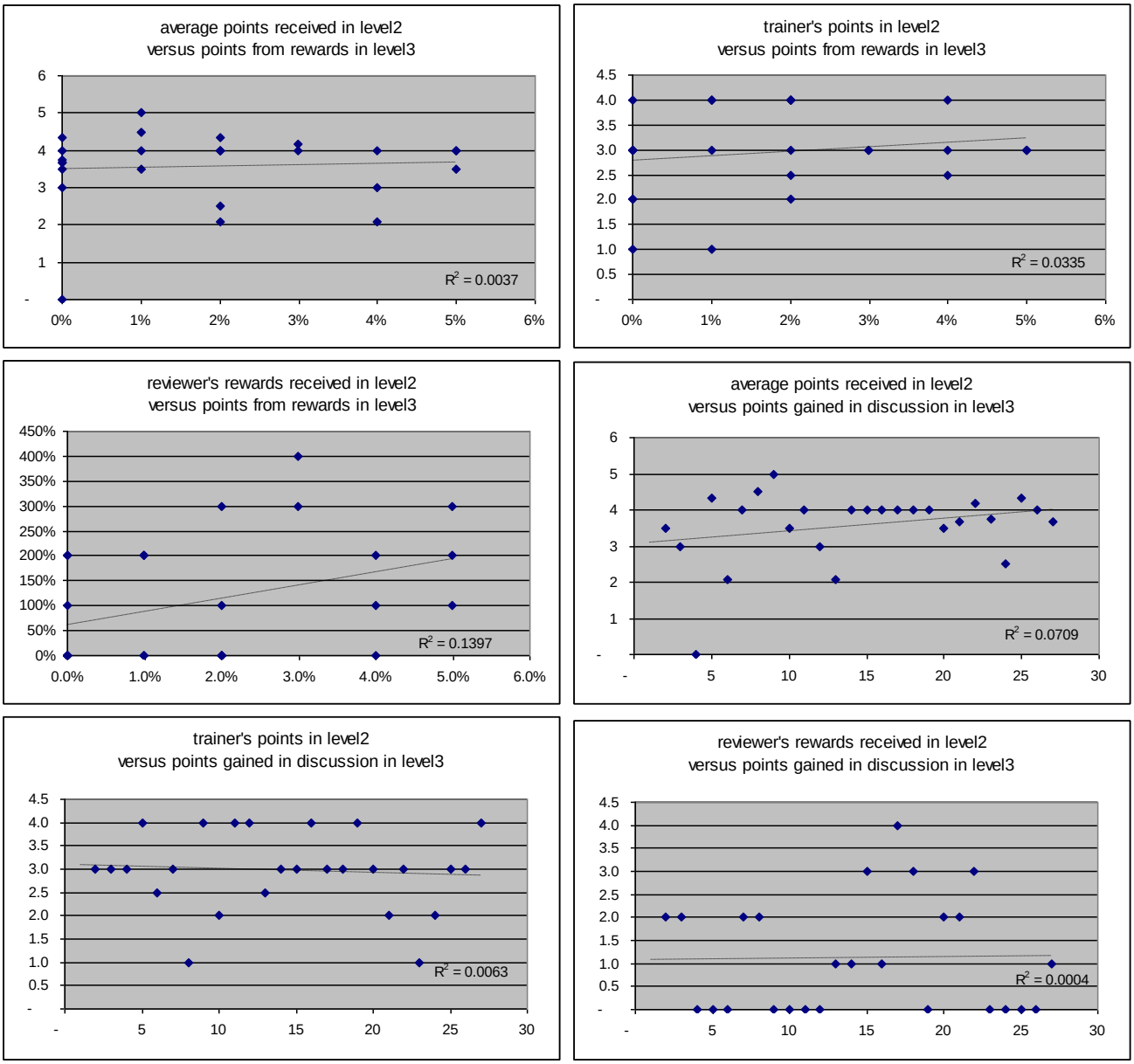


Figure 13: Six correlations of level 3 points (first three: resulting rewards for explanation of voting decision and second three: resulting from the discussion rules) with three types of points gained in level 2 (average points for authors, points from trainer, rewards for reviewers), valid for electronics students (IEL).

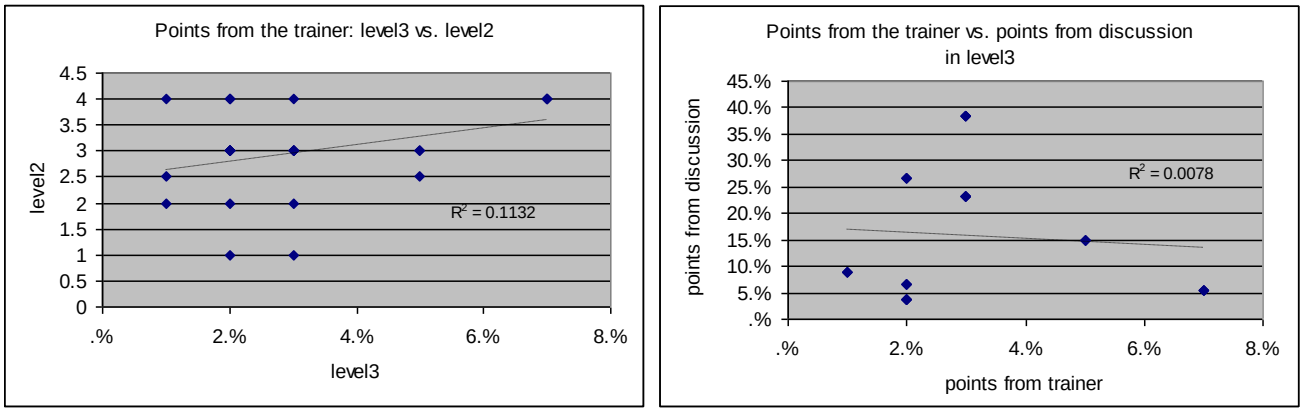


Figure 14: Two correlations of level 3 points from the trainer with points from trainer in level 2 (left) and points from the discussion (right), electronics students (IEL).

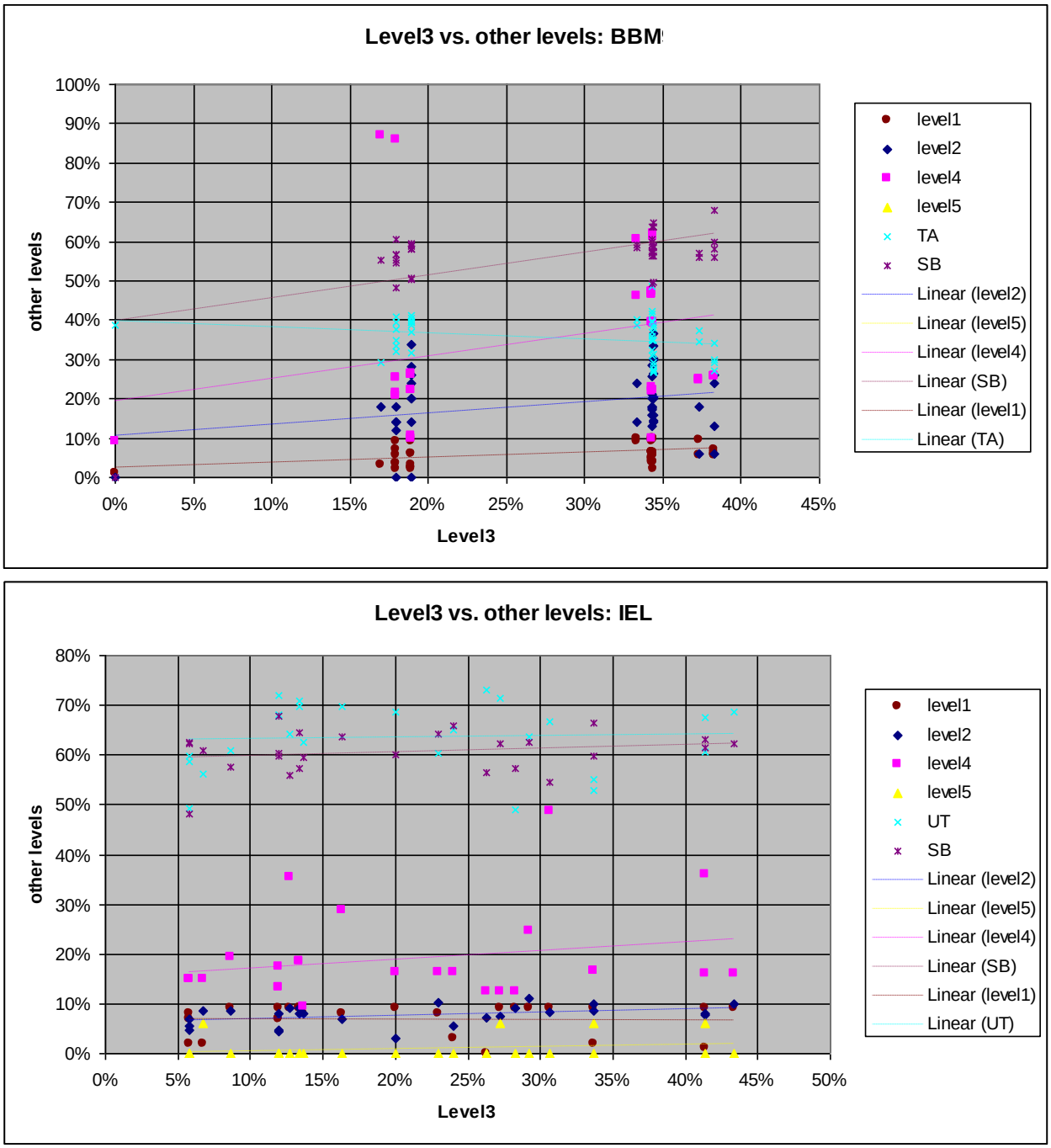


Figure 15: Connection between success in level 3 and other different levels for students in construction engineering (BBM) and electronic engineering (IEL).

There is only weak correlation between the trainer's assessment in level 3 and level 2 (Figure 14 left) and none with the points from discussion in level 3 (Figure 14 right).

Summing up, we find only a weak correlation between

- points received as rewards as for review in levels 2 and 3.
- points received from the trainer in level 2 and level 3, but no correlation between mixed variables.

(b) Students of both specialties

Regarding the comparison of overall level 3 results with other levels (Figure 15) it can be said that

- for construction students (BBM) there is a positive correlation with
  - SB quiz (weak negative with TA quiz)
  - level 4 (and weak with level 2)
- for electronics students (IEL) there is a weak positive correlation with
  - SB quiz
  - level 4 (and weak with level 2).

This hints to the fact that the above correlations are *independent of the students' specialty and their specific situation*. Apparently, the skills demanded in the discussion oriented levels 2, 3, 4 correlate weakly with each other. It may be concluded on a general level that this SGC system of threefold *mutual student assessment* averages potential distorting effects like "help to the friends" and is complemented by the assessment by the trainer.

3. Facts and statistics for level 4

3.1 The discussion process

Level 4 consists in a *consensus oriented discussion* on the basis of earlier preparation through *posted standpoints* (Figure 16).

After discussion, the procedure of voting in level 4 is very simple as it consists only in the selection of the option "consensus established" or "consensus failed".

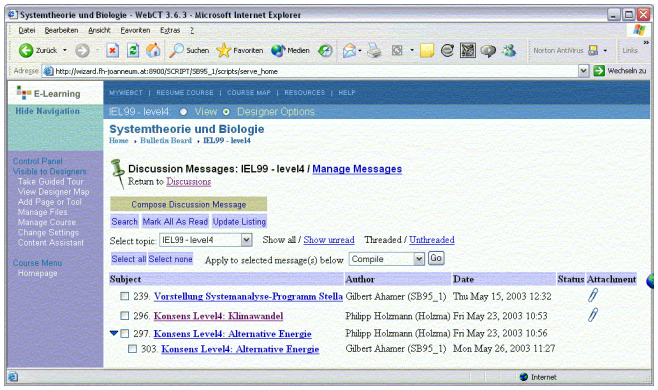


Figure 16: The proposed consensus texts are posted in the bulletin board were agreed"); they have been agreed on orally by the team speakers at the end of the consensus discussion

(a) Students of "construction engineering and construction management"

As mentioned above in the description of level 3 (see Table 2), the third round of discussion was counted as level 4. The statistics are discussed and displayed in the chapter on level 3 (Figure 10 and Figure 11 right).

(b) Students of "electronic engineering"

Due to the brevity of the process, no "trainer's assessment" has been performed in level 4. It is possible to perform a correlation between the score from discussion and the rewards for being an expert (Figure 17 left), which exhibits a correlation coefficient of almost zero but tends to a negative correlation as already found in the level 3 chapter. The correlation at right shows the connection of "points resulting from the rule" between level 3 and level 4 which is quite astonishingly practically non-existent (R^2 about zero).

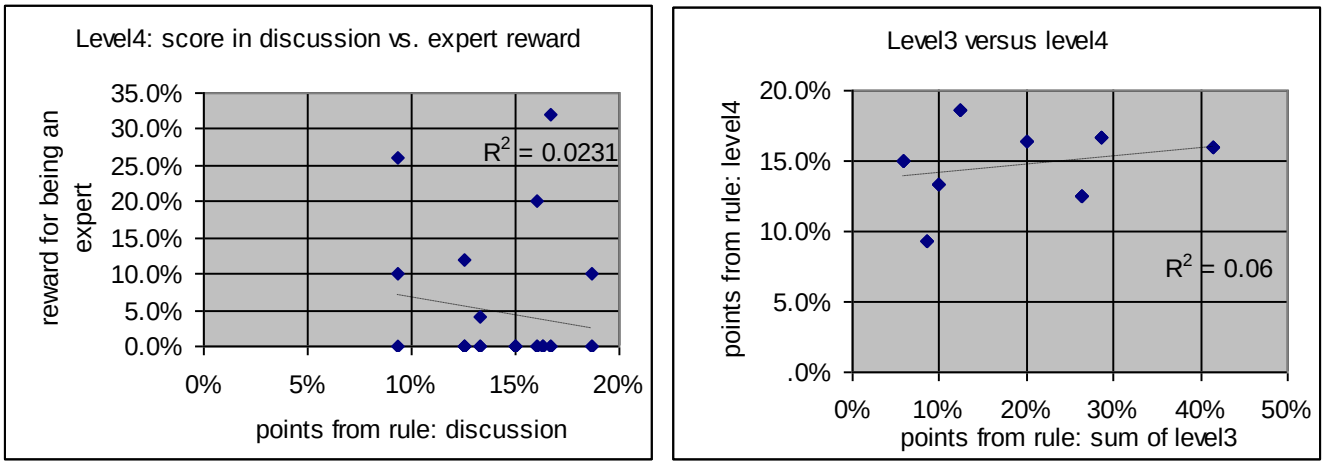


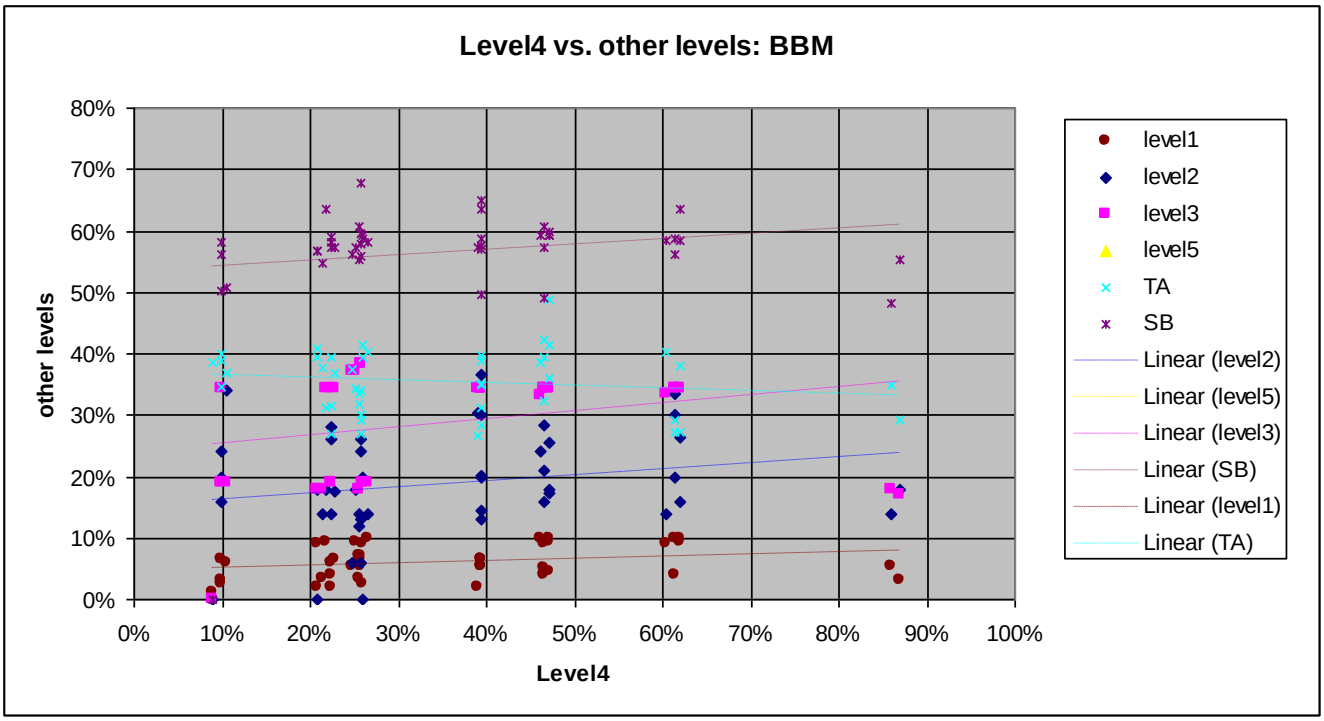
Figure 17: Two correlations of level 4 points resulting from the discussion rules; at left: with rewards for being an expert; at right: with the reasons for voting decisions; valid for electronics students (IEL).

3.2 Comparison of level 4 with other skills

Regarding the comparison of overall level 4 results with other levels (Figure 15) it can be said that

- for construction students (BBM) there is a positive correlation with
  - SB quiz (weak negative with TA quiz)
  - level 3, level 1 (and weak with level 2)
- for electronics students (IEL) there is a weak positive correlation with
  - UT quiz (weak negative with SB quiz)
  - level 3 (and weak with level 1),

hence that this analysis is mostly well in line with the one for level 3 (Figure 15) but again shows very weak correlations.



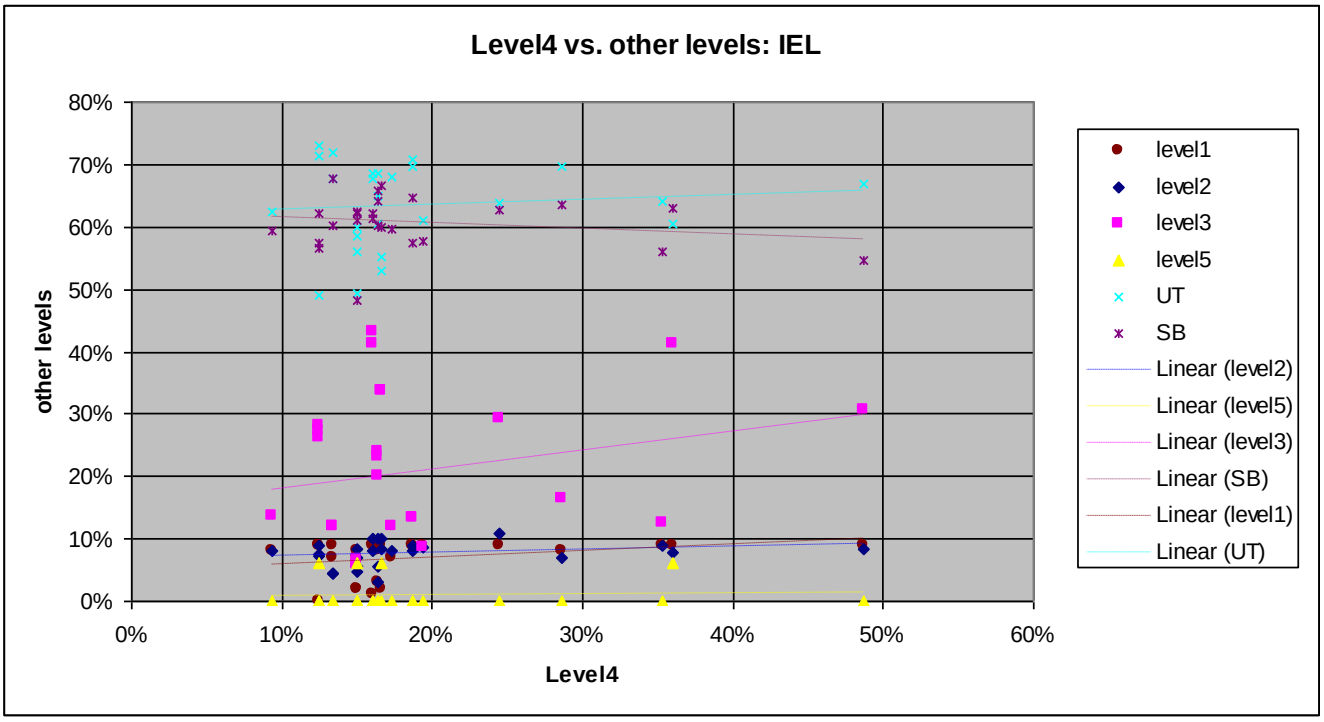


Figure 18: Connection between success in level 4 and other different levels for students in (BBM) and electronic engineering (IEL).

4. Facts and statistics for level 5

(a) Students of "construction engineering and construction management"

No explicit level 5 was undertaken for construction students due to time restrictions.

(b) Students of "electronic engineering"

At the end of the course period, students were presented the "Global Change Data Base" GCDB (Ahamer, 2001; Ahamer, Esser, 1997) and given the chance to improve their marks by voluntarily taking part in level 5, this option for "overwork" was taken by only one to two teams (Figure 19). For the future implementations, a better integration of level 5 into the regular course curriculum is envisaged.

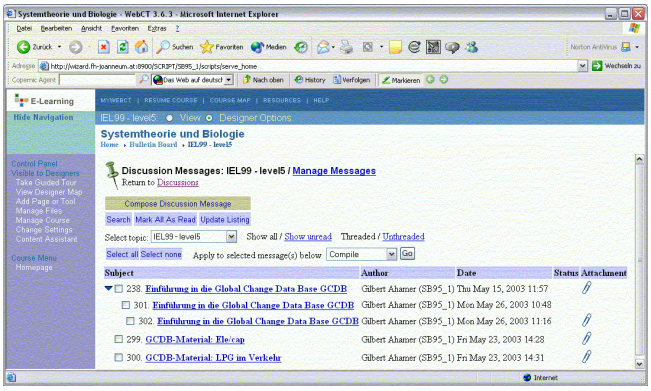


Figure 19: At the end of the game SGC the integrative analysis of a selected global trend (taken from the "Global Change Data Base" GCDB) is posted in folder "level 5" of the bulletin board, valid for IEL students.

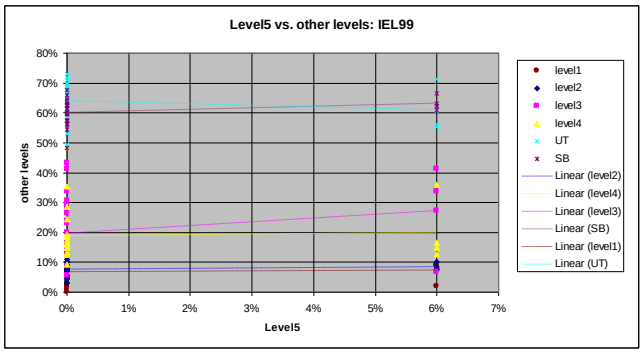


Figure 20: For the sake of completeness, the connection between success in level 5 and other different levels for students in (BBM) and electronic engineering (IEL) is displayed.

For the sake of completeness, the comparison of overall level 4 results with other levels is displayed in Figure 20 which tends to show

- for electronics students (IEL) a weak positive correlation with
  - SB quiz (weak negative with UT quiz)
  - level 3

thus being in line with the above two analogous comparisons.

5. Conclusion: Comparison of points from rules or from trainer

Looking at the construction student class (BBM) on an average, approximately 17% of the final mark is based on the rules of SGC, about 32% on the trainer's assessment and about 51% on quizzes (Figure 21). However, looking at the electronics student class (IEL) on an average, approximately 23% of the final mark is based on the rules of SGC, only about 8% on the trainer's assessment and about 69% on quizzes (Figure 22).

All in all, roughly one third of the final average score is based on the rules from SGC which was a very cautious strategy chosen for the first two implementations.

There seems to be *no* (BBM) or only a *very weak* (IEL) correlation between *points from the rule versus points from the trainer*, again *underlining the principal difference of the two kinds of skills monitored*. The correlation with points gained from the quizzes in the same figures below does not really add to a more striking impression of substantial correlation. Therefore *the three dimensions* of

1. quizzes (*fact-oriented knowledge*)
2. trainer's assessment (*academic writing* of a standpoint)
3. success in reviews and discussions (*presenting and arguing for a standpoint*)

really appear as "*linearly independent* dimensions" in the "space" of a *realistic and professional world*!

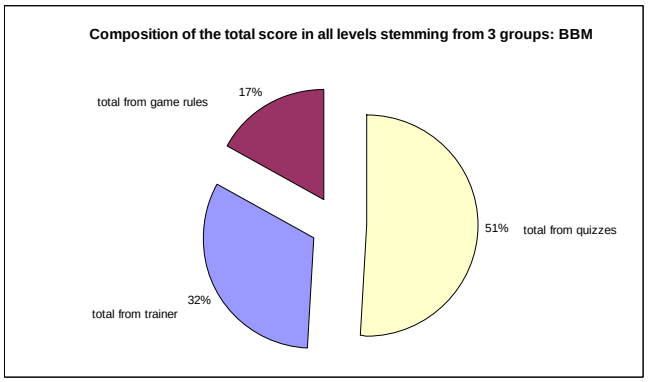


Figure 21: Three groups of points make up the overall sum of scores for construction students (BBM): game rules, trainer's points and quizzes; here it is shown from where they stem originally, regardless of the level.

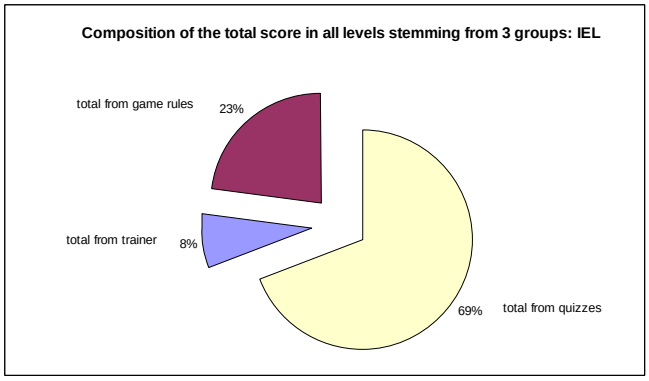


Figure 22: Three groups of points make up the overall sum of scores for electronics students (IEL): game rules, trainer's points and quizzes; here it is shown from where they stem originally, regardless of the level.

From this analysis it can be practically concluded that fine-tuning of SGC is facilitated by the relative weight of game points versus trainer's points.

By doing so, SGC can be *adapted to different levels of pragmatism versus idealism* expected from students.

It can also be learned from the above analyses of social processes that *the following categories of "realities"* are *dependent of the perspectives taken by stakeholders*:

- What is true and correct?
- What constitutes a "moral, ethical" value?
- What can be called "*good academic quality*"?
- What is relevant and what is irrelevant?

- What are the weighing factors for the single components of "relevant, true, applicable truth"?

All in all, the web-based negotiation game SGC analyzed above *is a means to converge students' world views by negotiation procedures*. For that target it is a valuable tool, as confirmed by other analyses (MD, 2007).

A symbolic way to depict "differing perspectives onto the same reality" are tools provided by Geographic Information Systems (Figure 23): one and the same act of running, cycling or walking through an "*objective physical* scenery (left sides, Graphics displayed by Google Earth) creates different "*subjective physiological* sceneries" in the active stakeholder, i.e. the sportive subject (right sides, graphics from Polar 2011).

Similarly, in (political) reality (compare GS, 2011, IE, 2011) one and the same physical data trigger personality-dependent *images* to the involved stakeholders.

Therefore, *political participation* is indispensable to take account of this structure of reality. Public participation GIS (*PPGIS*) is one possible IT-based tool to achieve consensus.

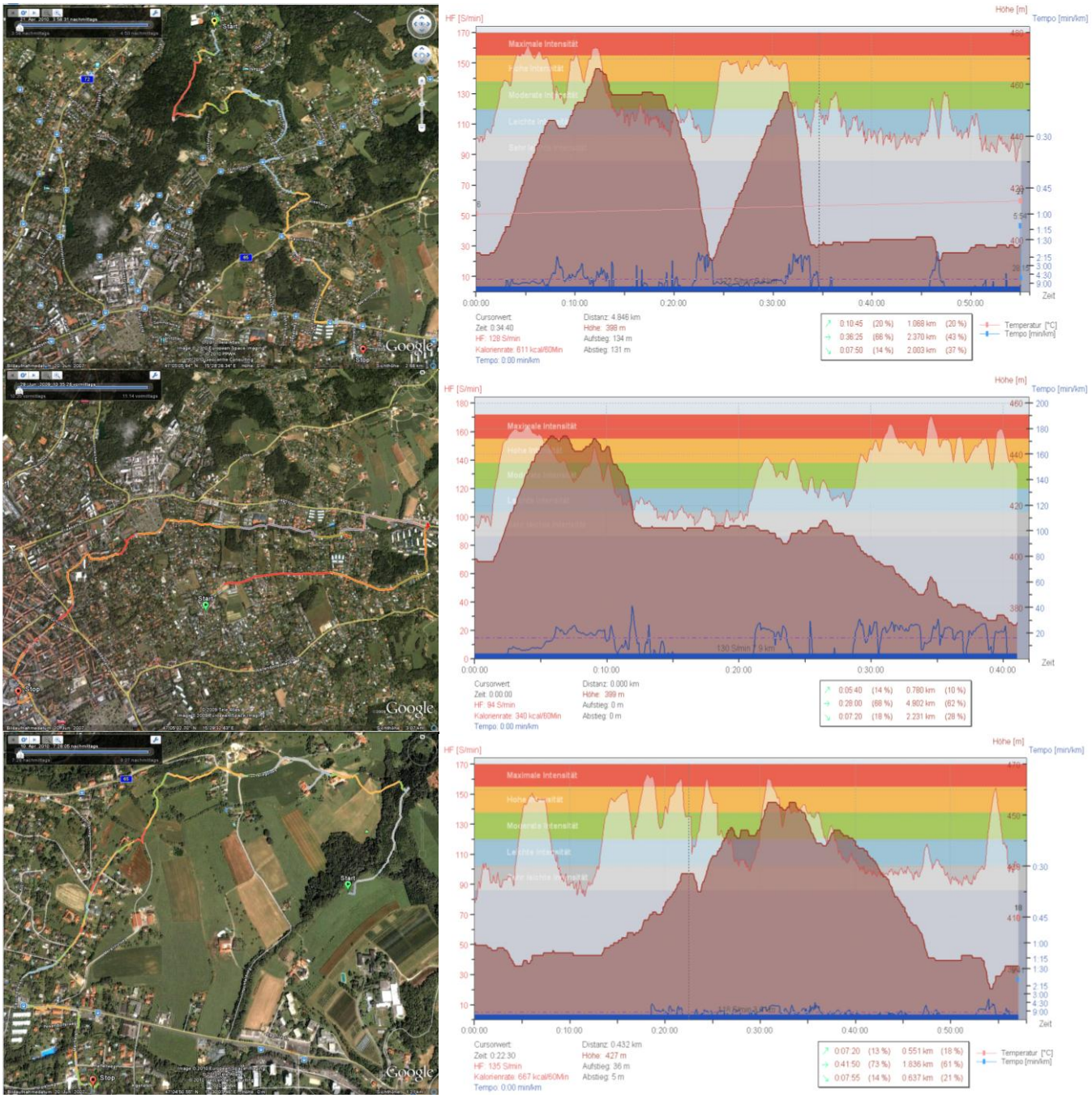


Figure 23: Moving through "*objective*" physical landscape (left sides) creates different "*subjective*" physiological landscapes for the active person (right sides), when running, cycling or walking. Legend: thin red line: heart rate (ranging from gray = low to red = high; these colors are marked also in the path measured by GPS), brown: altitude, blue: speed.

References

Ahamer, G. (2004). Negotiate your future: Web based role-play. *Campus-Wide Information Systems*, *21*(1), 35-58, see http://www.emeraldinsight.com/1065-0741.htm. (Outstanding Paper Award 2005: http://www.emeraldinsight.com/info/authors/literati_news/awards/papers_2005.jsp#5).

Ahamer, G. (2006). SURFING GLOBAL CHANGE: Negotiating sustainable solutions. *Simulation & Gaming - an International Journal*, 37(3), 380-397. http://www.unice.fr/sg/, text at http://sag.sagepub.com.

Ahamer, G. (2010). A short history of web based learning including GIS. *International Journal of Computer Science & Emerging Technologies (IJCSET)*, 1(4), 101-111, http://ijcset.excelingtech.co.uk/vol1issue4/17-vol1issue4.pdf.

Ahamer, G., Strobl, J. (2010). Learning across Social Spaces. In: "*Cases on Technological Adaptability and Transnational Learning: Challenges and Issues*", Mukerji S. & Tripathi, P. (Eds.), pp. 1-26, IGI Global, Hershey, New York, for its content click on "free sample chapter" at http://www.igi-global.com/bookstore/titledetails.aspx?titleid=37311&detailstype=chapters.

Castells, M. (2010). An Introduction into the Information Age. In: G. Bridge, S. Watson (eds.), The Blackwell City Reader, John Wiley and Sons, pp. 40-48, see http://books.google.com/books?id=P2aC62fqCyQC&hl=de&source=gbs_navlinks_s.

FHJ (2011). Curricula of construction Management and of Electronic Engineering at the University of Applied Sciences (= Fachhochschule) Joanneum in Graz and Kapfenberg, Austria. See http://www.fh-joanneum.at/aw/home/Studienangebot/fachbereich_leben_bauen_umwelt/~czk/bmi/?lan=en and http://www.fh-joanneum.at/aw/home/Studienangebot/fachbereich_information_design_technologien/~boct/aee/?lan=en.

Gierlinger-Czerny, E. (2003). Gutachten des Spiels „SurfingGlobalChange" durchgeführt in einer Vorlesung Systemtheorie im Lehrgang für Baumanagement an der FH Joanneum Graz.

Gierlinger-Czerny, E. & Peuerböck, U. (2002). *Auf dem Weg zur Selbstorganisation – eine Ermutigung neue Unterrichtswege zu beschreiten*, LIT, Münster.

Global Studies (2011). Masters Curriculum Global Studies, Karl-Franzens University Graz, http://www.uni-graz.at/globalstudies/.

Healey P.G.T., White, G., Eshghi, A., Reeves, A.J., Light, A. (2008). Communication Spaces. *Computer Supported Cooperative Work*, 17(2-3), 169-193.

Heiskala, R. (1990). Sociology as a Discursive Space - The Coming Age of a New Orthodoxy? *Acta Sociologica* 33(4), 305-320.

IE (2011), Internationale Entwicklung (= International Development). Curriculum at the University of Vienna, http://www.univie.ac.at/ie/.

Mukerji, S., Tripathi, P. (2010). Information Technology for Enhanced Learning and Understanding: Are We Truly Inclusive? *Journal of Cases on Information Technology* (JCIT), 12(3), i-iii, http://www.igi-global.com/Files/Ancillary/1548-7717_12_3_Preface.pdf.

MP (2007). Selection of finalists in the highest rewarded European prize on Media Didactics MEDIDAPRIX, http://www.medidaprix.org/mdd_2007/dynframeset_006.html.

Pavan E., Diani M. (2010). Structuring online and offline discursive spaces on Internet governance. Insights from a network approach to map an emergent field.. Sprouts: Working Papers on Information Systems, 10(21). http://sprouts.aisnet.org/10-21.

Polar (2011). RS800CX: Wrist watch monitoring heart rate, location, speed, altitude, temperature etc., see http://www.polar.fi/en/support/product_support?product=7976.

Rauch, H. (2003). *Report about the social dynamics of the digital learning game "SurfingGlobalChange" (SGC).* Expert opinion by Institut für Socialanalyse.

Rauch, H. (2000). *The Challenge Principle - Introduction to Systemic Social Analysis (Synoptics): Method, Theory and Case Studies*. Institute for Social Analysis, Vienna, Austria, 275 p.

USW (2011). Environmental Systems Analysis (Umweltsystemwissenschaften), Reports of Interdisciplinary Practicals, see http://www.uni-graz.at/usw1www/usw1www_magazin/usw1www_berichte.htm.

Wikipedia (2011). Pierre Bourdieu. See http://en.wikipedia.org/wiki/Pierre_Bourdieu#Work.

Author Biography

Gilbert Ahamer: After numerous struggles in environmental politics, he strived to produce an IT-based methodology to better solve complex interdisciplinary and multi-stake-holder issues for his students in architecture, construction management and industrial electronics. At the Institute for Geographic Information Sciences he learned that "spaces" are rather constructed by human communication than "real"… … just as reflected by experiences from "*Surfing Global Change*".

Design Considerations for Ultra-Low Energy Wireless Micro sensor Nodes

Khyati Chourasia[*3], Dr. Anubhuti Khare[1], Manish Saxena [*2]

[1]Dr. Anubhuti Khare, Reader, Department of Electronics and Communication, University Institute of Technology, Rajeev Gandhi Technical University, Bhopal, Email:- anubhutikhare@gmail.com, Mobile:+919425606502
[2]Manish Saxena, Head Of Electronics and Communication Department, Bansal Institute Of Science And Technology Bhopal, Email:- manish.saxena2008@gmail.com, Mobile: +919826526247
[3*] Khyati Chourasia,Student,Mtech(Digital Communication), Bansal Institute Of Science And technology Bhopal. Email- khyati.chourasia@gmail.com.

Abstract—*this tutorial paper examines architectural and circuit design techniques for a micro sensor node operating at power levels low enough to enable the use of an energy harvesting source. These requirements place demands on all levels of the design. We propose architecture for achieving the required ultra-low energy operation and discuss the circuit techniques necessary to implement the system. Dedicated hardware implementations improve the efficiency for specific functionality, and modular partitioning permits fine-grained optimization and power-gating. We describe modeling and operating at the minimum energy point in the transmitter and the ADC. A micro sensor node using the techniques we describe can function in an energy-harvesting scenario.*

Index Terms—Integrated circuits, energy-aware systems, low-power design, wireless sensor networks

1. Introduction

Wireless microsensor networks consists of tens to thousands of distributed nodes that sense and process data and relay it to the end-user. Applications for wireless sensor networks range from military target tracking to industrial monitoring and home environmental control. The distributed nature of micro sensor networks places an energy constraint on the sensor nodes. Typically, this Constraint is imposed by the capacity of the node's battery For this reason, most micro sensor networks duty cycle, or shutdown unused components whenever possible. In this paper, duty cycling refers generically to alternating between an active mode and a low-power sleep mode. Although duty cycling helps to extend sensor network lifetimes, it does not remove the energy constraint placed by the battery. For some applications, a limited lifetime is sufficient and battery power is the logical choice. A 1cm Lithium battery can continuously supply 10 W of power for five years. This tutorial focuses on applications demanding higher peak power or longer lifetime in an environment where changing batteries is impractical or impossible, therefore requiring a renewable energy source

Research into energy scavenging suggests that micro sensors can utilize energy harvested from the environment Energy harvesting schemes convert ambient energy into electrical energy, which is stored and utilized by the node the most familiar sources of ambient energy include solar power, thermal gradients, radio-frequency (RF), and mechanical vibration. Table 1 gives a comparison of some energy harvesting technologies. Power per area is reported because the thickness of these devices is typically dominated by the other two dimensions. The power available from these sources is highly dependent on the nodes environment at any given time. However, these examples show that it is reasonable to expect 10s of microwatts of power to be harvested from ambient energy. Barring significant advances in energy scavenging technology, the high instantaneous power consumption of an active wireless transceiver (mill watts for Mbps) requires micro sensors to retain local energy storage. Coupling energy harvesting techniques with some form of energy storage can theoretically extend micro sensor node lifetimes indefinitely.

Using a rechargeable energy reserve with energy-harvest in implies several constraints for improving node efficiency First, the standby power of the node must be less than the average power supplied by the energy-harvesting mechanism. If this is not the case, then energy-harvesting cannot recharge the battery and the nodes will expire. Second, the node should use as little energy as possible during active operation. Minimizing energy per operation allows decreased energy storage capacity (size, weight, and cost) and/or a higher duty cycle (better performance). Third, the node should transition gracefully to and from standby mode with very little time or energy overhead, increasing the efficiency of duty cycling for extremely short periods of time in the active mode.

2. Micro Sensor Node Architecture

The AMPS-1 sensor node, a representative node example, provides a hardware platform for distributed micro sensor networks using commercial, off the-shelf (COTS) components. The sensor node processor uses dynamic voltage scaling (DVS) to minimize energy consumption for a given performance requirement. The radio transmit power adjusts to one of six levels, depending on the physical location of the

target nodes. Power consumption of the node varies from 3.5mW in the deepest sleep state up to almost 2W (1.1W of which goes into the transmitter power amplifier) with the processor running at the fastest clock rate and the radio transmitting at the highest power level. Fig. shows the instantaneous power consumption of a AMPS-1 node as it collects data samples from the microphone, performs a line-of-bearing (LOB) calculation on the collected data, and relays the results of this calculation to other nearby nodes. Using generic components makes the power too high for the constraints we have described, so a customized architecture is necessary

The energy savings of a custom approach come from modularizing the sensor node by considering common tasks for sensor network applications. Key tasks which can be implemented in hardware include the fast Fourier transform (FFT), finite impulse response (FIR) filters encryption, source coding, channel coding/decoding, and Encryption, source coding, channel coding/decoding, and interfaces for the radio and sensor. In order to achieve energy efficiency throughout the entire system, the hardware modules can use independent voltage supplies and operate at different clock frequencies. The drawbacks of this architecture are the increase in system complexity and area the need for additional data

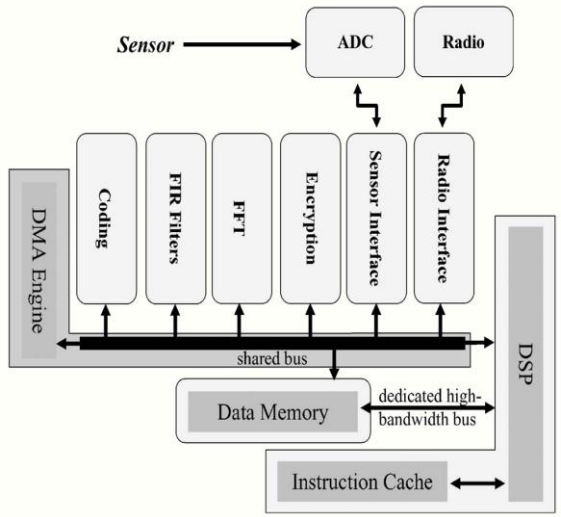


Figure 1 - Proposed architecture of an energy-efficient sensor node

transfers between the DSP and specialized modules, and the difficulty of interoperability across different voltage and clock islands Fig1 shows our proposed architecture for an energy efficient sensor node. The digital architecture contains a simple DSP that executes arbitrary programs. The DSP communicates with the specialized modules through a shared bus and the DMA schedules the transfer of data between modules and the bus. Data memory is accessible by both the specialized modules and the DSP.

Dynamic voltage scaling (DVS) can be used to trade energy for computational latency for each module. A module's supply voltage should be set to the lowest possible value that satisfies its speed requirements. However, there is a supply voltage below which computations become less energy efficient due to leakage currents .When no computation is taking place, the supply voltage should be shut off from the CMOS logic to reduce leakage power. The analog modules require the same dynamic performance controls as the digital modules. Both the sensor and radio must have an "always on," low-power standby mode that allows for basic threshold detection of a wake-up signal. For instance, an audio sensor might operate in a low-power mode until sound of a certain magnitude is detected.

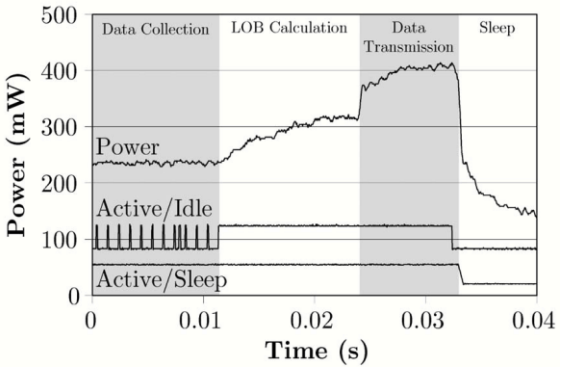


Figure 2 - Power-scaling measurements on the AMPS-1 node

3. Digital Circuit Techniques

Digital circuit design for the micro sensor space must focus primarily on the energy and power constraints we have presented, rather than solely on maximizing performance .The unpredictable environment of micro sensor networks coupled with less stringent performance requirements allows a trade-off of speed for reduced energy at both the architecture and circuit levels.

3.1. Sub threshold Operation:--

When minimizing energy is the primary system requirement, the sub threshold region gives the minimum energy solution for most circuits. Sub threshold circuits use a supply voltage V DD that is less than the threshold voltage, V T voltage of the transistors. In this regime, sub threshold leakage currents charge and discharge load capacitances Limiting performance but giving significant energy savings over nominal V DD operation. Fig. 5 gives an example of sub threshold operation for a 0.18 m CMOS technology. The left-hand plot shows the measured frequency of a ring oscillator versus V DD, Once V DD drops into the subthres- hold region, the on-current of the transistors becomes exponential with voltage and the I on = I off ratio reduces quickly. This causes the delay to increase exponentially. The right-hand plot shows an oscilloscope plot of an FIR filter

operating at 150mV and 3.2 kHz.

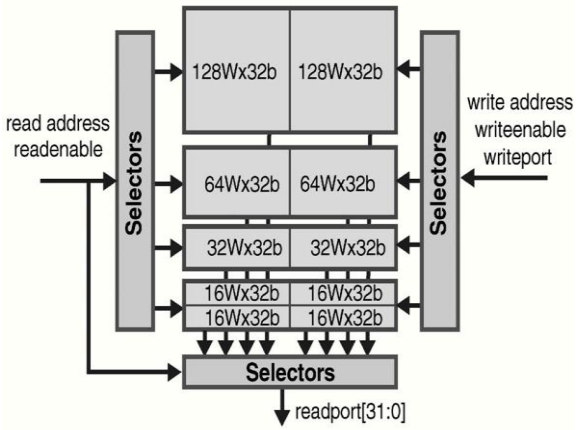


Figure 3 - Scalable FFT memory that enables variable memory size

Fig. shows give measurements from a sub threshold FFT processor that shows how minimum energy operation does not necessarily occur at minimum voltage operation. The 0.18 m CMOS chip implements a 1,024-point, 16-bit FFT A new sub threshold design methodology using a modified standard logic cell library, custom multiplier and memory generators was employed to implement the processor without additional process steps or body-biasing The processor operates down to 180mV, where it runs at164Hz and 90nW. The figure shows the minimum energy point for the 16b, 1,024-pt FFT processor at 350mV, where it dissipates 155nJ/FFT at a clock frequency of 10 kHz. As V DD decreases, the switching energy reduces quadratically. But propagation delay increases exponentially in the sub threshold region, allowing leakage current to integrate longer for each operation. The resulting increase in leakage energy causes the minimum energy point. For 8-bit operation, the minimum energy point moves to higher V DD Since the scenarios, we present a model for finding minimum energy operation in the sub threshold region.

3.2. Sub threshold Energy Modeling:--

In order to develop a model for sub threshold operation of arbitrary circuits, we first examine the sub threshold propagation delay of a characteristic inverter

4. Standby Power Reduction—

In the energy-aware FFT architecture described earlier signals are gated to improve energy efficiency. This technique reduces active power dissipation, but leakage power is not affected. As nanometer CMOS processes are leveraged to improve performance and energy-efficiency leakage mitigation becomes an increasingly important design consideration. Deep submicron processes have increased sub threshold leakage, gate leakage, gate-induced drain leakage, and reverse biased diode leakage [13]. The literature contains many techniques for standby power reduction. Two promising approaches for micro sensor nodes are multi-threshold CMOS (MTCMOS) and standby Voltage scaling Fig. 8 shows how MTCMOS circuits reduce standby leakage power by severing a circuit from the power rails with high VT sleep devices . Sizing the sleep transistor has received a lot of attention since over

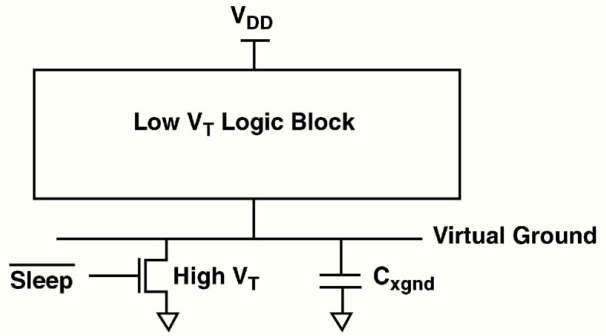
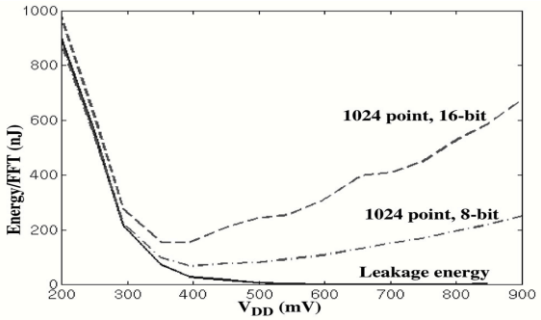


Figure 4 - MTCMOS power-gating circuits for standby power reduction

sizing limits the leakage savings while under sizing restricts performance Likewise, designing sequential MTCMOS circuits takes special care to reduce leakage during sleep without losing state Most MTCMOS designs use large sleep devices at the block level, but local sleep devices allow circuit partitioning into local sleep regions. Any unused circuit regions can enter sleep mode while surrounding circuits remain active. This approach only provides savings if all leakage currents are prevented during sleep mode. A careful



design methodology can prevent subtle leakage paths from occurring at the MTCMOS interface to active circuits. A fabricated 0.13- m, dual V T CMOS test chip shows low power FPGA architecture with over 8X measured standby current reduction [19]. The local sleep regions reduce active chip leakage by up to 2.2X for some configurations. The test chip uses sequential elements that allow power gating without the loss of data.

5. ADC and Sensor Subsystem

In sensor nodes, where a low-power DSP performs application-level processing, a front-end analog-to-digital conversion system acquires data from the physical sensor Since the ADC requirements are tightly coupled to a generally unpredictable environment, the ability to dyna- mically compromise features and performance in favor of power reduction

is a valuable characteristic. In the limit, the ADC subsystem may act only as a threshold detector. This requires downstream data processing units to tolerate the compromises and to provide feedback to the ADC Subsystem regarding the desired operating mode. Factors affecting that decision feedback might include characteristics of the sensing environment or the availability of harvested energy. This section examines a number of dimensions along which scaling could have a significant effect on overall power for the sensor front-end and ADC .The design of a low power ADC subsystem requires consideration of the entire front-end, not just the ADC

Fig. shows a very simple ADC subsystem. The components shown include a sensor, a low-noise preamplifier, an ant aliasing filter, an ADC, and a DSP. Here, the DSP may be used for the application of ADC linearity calibration coefficients offset/gain error cancellation or digital decimation filtering.

In the case of low-event sensor nodes, optimizations in three critical states have been identified. These include

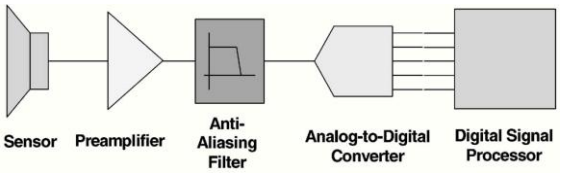
1. As used here, the power consumption of the physical sensor would be prohibitive to a self-powered node. Innovations in sensor technology or customized raw transducers are required.
2. This factor does not consider an increase in unit capacitances required in order to improve matching characteristics of fabricated elements
3. Some minimal circuitry to manage standby-to-active state transitions such as a counter, might impose additional overhead

6. Conclusion

This paper describes the challenges facing wireless micro- sensor design and presents a general micro sensor node architecture. The challenge for next generation nodes is to further reduce energy consumption by optimizing energy awareness over all levels of design. Sub threshold operation power gating, and standby voltage scaling enable digital circuits to meet the low active energy and standby power requirements of micro sensor nodes. Reducing startup time improves the energy efficiency of a transmitter for short packets and multi routing reduces energy for long- distance communication. Since the ADC subsystem might be the front-end of a reactive sensor node, it is important to seek alternatives to full sleep modes. We analyzed the dimensions along which ADC performance might be compromised in order to recover power savings. Applying all of these techniques to a micro sensor node makes energy-harvesting operation a possibility for micro sensor networks.

7. Acknowledgment

Mrs.Anubhuti Khare one of the authors is indebted to Director UIT RGPV Bhopal for giving permission for sending the paper to the journal. Manish Saxena is also thankful to the chairman, Bansal Institute of Science &Technology Bhopal for giving permission to send the paper for publication. Last but not least, I would also like to thank our HOD and colleagues for supporting us.



References

[1] S. Roundy, P. Wright, and J. Rabaey, “A Study of Low Level Vibrations as a Power Source for Wireless Sensor Nodes,”
Computer Comm., vol. 26, no. 11, pp. 1131-1144, July 2003

[2] H. Kulah and K. Najafi, “An Electromagnetic Micro Power Generator For Low-Frequency Environmental Vibrations,” Proc
17th IEEE Int’l Conf. Micro Electro Mechanical Systems (MEMS) pp. 237-240, Jan. 2004

[3] S. Meninger et al., “Vibration-to-Electric Energy Conversion,” IEEE Trans. Very Large Scale Integration (VLSI) Systems, vol. 9, no. 1 pp. 64-76, Feb. 2001

[4] H. Bottner et al., “New Thermoelectric Components Using Microsystem Technologies,” J. Micro Electro Mechanical Systems vol. 13, no. 3, pp. 414-420, June 2004

[5] “Panasonic Solar Cell Technical Handbook ’98/99,” Aug. 1998

[6] J.M. Kahn, R.H. Katz, and K.S. J. Pister, “Next Century Challenges: Mobile Networking for ’Smart Dust’,” Proc. Mobicom 1999, pp. 271278, 1999

[7] J. Rabaey et al., “PicoRadio Supports Ad Hoc Ultra-Low Power Wireless Networking,” Computer, pp. 42-48, July 2000.

[8] A. Wang and A.P. Chandrakasan, “A 180 mV FFT Processor Using Subthreshold Circuit Techniques,” Proc. Int’l Solid-States Circuits Conf. (ISSCC), pp. 292-293, Feb. 2004.

[9] A. Wang, A. Chandrakasan, and S. Kosonocky, “Optimal Supply and Threshold Scaling for Subthreshold CMOS Circuits,” Proc Symp. VLSI, pp. 5-9, 2002

[10] J. Burr and A. Peterson, “Ultra Low Power CMOS Technology,” Proc. Third NASA Symp. VLSI Design, pp. 4.2.1-4.2.13, 1991

[11] B.H. Calhoun and A. Chandrakasan, “Characterizing and Modeling Minimum Energy Operation for Subthreshold Circuits,” Proc Int’l Symp. Low Power Electronics and Design (ISLPED), Aug. 2004

[12] K. Osada et al., “SRAM Immunity to Cosmic-Ray-Induced Multierrors Based on Analysis of an Induced Parasitic Bipolar
Effect,” IEEE J. Solid State Circuits, vol. 39, no. 5, pp. 827-833, May2004

[13] R.H. Walden, “Analog-to-Digital Converter

Survey and Analysis IEEE J. Selected Areas in Comm., vol. 17, no. 4, pp. 539-550, Apr1999
[14] M. Bhardwaj, T. Garnett, and A. Chandrakasan, "Upper Bounds on the Lifetime of Sensor Networks," Proc. IEEE Int'l Conf. Comm., pp. 785-790, 2001
[15] J. Kao and A. Chandrakasan, "MTCMOS Sequential Circuits Proc. European Solid State Circuit Conf. (ESSCIRC), 2001
[16] F.M. Gardner, Phase Lock Techniques. New York: Wiley, 1979
[17] S.H. Cho and A.P. Chandrakasan,"6.5GHz CMOS FSK Modulator for Wireless Sensor Applications," IEEE Symp. VLSI Circuits, pp. 182-185, 20

Trends of Utilisation of Online Electronic Resources in Higher Education System- A Facility Being Provided by University Grants Commission through Information and Library Network

Vikas Sharma[1], Anjana Sharma[2]
[1]International Centre for Distance Education and Open Learning (ICDEOL), Himachal Pradesh University, Shimla, H.P. India
[2]Web Tech Computer Education, Sanjauli, Shimla, H.P. India
dr.vikas.hpu@gmail.com, anjana_vashisht@yahoo.com

Abstract: Universities play very important role for social and cultural development, build knowledge economy and serve as leaders of innovation for prosperity. It has become essential to have access of technology with innovative ideas to compete in this growing knowledge economy of 21st century. The technology has the potential to pave the way of innovations by creating and dissemination of knowledge. The applications of Information and Communication Technology (ICT) in higher education system have provided enough opportunities for development and dissemination of online electronic resources (e-resources). The e-resources contain e-journals, e-books, abstracts, full texts, databases, etc. and these are mostly in demand by the teachers, researchers and students at universities and colleges level. Keeping in mind the changing needs of the users, the current paper has tried to evaluate the usage of online e-resources among teachers, research scholars and students within the campus of Himachal Pradesh University, Shimla. This university is a member of UGC-INFONET (University Grants Commission- Information Network) consortium and has the facility to access online electronic resources free of cost through Information and Library Network (INFLIBNET). Results of the study indicate that e-resources are becoming popular gradually among teachers, research scholars and students but still there is a need to improve infrastructure, communication service and enhance awareness level among users for optimal utilisation

Keywords: ASC-UGC, ICT, e-resources, UGC-INFONET, INFLIBNET, Internet, World Wide Web.

1. Introduction

The emerging competition in education sector at global level is forcing the academic institutions to change their curricula accordingly and introduce new disciplines to compete at world level. This in turn has imposed a greater demand on educational institutions to put in place robust and modern communication system so that teachers, researchers and students can access the most up-to-date information especially in emerging disciplines [5]. The applications of ICT have enhanced the efficiency and capacity of the universities to provide quality education and conduct high caliber research works. Due to little or no access of electronic resources, the traditional Indian Universities are lacking behind on information production and dissemination of knowledge at world level as compared to the other private/ foreign sector universities [10]. With the exponential growth of information resources in the era of web 2.0 and e-Science, almost all kinds of online text and multimedia information are expanding rapidly. The web becomes an enormous academic-related document repository and Internet turns out to be an important platform for people participating in academic research [3]. With the growing popularity of e-resources, the traditional libraries are gradually migrating from print documents to digitisation of contents. There are several forms and types of electronic resources which are available on the Internet, some of the popular ones are the electronic journals, standards, technical specifications, reports, patents, full text articles, trade reports and hosts of other document sources [6]. With wider Internet connectivity, educational institutions have started to tap opportunities offered by today's information societies. These digital connections act as gateways where researchers and librarians can find, download and share world knowledge and learning materials [4]. So, electronic resources are becoming integral components in present academic and research works. The applications of ICT have been replacing the traditional books, journals and catalogs within the libraries with electronic resources. This is due to the continuous developments in the field of Information and Communication Technology, emerging competition at global level, changing demands of users, 24 hrs accessibility and availability of resources in an integrated way on a single platform.

2. University Grants Commission-Information Network at National Level

The Indian Universities has one of the largest higher education systems in the world with more than 431 universities and 20,677 affiliated colleges. It is a great challenge to ensure effective coordination and communication amongst 116.12 lakh students and 5.05 lakh teachers. Fast changing curricula and frequent introduction of new subjects have imposed a great demand of state-of-the-art system in place for effective management of resources and remain competitive in emerging knowledge economy [5]. A need was felt at national level to build modern network system to interconnect all academic institutions at national level as well as at global level with academic community to share knowledge resources and scholarly information in electronic format. The UGC has launched an ambitious programme to bring about a qualitative change in higher education system. Under this initiative, the UGC facilitates the universities to modernize themselves with state-of-the-art campus wide networks with nationwide communication and e-resource facility named UGC-INFONET with INFLIBNET (Information and Library network). The INFLIBNET, as an IUC (Inter-University Centre) of the UGC, acts as a coordinating agency for monitoring the network and Internet bandwidth provided to the universities. The UGC-INFONET is based on open IP (Internet Protocol) platform, TCP (Transmission Control Protocol) spoofing and other Internet tools that provide interactive education and on-line response to queries [11]. Initially, the UGC-INFONET was overlaid on ERNET (Education and Research Network) infrastructure to provide assured quality of service and optimal utilization of bandwidth resources [11]. The UGC INFONET 2.0 is upgraded network infrastructure to connect Universities by an ISP (Internet Service Provider) with 10 Mbps line. The INFONET 2.0 scheme is operated and executed by the INFLIBNET Centre. Presently, the INFLIBNET has been providing access of e-resources to 200 Indian Universities using Internet leased line network of BSNL since 1st April 2010. Normally for 10 Mbps (1:1) Internet leased line; the bandwidth has to be provided on OFC (Optical Fiber Cable) and equipments like STM1/ STM4/STM16. The UGC-INFONET mainly provides Internet bandwidth, a pre-requisite for delivery of scholarly content subscribed through the UGC-INFONET Digital Library Consortium. The Himachal Pradesh University, Shimla is also a member of UGC-INFLIBNET consortium and has been using 10 Mbps bandwidth against LL-2 Mbps since 18th March 2010 [5].

3. Review of Literature

(Fatemi,1999) observed that students using the Web were often overwhelmed by the amount of information available. Further, the more difficult part at the end of the students is to locate high quality Web-based information.

(MaKinster,2002) summarised that low yield of useful information had presented a significant challenge for students and teachers using the Web, especially when one considers the amount of time invested in searching the Web and the considerable variation in the quality and accuracy of search results.

(Larive,2004) observed that e-resources like email had made communication with all of the students in a class simple and rapid. Costs of providing students with paper copies of handout like course syllabi can be eliminated by posting the material on the web. More creative uses of electronic resources provide a true enhancement to the educational process, and a wide range of web-based content is available, including lecture notes, animations, on-line texts, simulations and virtual instruments.

(Bauer & Kenton 2005) added that although teachers were having sufficient skills, innovative and skills to easily overcome obstacles but they did not integrate technology consistently both as a teaching and learning tool.

(Kaur,2009) summarised that the advent of Information Technology had resulted in reducing the size of the libraries. In fact, these smaller modern libraries are rich potential of information. It has been possible due to the digitization of information. The digital and electronic information is based on digitized data/information, which has gradually replaced paper-based records. The visual information system in comparison to text based information system is getting more and more popular these days.

(Kumar,2009) concluded that libraries had been changing with time from mere storehouses of collection of documents to dynamic service centers. The present period is a period of digital libraries, electronic libraries and virtual libraries. The information that is available in digital form, requires new and modern methods for its handling..

4. General Objective

To evaluate the usage of online electronic resources facility being provided by the Himachal Pradesh University Summer Hill, Shimla to its teachers, research scholars and students in collaboration with UGC-INFONET consortium through INFLIBNET.

5. Specific Objectives

1. To study the trends of utilisation of online electronic resources among users.
2. To study users' perceptions pertaining to online electronic resources facility being provided to them.
3. To identify problems being faced by the users while accessing online electronic resources facility.
4. To recommend on how to improve accessibility and usage of online electronic sources.

6. Significance of Research

This research is important because of the following reasons:

1. The research leads to increased knowledge on how teachers, students and research scholars access and use online electronic information in higher education system.
2. It also exposes the bottlenecks in existing system.
3. This study also contributes to future scope of similar studies.

7. Research Design and Methodology

The research methodology of this study has been divided into four main parts, namely: 1) Scope of Study, 2) Population, 3) Sample, and 4) Research Tool.

7.1 Scope of Study

The study was conducted within the campus of Himachal Pradesh University, Summer Hill, Shimla in the months of May to July 2010. This university is a member of UGC-INFONET consortium and has the facility to access online electronic resources free of cost such as e-journals, e-books, abstracts, databases, Internet, etc. on 10 mbps line through INFLIBNET. This service is being provided to all teaching departments, cyber café and computer centres within the university campus through optical fiber network as backbone and CAT6 cable at end terminals.

7.2 Population

Population of this study includes three target users of electronic resources – teachers, research scholars and students (postgraduate & undergraduate) of different teaching departments within the university campus.

7.3 Sample

The study is based on 61 users of different categories from various teaching departments within the university campus. The above sample is collected using non-probabilistic convenient sampling technique. The characteristics of above sample are shown in table 1.

Table 1. Sample Characteristics of Users

Sr. No.	Sample Characteristic Descriptions				
1.	**Gender**	**Males**		**Females**	
	Frequency	43		18	
	(% ages)	(70.5)		(29.5)	
2.	**Age (in years)**	**18-22**	**23-27**	**28-32**	**>32**
	Frequency	8	34	7	12
	(% ages)	(13.1)	(55.7)	(11.5)	(19.7)
3.	**Education Qualification**	**Ph.D.**	**M. Phil.**	**PG**	**UG**
	Frequency	13	18	21	9
	(% ages)	(21.3)	(29.5)	(34.4)	(14.8)
4.	**Designation**	**Teachers**	**Research Scholars**		**Students**
	Frequency	12	19		30
	(% ages)	(19.7)	(31.1)		(49.2)
5.	**Computer Handling Knowledge**	**Yes**			**No**
	Frequency	59			2
	(% ages)	(96.7)			(3.3)
6.	**Web Browsing Knowledge**	**Yes**			**No**
	Frequency	48			13
	(% ages)	(78.7)			(21.3)

The above table shows that majority of users in the sample i.e. 96.7 percent have computer handling knowledge, 78.7 percent users have web surfing knowledge, 70.5 percent users are male, 55.7 percent users are in the age group of 23-27 years, 49.2 percent users are students and 34.4 percent users are doing post graduation degree/diploma courses.

7.4 Research Tool

The data collection tool used here was self designed questionnaire containing different items pertaining to usage of online electronic resources such as Internet, e-journals, abstracts, full text, etc. The items of the questionnaires were selected from intensive review of literature which revealed similar studies conduced on usage of electronic resources. The questionnaire had both open ended and close ended questions to study the accessibility, usability and problems being faced by users. A 5-point Likert Scale was used to observe the satisfaction level and to rate the importance of information available through e-resources. The collected data was organised, classified, coded and analyzed. The Statistical Package for Social Sciences (SPSS) Ver. 10 and Microsoft Excel 2007 were used for analyzing the quantitative data collected through questionnaires.

8. Results and Discussion

In this section, the results of the study are presented. To answer the issues raised in the form of objectives, the findings of the study have been divided into three subsections.

8.1 Electronic Resources Utilisation Trends

The online electronic resources in the form of e-journals, databases, e-books, abstracts and Internet service have been used by three categories of users namely- teachers, students and research scholars. Amongst above electronic resources, the Internet has emerged as fast growing channel not only for communication purpose but also to acquire information from World Wide Web. Internet is being used for various purposes in which 72.1 percent users had been using it for communication purpose such as emails/chatting followed by 60.7 percent users who used it for research works, 37.8 percent users who used it to acquire information from web, 24.7 percent users who used it for career development, 9.9 percent users who used it for entertainment and 1.6 percent users who used it for other purposes. This indicates that majority of users had been using Internet for communication purpose followed by research works. Among users category-wise utilisation of Internet, it was observed that teachers were the top users to utilize it for research works,

communication, career development and entertainment purposes while the students looked more curious to acquire information from web. Table 2 shows the utilisation of Internet Service.

Table 2. Utilisation of Internet Service
(Users' category-wise number and % ages)

Sr. No.	Internet Service	Users Category			
		Research Scholars	Students	Teachers	Total (in % ages)
1.	eMails	15 (78.9)	19 (63.3)	10 (83.3)	44 (72.1)
2.	Finding Informatio	3 (15.80)	14 (46.70)	6 (50.00)	23 (37.8)
3.	Career Developmer	2 (10.50)	7 (23.30)	6 (50.00)	15 (24.7)
4.	Entertainment	2 (10.50)	2 (6.70)	2 (16.70)	6 (9.9)
5.	Research Works	15 (78.90)	10 (33.30)	12 (100.00)	37 (60.7)
6.	Others	1 (5.30)	0 (0.00)	0 (0.00)	1 (1.6)

The Internet has emerged as an integral component in our education system. This view is supported with the fact that 88.5 percent users had been using this facility at least once in a week in which 47.5 percent users used this facility daily followed by 23.0 percent users who used it 2 to 3 times in a week and 18.1 percent users who used it once in a week. Further 83.3 percent teacher had been using Internet daily followed by 40.0 percent students and 36.80 percent research scholars. Table 3 shows the Internet usage frequency.

Table 3. Internet Usage Frequency
(Users' category-wise number and % ages)

Sr No	Internet Usage Frequency	Users category			
		Research Scholars	Students	Teachers	Total (in % ages)
1.	Daily	7 (36.80)	12 (40.00)	10 (83.30)	29 (47.5)
2.	2 to 3 times in a Week	5 (26.30)	9 (30.00)	0 (0.00)	14 (23.0)
3.	Once in a Week	4 (21.10)	5 (16.70)	2 (16.70)	11 (18.1)
4.	Occasionally	3 (5.30)	4 (13.30)	0 (0.00)	7 (11.5)

The Internet is a major source of information and this information can be used in two ways- printed or electronic/digital form. It was observed that 90.2 percent users preferred printed as well as electronic form of information whereas 9.90 percent users preferred only electronic form. This indicates that electronic form of information is making its place gradually in university education system but majority of users prefered both printed and electronic form of information. All research scholars had top preference for printed as well as digital (electronic) form of information followed by 93.30 percent students and 66.70 percent teachers. This may be due to because paper based information is convenient to read, study and analyse whereas electronic form of information (content, references, diagrams, figures, etc.) is easier to incorporate in research works without much efforts in the form of retyping or redrawing of figures, tables ,etc. Further 33.30 percent teachers preferred electronic form of information to acquire information followed by 6.70 percent students. This means that electronic form of information is gradually replacing our physical paper system. Figure 1 shows the formats preferred by the users to acquire information from World Wide Web.

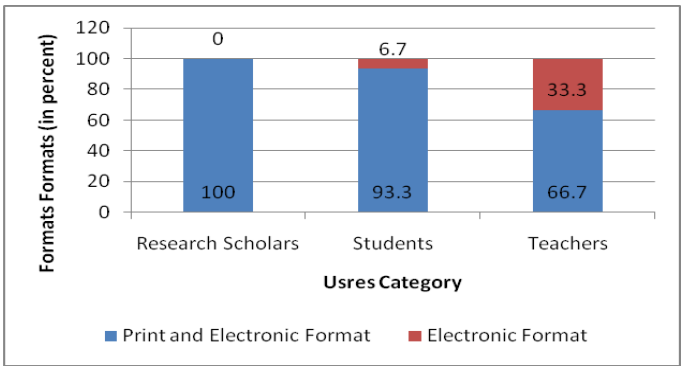


Figure 1. Formats Preferred by the Users to Acquire Information from World Wide Web (in % ages)

The UGC-INFONET consortium has been providing free online electronic resources facility through INFLIBNET. It was observed that 60.7 users had been consulting the electronic resources available through INFLIBNET for their research works followed by 44.3 percent users who used it for classroom notes preparation, 31.2 percent users who used it for project completion, 23.0 percent users who used it for consultation of online books, 18.1 percent users who used it for academic purpose, 18.0 percent users who used it for seminar preparation, 16.4 percent users who used it for paper writing and 4.9 percent users who used it for other purposes. The table 4 shows the utilisation of online electronic resources.

Table 4. Utilisation of Electronic Resources
(Users' category-wise number and % ages)

Sr No	Utilisation of Online Electronic Resources	Users category			
		Research Scholars	Students	Teachers	Total (in % ages)
1.	Paper Writing	0 (0.00)	0 (0.00)	10 (83.30)	10 (16.4)
2.	Online Books	0 (0.00)	4 (13.30)	10 (83.3)	14 (23.0)
3.	Project Completion	3 (15.80)	6 (20.0)	10 (83.30)	19 (31.2)
4.	Notes Prep-ration	7 (36.80)	14 (46.7)	6 (50.00)	27 (44.3)
5.	Academic Purpose	0 (0.00)	5 (16.70)	6 (50.00)	11 (18.1)
6.	Research Work	11 (57.90)	16 (53.30)	10 (83.30)	37 (60.7)
7.	Seminar Preparation	0 (0.00)	1 (3.30)	10 (83.30)	11 (18.0)
8.	Other Purposes	0 (0.0)	1 (3.3)	2 (16.7)	3 (4.9)

This indicates that main utilisation of this facility is for research works followed by classroom notes preparation. Each 83.30 percent teachers had been using this facility for paper writing, research works, seminar preparation, projection completion, e-books consultation, etc. Majority of users, 57.90 percent research scholars and 53.30 percent students had been using this facility for research works but 50.0 percent teachers and 46.7 percent students used it for class room notes preparation. This indicates that students are also showing their interest in research works. The academic and research information available through electronic resources can be downloaded, printed, read, etc. The Figure 2 shows the preferred modes of utilisation of information available through online electronic resources.

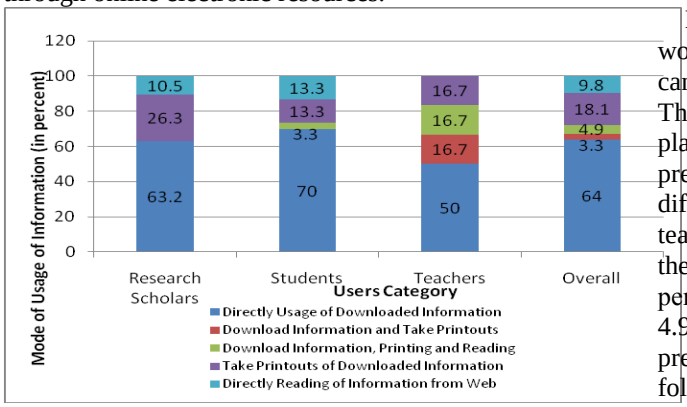


Figure 2. Preferred Modes of Usage of Information Available through Online Electronic Resources (in % ages)

It was observed that 64.0 percent users preferred to download information followed by 18.1 percent users who preferred to take printouts and 9.8 percent users who preferred to read information. Further, 70.0 percent students preferred to download information followed by 63.20 percent research scholars and 50.0 percent teachers. 26.30 percent research scholars preferred to take printouts of downloaded information followed by 16.70 percent teachers and 13.30 percent students. Similarly 13.30 percent students preferred to read information followed by 10.50 percent research scholars. This indicates that users are shifting towards digital form of information. There are also variations in consultation of online electronic resources at the end of the users. It was observed that majority of users 68.8 percent had been using electronic resources facility at least once in a week in which 24.7 percent users used it daily whereas 27.9 percent users who used it 2 to 3 times in a week and 16.4 percent users who used it once in a week. This indicates that frequency of using of online electronic resources is higher among users. Further, majority of teachers, 66.70 percent were the regular users to consult electronic resources followed by 15.80 percent research scholars and 13.30 percent students. The students were observed as casual users to utilise electronic resources. Figure 3 shows the frequency of utilisation of electronic resources.

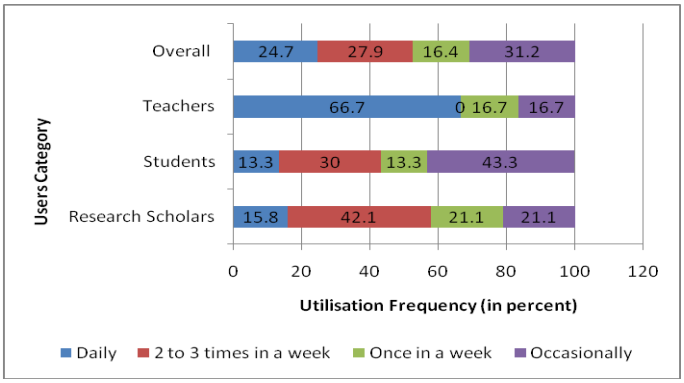


Figure 3. Frequency of Utilisation of Online Electronic Resources (in % ages)

In this era of Information Technology, the whole world has become a virtual village where information can be accessed 24 hrs in a day and from any location. The Internet can be accessed from cyber cafés, working places/ departments or homes. The Figure 4 shows the preferred places for utilisation of Internet Service by different categories of users. It was observed that teaching departments within the university campus were the first choice of 75.4 percent users followed by 19.7 percent users who preferred university's cyber café and 4.9 percent users who preferred their homes. All teachers preferred their departments for utilisation of Internet followed by 73.3 percent students and 63.2 percent research scholars. World Wide Web is a vast sea of knowledge from where information can be extracted using different sources such as electronic journals, electronic books, databases, general websites, emails, chatting, etc. Usage of general websites had remained the first choice to acquire information for 91.8 percent users followed by emails of 21.3 percent users, e-books of 16.4 percent users, current issues of journals of 14.8 percent users, back issues of journals of 6.6 percent users and databases of 4.9 percent users. This indicates that general websites are the major source of acquiring information followed by communication through emails and consultation of electronic journals. But, the consultation of general website raises some crucial issues related to authenticity & credibility of source in addition to quality of information, so contents should be chosen very carefully. Table 5 shows the preferred sources of acquiring information and their utilisation trend.

Table 5. Preferred Sources of Acquiring Information (Users' category-wise number and %ages)

Sr. No.	Preferred Sources of Acquiring Information	Users Category			
		Research Scholars	**Students**	**Teachers**	**Total (in %ages)**
1.	Current Journals	1 (5.30)	2 (6.70)	6 (50.00)	9 (14.8)
2.	Back Journals	0 (0.00)	0 (0.00)	4 (33.30)	4 (6.6)
3.	Databases	3 (15.8)	0 (0.00)	0 (0.00)	3 (4.9)
4.	e-books	0 (0.00)	8 (26.70)	2 (16.70)	10 (16.4)

5.	Internet Websites	17 (89.50)	27 (90.00)	12 (100.00)	56 (91.8)
6.	eMails	0 (0.00)	3 (10.00)	10 (83.30)	13 (21.3)

The findings of the above discussion indicate that e-resources are being accepted in university education system for research works, finding information, communication, etc. The electronic form of information is also gradually replacing physical paper system.

8.2 Users' Perceptions Pertaining to Electronic Resources Facility

Computer has become an integral component in our teaching and learning process. In Himachal Pradesh University, some teaching departments have their own computer labs to facilitate their students and teachers. An attempt was made to analyse the satisfaction level of the students, teachers and research scholars corresponding to available computing facility in their respective departments. It was observed that 41.0 percent users were satisfied whereas 21.3 percent users were unsatisfied with the available computing facility. The table 6 shows the satisfaction level of the users w.r.t. available computing facility in teaching departments.

Table 6. Satisfaction Level of the Users w.r.t. Available Computing Facility in Teaching Departments (Users' category-wise number and %ages)

Sr. No.	Satisfaction Type	Users Category			
		Research Scholars	Students	Teachers	Total (in % ages)
1.	Highly Dissatisfied	2 (10.5)	1 (3.3)	0 (0.0)	3 (4.9)
2.	Dissatisfied	3 (15.8)	5 (16.7)	2 (16.7)	10 (16.4)
3.	Neutral	3 (15.8)	16 (53.3)	4 (33.3)	23 (37.7)
4.	Satisfied	11 (57.9)	8 (26.7)	6 (50.0)	25 (41.0)
5.	Highly Satisfied	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)

In Himachal Pradesh University, all teaching departments who have computer labs also have Internet facility. It was observed that majority of users 41.0 percent were unsatisfied with the available Internet facility in their departments. Amongst above dissatisfied users, 57.9 percent users were research scholars followed by 40.0 percent students and 16.7 percent teachers. This may be due to slow speed of Internet, non availability and non functionality of computer systems in labs. Table 7 shows the satisfaction level of the users w.r.t. available Internet Facility in teaching departments.

Table 7. Satisfaction Level of the Users w.r.t. Available Internet Facility in Teaching Departments (Users' category-wise number and %ages)

Sr. No.	Satisfaction Type	Users Category			
		Research Scholars	Students	Teachers	Total (in % ages)
1.	Highly Dissatisfied	0 (0.0)	2 (6.7)	0 (0.0)	2 (3.3)
2.	Dissatisfied	11 (57.9)	10 (33.3)	2 (16.7)	23 (37.7)
3.	Neutral	2 (10.5)	11 (36.7)	0 (0.0)	13 (21.3)
4.	Satisfied	6 (31.6)	7 (23.3)	8 (6.7)	21 (34.4)
5.	Highly Satisfied	0 (0.0)	0 (0.0)	2 (16.7)	2 (3.3)

Through UGC-INFONET Consortium, the Himachal Pradesh University has the facility to provide accessibility of international level journals free of cost to its teachers, research scholars and students. The Figure 4 shows the perception of users regarding content quality of electronic journals. It was observed that majority of users 77.1 percent rated electronic journals of good quality and this further included all teachers followed by 94.7 percent research scholars and 56.7 percent students.

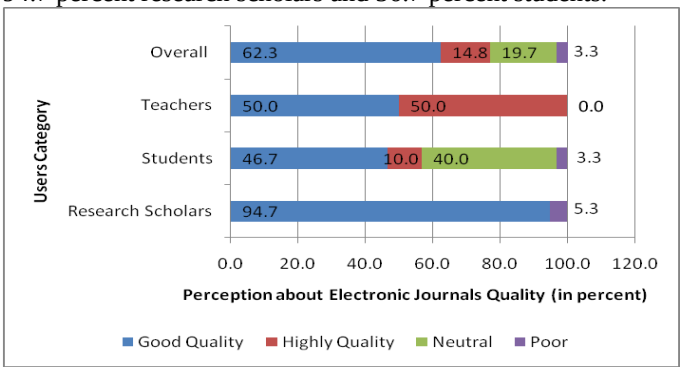


Figure 4. Perception of Users about Content Quality of Electronic Journals (in % ages)

Internet has emerged as one of the essential service to acquire information through World Wide Web. It was observed that 90.1 percent users had opinion that knowledge of Internet basics is essential to acquire information. This view was further supported by all teachers and research scholars but 16.7 percent students considered it highly irrelevant. Figure 5 shows the perception of the users regarding knowledge of Internet basics for acquiring information from World Wide Web.

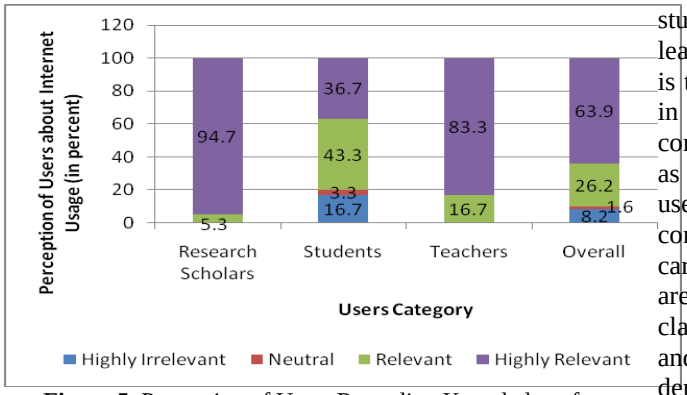


Figure 5. Perception of Users Regarding Knowledge of Internet basics (in % ages)

8.3 Problems Being Faced while Accessing Online Electronic Resources

No system is hundred percent perfect. Similarly online electronic resources facility being provided by Himachal Pradesh University using UGC-INFONET through INFLIBNET consortium has also some problems. The Figure 6 shows the problems being faced by users.

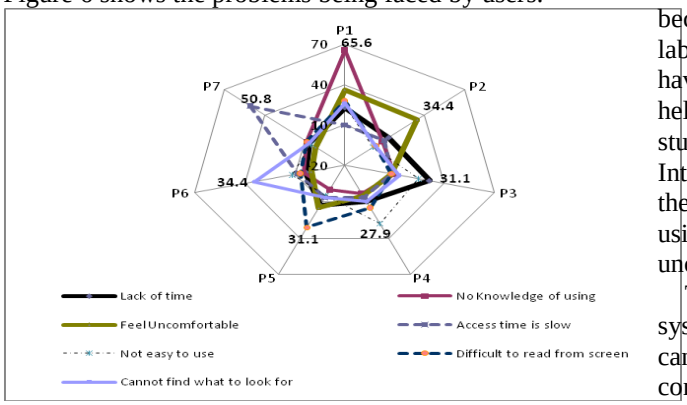


Figure 6. Priorities Assigned to Problems Being Faced by the Users

In descending order of problems being faced by users, 65.6 percent users rated lack of online e-resources usage knowledge (P1) on the top of the list of problems being faced followed by slow speed Internet Connection (P7) by 50.8 percent users, difficult to get necessary information (P2) and feeling of uncomfortable (P6) each by 34.4 percent users, difficult to use or read information from computer screen (P3) and lack of time (P5) each by 31.1 percent users, and inconvenient to use electronic resources-non user-friendly interface (P4) by 27.9 percent users. This indicates that lack of awareness, slow speed of Internet, difficulty to find required information, uncomfortable and non user-friendly interface have been disappointing users to avail online electronic resources facility being provided by this university.

9. Conclusion

The applications of Information and Communication Technology (ICT) in higher education system especially at university level have paved the way for teachers, students and research scholars to improve their teaching, learning and research works. The main objective of UGC is to provide high quality teaching and research material in the form of e-resources so that our universities can compete at global level. The Internet service has emerged as one of the most popular facilities and this is being used by the teachers, research scholars and students for communication, research works, finding information and career development. Similarly the electronic resources are also being used to do research works, prepare classroom notes, seminar presentations, communication and project completion purposes. The teaching departments emerged as most preferred places to avail e-resource facility followed by university's cyber café. Further, the electronic form of information is replacing the physical papers gradually. This indicates that e-resource facility is gradually making its place in our university education system where majority of users are availing it at least once in a week.

But there are also some users who are not aware about the free availability of e-resources. In addition to above, few users are still deprived of online e-resources facility because of their departments do not have the computer labs as well as Internet facility. A few departments who have computer labs and Internet facility are not looking helpful to satisfy the emerging requirements of their students, teachers and research scholars. The slow speed Internet connection is the major problem being faced by the users followed by difficulty to extract information using web, inconvenient to read information, uncomfortable to use online e-resources, etc.

This indicates that there is a need to improve existing system for optimal utilisation of online e-resources. This can be done by following ways: 1) improve communication and computing infrastructure in all teaching departments to avoid users' rush towards university's cyber café, 2) proper maintenance of computer systems installed in university's cyber café, 3) improve existing bandwidth of Internet connectivity (10 mbps to at least 1 gbps) for fast accessibility and transfer of information, 4) enhance awareness level among users by organizing seminars and workshops, 5) provide proper training to users for optimal utilisation of e-resources, 6) design and implementation of online e-resource accessibility policies for different categories of users keeping in view their needs and expertise, 7) provision to extent the existing facility of online e-resource beyond university campus such as in the students' hostels and homes of the authorized and authenticated teachers, research scholars, etc. 8) deployment of special trained staff in the university library/cyber café for the assistance of the users to find necessary information from electronic journals, database, abstracts, etc. 9) deployment of technically sound and secure network management solutions to avoid any misuse of bandwidth & e-resources, data thefts, data hacking, etc. 10) development of data storage centre for frequently demanded research papers, articles, abstracts,

databases, ebooks, etc. and their storage in archival form to avoid unnecessary data traffic on the network and fast accessibility of information to the needy users.

References

[1] Bauer, J. and Kenton, J. "Toward Technology Integration in the Schools: Why it isn't Happening." *Journal of Technology and Teacher Education*. 13.4 (2005):519-546.

[2] Fatemi, E. (1999). Building the digital curriculum. *Education Week Magazine*. 19(1999): 5–8.

[3] Gray, K., Thompson, C., Clerehan, R., et al. Web 2.0 authorship: Issues of Referencing and Citation for Academic Integrity. *The Internet and Higher Education*, 11(2008):112–118.

[4] INASP. "Optimising Internet Bandwidth in Developing Country Higher Education." International Network for the Availability of Scientific Publications. A Study Presented at the Regional Training Conference on Improving Tertiary Education in Sub-Saharan Africa: Things That Work! Accra. September 23-25, 2003.

[5] INFLIBNET. "UGC-INFONET Connectivity Programme." (2010). [Online]. Available: http://www.inflibnet.ac.in/infonet/aboutus.php (accessed on June 10, 2010).

[6] Kaur, Baljinder. "Use and Impact of Electronic Resources in Engineering and Technological Institutions in India." Ph.D. diss., Thaper University Patiala, 2009.

[7] Kumar, Arun. "Use and Usage of Electronic Resources in Business Schools in India: FIIB." (2009). [Online]. Available: http://crl.du.ac.in/ical09/papers/index_files/ical-96_173_706_1_PB.pdf (accessed on April 3, 2010).

[8] Larive, Cynthia K. (2004). "Digital resources to enhance instruction." *ABCs of Teaching Analytical Science, Anal Bioanal Chem*. 379 92004):321–322.

[9] MaKinster, James G. , Ronald A. Beghetto, and Jonathan A. Plucker. (2002). "Why Can't I Find Newton's Third Law? Case Studies of Students' Use of the Web as a Science Resource." *Journal of Science Education and Technology*. 11. 2. (2002).

[10] Ocampo, Saturnino M. "ICT in Philippine Higher Education and Training." 15th SEAMEO-RIHED Governing Board Meeting and back-to-back Seminar on ICT in University Teaching/Learning and Research in Southeast Asian Countries held at the Millennium Sirih Hotel; Jakarta, Indonesia. August 23-24, 2007

[11] UGC. "UGC INFONET." (2008). [Online]. Available: http://www.ugc.ac.in/new_initiatives/infonet.html (accessed on June 2, 2010).

Authors

Vikas Sharma received his MCA and Doctoral degrees in 1998 and 2008 respectively from Himachal Pradesh University, Summer Hill, Shimla, India. Currently he is serving as Senior Programmer in International Centre for Distance Education and Open Learning (ICDEOL), Himachal Pradesh University, Summer Hill, Shimla.

Anajan Sharma received her MCA degree from Maharishi Dyanand University, Rohtak, Haryana in the year 2007 and presently serving as senior faculty in Web Tech Computer Education, Sanjauli, Shimla, H.P. India.

Analyzing the Security System Applied to E-Shopping Using Elliptic Curve Cryptography

Sougata Khatua[1] and N.Ch.S.N Iyengar[2]

School of Computing Science and Engineering, VIT University,
Vellore-632014, Tamil Nadu, INDIA
sougatakhatua@yahoo.com[1], nchsniyengar48@gmail.com[2]

Abstract**:** *Current E-shopping systems use the Internet as its primary medium for transactions. Internet being heterogeneous, non secure medium, privacy, authenticity, integrity, and non-repudiation are the key requirements to be addressed by such systems where face to face interaction is not possible. Most of the systems do not provide the required level of security service such that many problems exist in the systems like denying, losing, misusing, stealing and double-spending etc. This project address all the above said security service problems to an E-shopping system using Elliptic Curve Cryptosystem (ECC).*

Keywords**:** *Encryption process, Decryption process, digital signature, confidentiality, integrity, non-repudiation, authentication, e-shopping***.**

1. Introduction

The e-shopping is defined as the use of computers and electronic networks to organize shopping with customers over the internet or any other electronic network.

Online shopping has grown in popularity over the years, mainly because people find it convenient and easy to buy various items comfortably from their office or home. One of the most advantages of online shopping, particularly during a holiday season, is that it eliminates the need to wait in long lines or search from store to store for a particular item.

The unpredictable growth of the Internet users in world opened a new business opportunity to the whole world. Shopping activities over the internet have been growing in an exponential manner over the last few years. Security is often sited as a major barrier to further development of e-shopping on the open Internet, such as clients' information divulging, credit card embezzling, and so on. These problems warn people in E-shopping and make them reluctant to pay on Internet. Therefore, the most important topic is how to establish a secure and well-suited applied condition to provide adequate protection to the related transaction information for each entity in an E-shopping transaction.

1.1. Security Features:

The main concept of security of the e-shopping is defined below:

Confidentiality: The shopping information in the transaction all demand for secrecy. For instance, all the things such as, credit number, total amount of shopping and the user name & password can't be known about by anybody else. Therefore, it is generally required to be encrypted in the process of information dissemination.

Integrity: It is classified into the following categories [2]:
i) Integrity of Transaction: when the money is sent from customer to the supplier the integrity of the transaction must be maintained i.e. debit and credit of amount must not changed. Failure to this will lead to an inconsistence state which is highly undesirable.
ii) Delivery of Product: The customer must receive the product in good condition. It is undesirable that customer pay the money without receiving the product.

Authentication: It ensures that the people using the computer are the authorized users of that system before transacting.

Non-Repudiation [3]: It ensures that neither the customer nor the supplier can deny communication or other action regarding information or resources at a specific time.
i) Non-repudiation of origin: The ability to identify who sent the information originally versus which intermediary forwarded it.
ii) Non-repudiation of receipt: The ability to identify that the information was received by the final addressed destination in a manner that cannot be repudiated.
iii) Non-repudiation of delivery: The ability to identify whether the information was delivered to an appropriate intermediary in a manner if cannot repudiate.

Availability: It ensures that end system (host) and data should be available when needed by the authorized user.

Accountability: The identities of all users are assured and are made responsible for their action [12].

Copy protection: This feature ensures protection from unauthorized copying of intellectual information [9].

1.2. Background:

The security of the e-shopping system is based on the following components of the cryptography:

Public key cryptosystem (PKC): i.e. for encryption and decryption of the confidential information such as credit card/debit card number. Both *Secure Socket Layer (SSL)* and *Public Key Infrastructure (PKI)* is based on PKC.

Digital signature: which is used to provide integrity of the information like payment amount, authenticity of the user and availability of the information to the authenticated user.

Password based authentication: It is used to check the user identity. It is the simplest and oldest method of entity authentication.

2. Literature Review:

2.1. Previous works:

Whether we consider final or partial transformation of shopping into an electronic one as e-shopping; in both cases concerns about security is increasing dramatically [9]. Though a great technical development have been experienced, security incidents continue to occur.

To provide the security in several sectors of e-commerce including e-shopping, several research work has been done. For securing the farm products in china a *PKI* based technology has been proposed [7]. In this paper *RSA* cryptosystem is used for encryption and *RSA* digital signature algorithm and *SHA1* has been used for providing authentication, integrity and the identity of the user. The *RSA* public key algorithm with 1024 digit widely applied in the current markets at all. But it is too tricky to use the key of 1024 digit and it is relatively slow for this large key size. However, the *RSA* itself is vulnerable [5]. Some *e-commerce* applications (including *e-shopping*) use *Elgamal* cryptosystem. But it also suffers from large key size (1024 bits) to achieve the required level security. In another research paper [2] , *PKI* technology is proposed for security in *e-commerce*. *SSL* [3] is used in many e-commerce applications but it also suffers from the problem of large key size because *SSL* depends on *RSA* encryption for exchange of the session key and client/server authentication. Biometric techniques [8] has also been proposed. But it is difficult to use and costly also. So use of biometric techniques for security is not economically feasible. A research work has suggested to use XML encryption [1] with the certain technologies for better security. But the drawback of this technique is that only XML files can be used. Many companies like IBM, Microsoft, Netscape RSA, Terisa and Verisign has developed the Secure Electronic Transaction (SET) to protect credit card transaction. But the disadvantage of the SET [4] is as follows:

- SET transactions are carried out between customer and merchant. It is vulnerable to attacks like transaction/balance modifications.

2.2. Proposed work:

To overcome the drawbacks of the existing e-shopping system which mostly uses *RSA* and *Elgamal* cryptosystem for providing security, in this project we emphasize on the *Elliptic Curve Cryptosystem* (ECC) as an alternative to *RSA* and *Elgamal* cryptosystem. ECC was first proposed by Miller (1986) and Koblitz (1987), and its security was based upon the difficulty of elliptic curve discrete logarithm problem (ECDLP).

Why ECC:

1. Faster than any other public key cryptosystem.
2. Low power consumption.
3. Low memory usage.
4. Low CPU utilization.
5. Less data traffic.
6. ECDLP is more harder than both integer factorization problem and discrete logarithm problem modulo p [11].
7. Less key size (160 bit) needed compared to *RSA* and *Elgamal*(both needs 1024 bit key) to achieve the required level of security.

Encrypted password: For password based *authentication*, we emphasize to use *encrypted password* using ECC to make almost impossible for the attacker to guess the password.

Besides these, a new key pair (private key and public key) is generated every the system is run. That means a new key pair is generated for each session to make almost impossible to do any type of forgery.

3. Design Analysis:

The design of the e-shopping system is divided into two parts:

Architectural diagram: It describes the overall design of the system how it works and what are the functional components and what is their functionality.

Sequence flow diagram: It shows how the how the components of the e-shopping communicate with each other the messages with respect to time.

3.1. Architectural diagram:

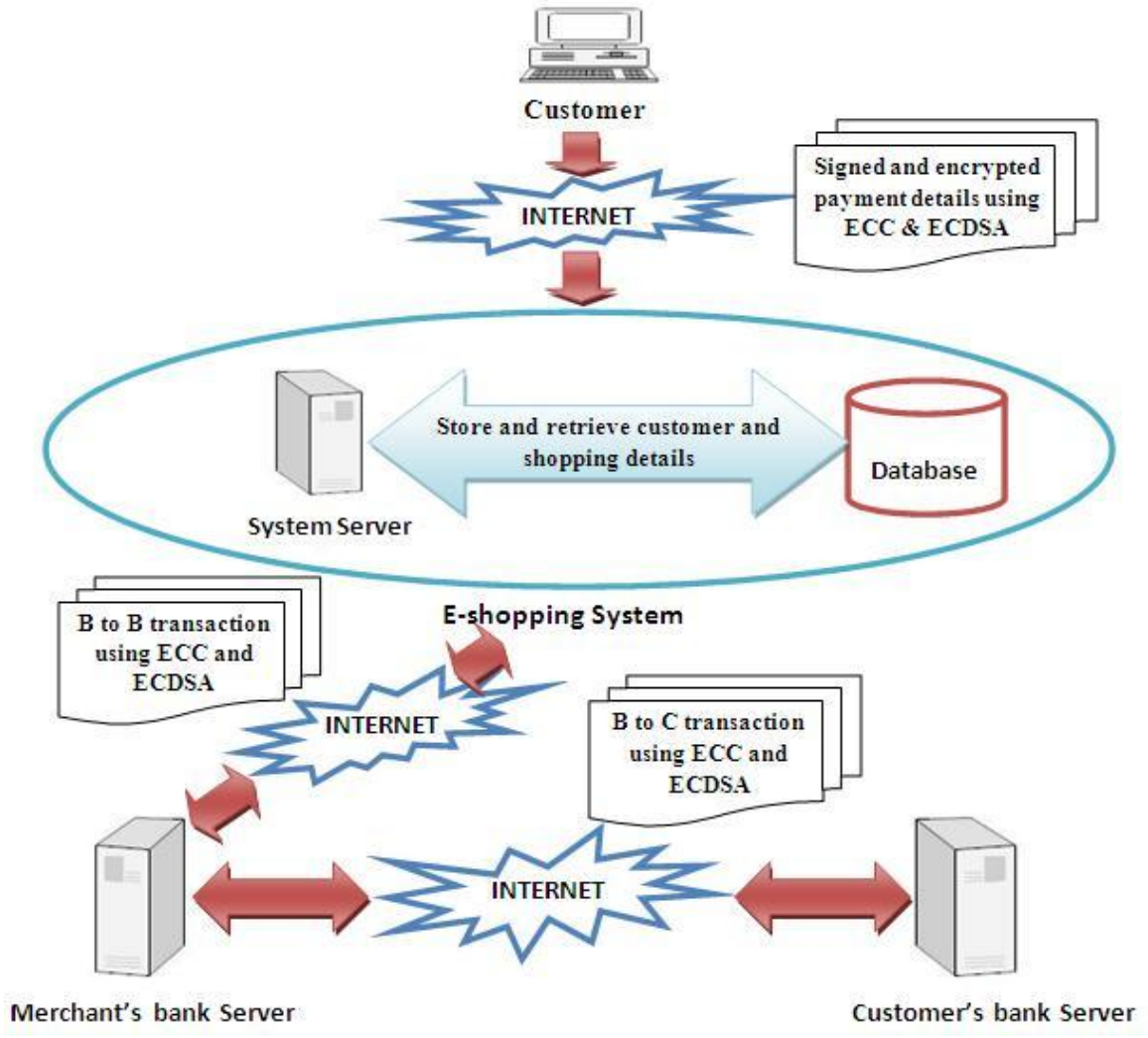


Figure 1. Architectural Diagram

3.1.1. Functional Components and their functionalities:

Customer side Terminal: The customer who wants to buy items from the e-shopping system, is authenticated by the e-shopping system. After that, he browses items in the various shops and put the selected items in the shopping cart. Then the customer enters his credit card number which is encrypted with ECC to achieve confidentiality and the total amount of shopping and the delivery address is signed with ECDSA to achieve integrity, authentication and non repudiation. Then this data is sent to the E-shopping system.

E-shopping System: After receiving the encrypted and signed data from the customer side terminal, it keeps only the signed delivery address and passes the encrypted data i.e. credit card number and the encrypted and signed amount to the merchant bank.

Merchant bank: The bank which has a business relationship with the e-shopping system receives the encrypted and signed data from the e-shopping system. This type of transaction is called as business to business transaction. The merchant bank first checks, if the customer is the user of this bank or not. If the customer is a user of this bank, then credit card number is decrypted and amount is also decrypted and verified. If the amount is not changed, then it transfers the money from customer's account to the e-shopping system's account. If the customer is not a user of this bank, then the data sent by the e-shopping is sent to the customer's bank.

Customer's bank: It receives the encrypted and signed data from the merchant bank. This type of transaction is called as business to consumer transaction. The merchant bank first checks, if the customer is the user of this bank or not. If the customer is a user of this bank, then credit card number is decrypted and amount is also decrypted and verified. . If the amount is not changed, then it transfers the money from customer's account to the merchant bank and the money is credited to the e-shopping system's account.

After that the merchant bank sends an approval message to the e-shopping system and then the e-shopping system verifies the delivery address and then sends a confirmation to the customer.

The confirmation message is in the form of a number which is called as "order number". The order number is unique for each shopping. This number is generated only after the successfully completion of the transaction.

3.2. Sequence flow diagram:

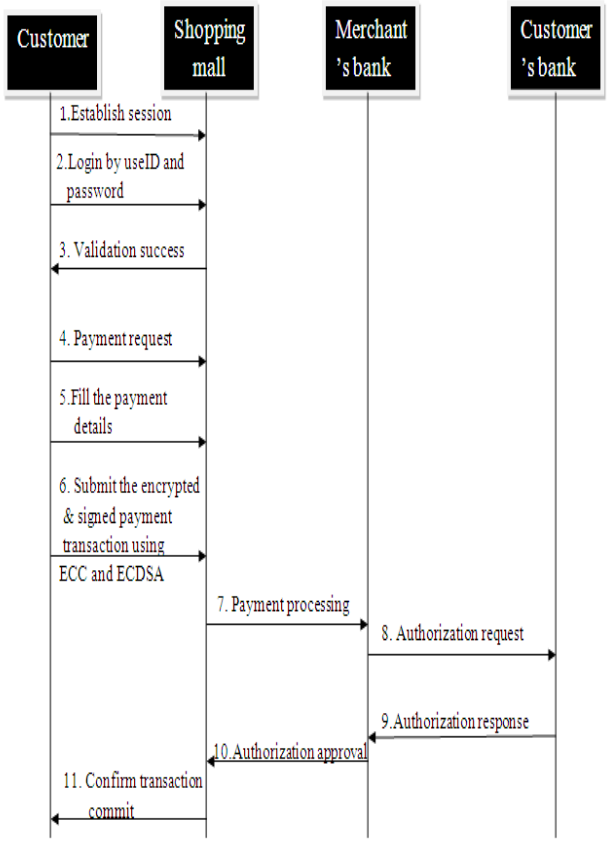


Figure 2. Information Flows for Transactions with a ECC and a ECDSA

As illustrated in Figure 2, following are the steps:

1. At first the session will be established between the customer and the shopping mall by setting the session attribute.
2. After that user submit his userID and password to the shopping mall system.
3. The e-shopping system returns validation success to the customer if the customer is an authenticated user of the e-shopping system.
4. Then customer make payment request to the e-shopping system.
5. At this stage, the customer fills the payment details.
6. The payment transaction details are encrypted and signed with ECC and ECDSA respectively and submitted to the e-shopping system.
7. After getting the customer's details, the shopping system (merchant) it contacts to the merchant's bank for customer authorization and payment.
8. Merchant's bank will contact to the customer's bank and send authorization request.
9. If the customer is authorized, then customer's bank will send authorization response to the merchant's bank.
10. Merchant's bank i.e. the e-shopping system's bank will send authorization approval to the e-shopping system.
11. After getting approval from its bank, the e-shopping system sends the transaction confirmation message to the customer.

4. Elliptic Curve Cryptosystem:

The general equation for the elliptic curve is $y^2=x^3+ax+b \ mod\ p$,p is a natural prime number, and the value of a, b should satisfy the discriminate $D=4a^3+27b^2\neq 0 \ mod\ p$ be used as the decrypting elliptic curve.

4.1. Pseudo code for finding points on an elliptic curve over GF(p):

```
Elliptic Curve points (p, a, b)          //p is the modulas
{
 x←0
 While(x<p)
  {
    w←(x^3+ax+b)mod p
    if(w is a perfect square in Zp)
        output(x, √w) , (x , -√w)
    x←x+1
  }
}
```

4.2. Elliptic Curve Integrated Encryption Standard (ECIES):

4.2.1. Key generation process:

The key generation process uses the ECC algorithm to create the public and private keys for encryption and decryption, respectively. A new key pair(public key and private key) is generated when the program is executed. The outputs of this component are the public and private keys. The steps required to generate each key are as follows:

1. Bob chooses a point E(a, b) with an elliptic curve over GF(p).
2. Bob chooses a point on the curve, $e_1(x_1,y_1)$.
3. Bob chooses a random integer d.
4. Bob calculates $e_2(x_2,y_2)=d \times e_1(x_1,y_1)$. Here the multiplication means multiple additions of points.
5. Bob announces E(a, b), $e_1(x_1,y_1)$ and $e2(x_2,y_2)$as his public key. He keeps d as his private key.

4.2.2. Encryption process:

The Elliptic Curve Integrated Encryption Scheme (ECIES) is used for this process. It then validates and encrypts the input message. The inputs include the public key encryption and the data items identified as user input in the system specifications. The encryption process involves the following activities:

1. Alice receives the public key from Bob.
2. Alice selects a random integer k.
3. Alice encrypts the message m to the cipher text by calculating C=($k \times e_1$, ($k \times e_2$) + m)
4. Alice sends cipher text C to Bob.

4.2.3. Decryption process:

The Elliptic Curve Integrated Encryption Scheme (ECIES) is used for this process. The input is the cipher text and the private key produced by the key generator and encryption processes, respectively. The decryption process involves the following activities:

1. Bob receives the cipher text C from Alice.
2. Bob then decrypts the cipher text by calculating:
   $m + (k \times e_2) - d \times k \times e_1 = m + (k \times d \times e_1) - (d \times k \times e_1) = m$.

4.3. Elliptic Curve Digital Signature (ECDSA):

Alice sends the message and the signature to the Bob. This signature can be verified only by using the public key of Alice. Since the Bob knows Alice's public key, it can verify whether the message is indeed send by Alice or not.

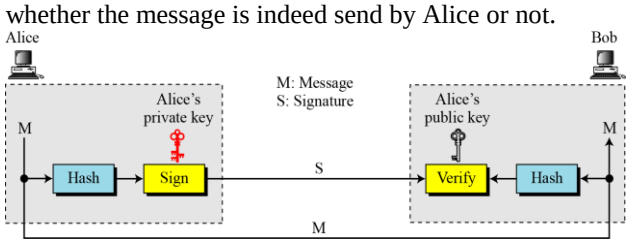


Figure 3. Signing the digest [6]

ECDSA is a variant of the Digital Signature Algorithm (DSA) that operates on elliptic curve groups. Sender 'A' have a key pair consisting of a private key d (a randomly selected integer less than n, where n is the order of the curve, an elliptic curve domain parameter) and a public key $e_2(x_2, y_2) = d \times e_1(x_1, y_1)$ (e_1 is the generator point/base point, an elliptic curve domain parameter). An overview of ECDSA process is defined below.

4. 3.1. Signature Generation:

For signing a message m by sender Alice, using Alice's private key d

1. Calculate e = HASH (m), where HASH is a cryptographic hash function, such as SHA-256
2. Select a random integer k from [1,n − 1]
3. Calculate $r = x_2 \pmod n$, where $(x_2, y_2) = k \times e_1$. If r = 0, go to step 2
4. Calculate $s = k^{-1}(e + d \times r) \pmod n$. If s = 0, go to step 2
5. The signature is the pair (r, s)

4.3.2. Signature Verification:

For B to authenticate Alice's signature, Bob must have Alice's public key e_2

1. Verify that r and s are integers in [1,n − 1]. If not, the signature is invalid
2. Calculate e = HASH (m), where HASH is the same function used in the signature generation
3. Calculate $w = s^{-1} \pmod n$
4. Calculate $u_1 = e \times w \pmod n$ and $u_2 = r \times w \pmod n$
5. Calculate $(x_2, y_2) = u_1 \times e_1 + u_2 \times e_2$
6. The signature is valid if $x_2 = r \pmod n$, invalid otherwise

5. Implementation:

To implement the Elliptic Curve Cryptography for providing the security for e-payment in the e-shopping system, the java cryptographic package and a third party security provider (Bouncy Castle)[14] is used. In this e-shopping system, every time, the application is executed, a new key pair(private key and public key) is generated.
Here, only the authorized customer can enter into the e-shopping system and can browse items from various shops and put the selected items into the shopping cart to buy. Then the total amount of the shopping is encrypted and signed using ECC-192 and SHA-256 with ECDSA respectively.

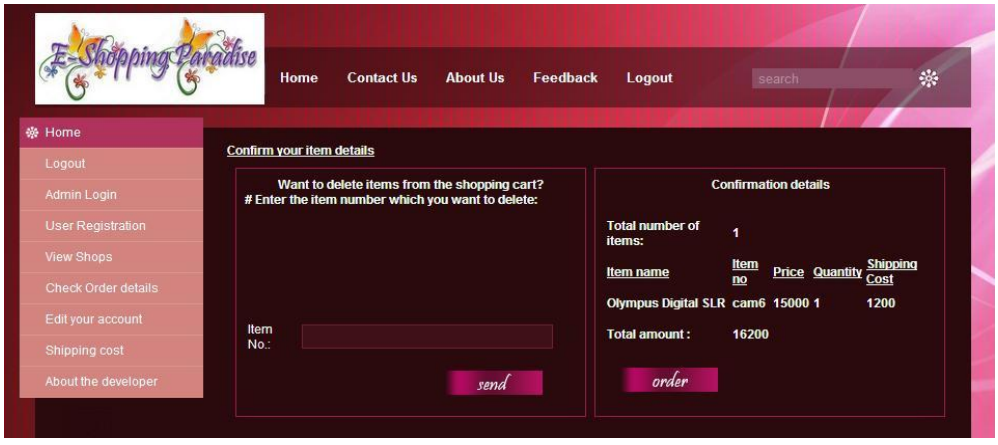


Figure 4. Items in shopping cart

After, the customer, selects the "order" button, the key pair of ECC is generated, the total amount which is shown in the above picture is encrypted and signed using ECC-192 and SHA256 with ECDSA and another is window is come in which the credit card number is encrypted using ECC-192 and the delivery address of the shopping items is signed using SHA256 with ECDSA, which are illustrated in Figure 5.

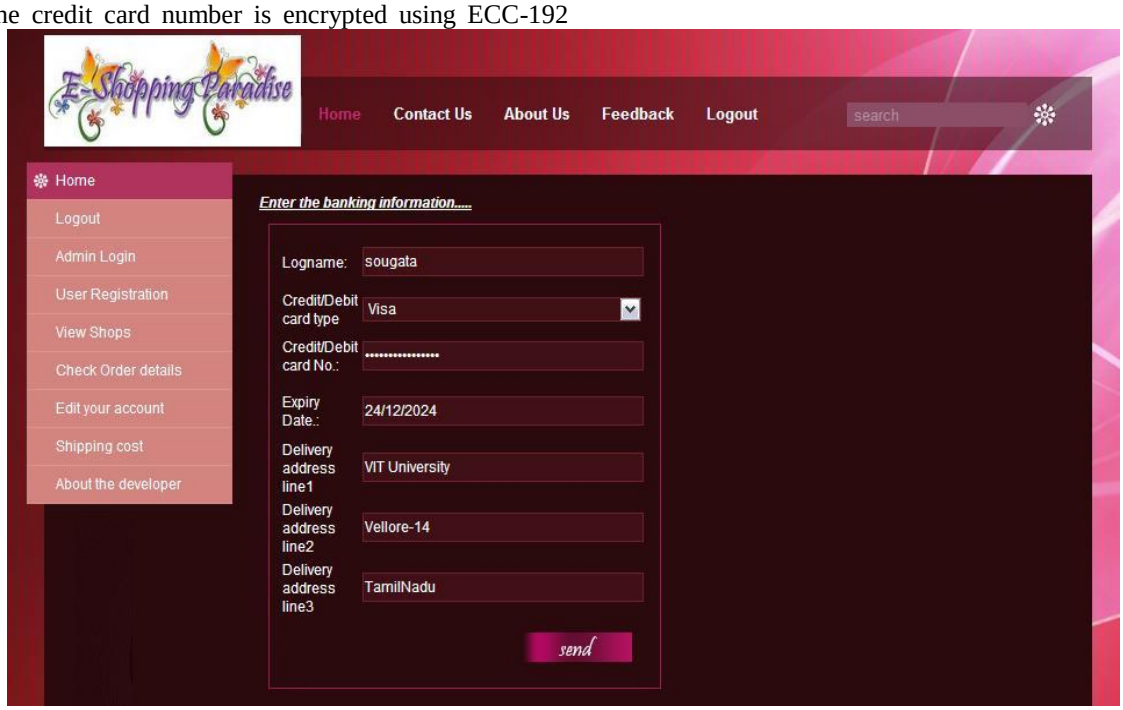


Figure 5. Input data entry process

After, the authenticated customer selects the "send" button as illustrated in Figure 5, encrypted and signed data is temporarily stored in a table in to the database.

Data Field	Value Constraints
Card number	16 characters encrypted with ECC-192
Logname/User Id	Maximum 12 characters encrypted with ECC-192
Provider Bank name	40 characters
Delivery address line1	Maximum500 characters signed with SHA256 with ECDSA
Delivery address line2	Maximum 500 characters signed with SHA256 with ECDSA
Delivery address line3	Maximum 500 characters signed with SHA256 with ECDSA
Amount	Maximum 500 characters encrypted with ECC and signed with SHA256 with ECDSA

Table1. Input processing table

Here, the credit/debit card number is encrypted using ECC-192 to achieve confidentiality, the total amount is encrypted and signed using ECC-192 and ECDSA with SHA256 to achieve confidentiality, integrity and authentication and the delivery address of the of the shopping items is signed using ECDSA with SHA256 to achieve the integrity so that it can not be changed.

Then it is sent to the merchant bank. The encrypted and signed data is sent to the provider of the credit card and the provider bank decrypts the encrypted data and verifies the signed data. Then the customer bank sends a reply to the merchant bank. The shopping amount is credited to the e-shopping system's account. After that the customer gets the confirmation of the transaction as shown in the Figure 6.

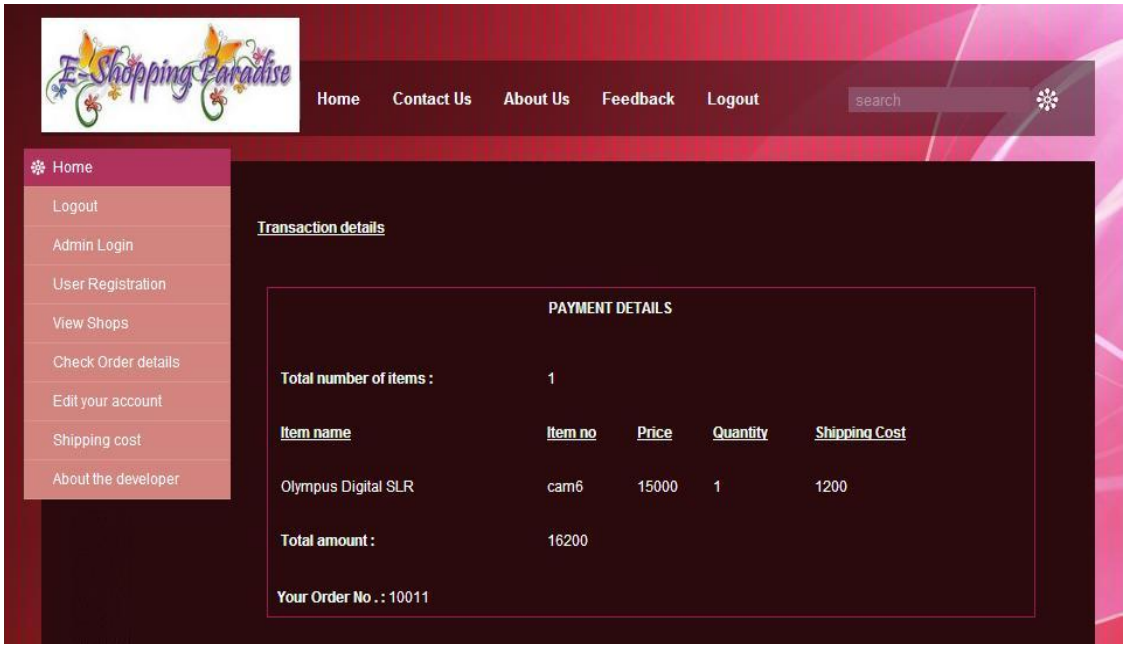


Figure 6. Verified and Decrypted data

After the that, the customer can check his order details if it is alright or not by entering the order number as shown in Figure 7 and then he can verify the total amount of shopping and his order is submitted for processing.

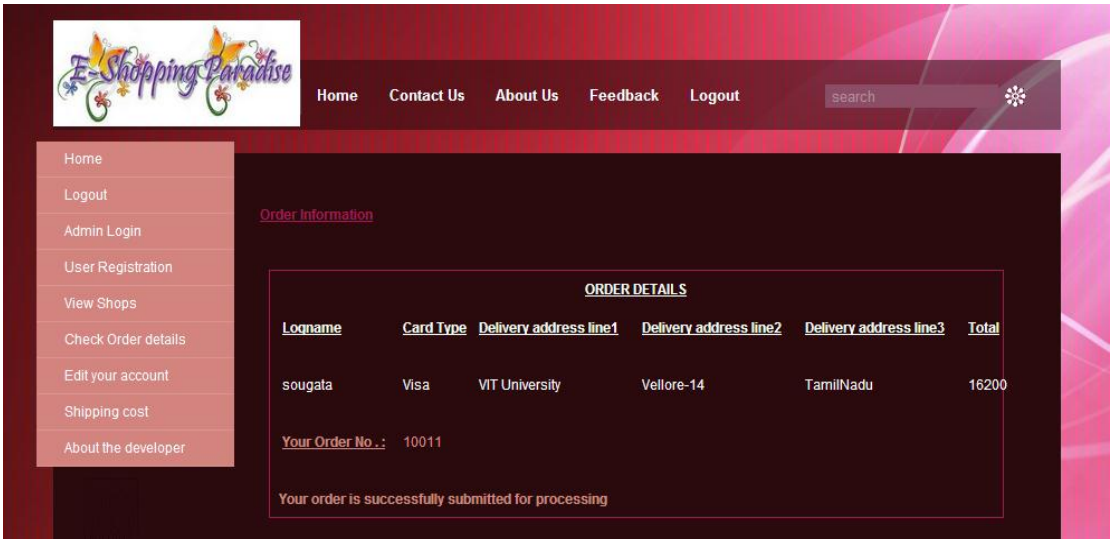


Figure 7. Order Details

6. Evaluation:

After completion of the system's implementation phase, multiple tests were conducted to ensure that each process and the entire system were operating properly.

So, here the process testing and system parameter testing is done to check the system is working properly or not.

6.1 Process Testing:

In this test, multiple keys were generated to ensure that the algorithm worked properly. The tests are repeated with different input and public/private key combinations. The results generated by the application program were displayed on Table2.

Test No.	Public Key	Private Key	I = Input O = Output C = Ciphertext	
1.	X: 8c53b724e53b27a8b25ad122e4a34d98d08e814badd94d7a Y: 57e2d8d57e8bc73fbab824bd08e70848cd9cd67c7d21ee7e	fd0c25b1	I	Sougata Khatua
			C	+L/nmjYchTqCl25RomRjFWIzf/xiiIEUsLnW6x7Q
			O	Sougata Khatua
2.	X: ecb0f0aa45469965b201e03dcf227b05a217aa8c4c4825f9 Y: 9bbcf5dd5bf2b23bd9503940242fc76eb5bcf82b0336f124	35c30e2	I	VIT University
			C	fDaZnSOI2Qg2nWg8NuU4KqE+pyugWgpRRSffXRyfCS/FxA==
			O	VIT University
3.	X: 8d2a8d88e0782d14d39776c938ccad9b09e5bb3e4b95f15a Y: edfcbf530f5b3904395a4ab9680ace90971402e462bb3fe7	120991b	I	VIT
			C	ACrZ3PeApcPmeDbZaE+VOA0XfHcK95g=
			O	VIT

Table 2. Process state of ECC

6.2.System Parameter Testing:

Here the test are done using the pre-determined test scripts. The system parameter values are encrypted and decrypted to check any abnormality is there in the security system or not as shown in Table 3.

Sl. No	Public Key	Private Key	L =Logname O = Output C=Ciphertext CC=Credit card No.	
1.	X: 8c53b724e53b27a8b25ad122e4a34d98d08e814badd94d7a Y: 57e2d8d57e8bc73fbab824bd08e70848cd9cd67c7d21ee7e	fd0c25b1	L	**sougata**
			C	ACrZ3PeApcPmeDbZaE+VOA0XfHcK95g=123+=dce=
			O	**sougata**
2.	X: ecb0f0aa45469965b201e03dcf227b05a217aa8c4c4825f9 Y: 9bbcf5dd5bf2b23bd9503940242fc76eb5bcf82b0336f124	35c30e2	CC	**1234567123456712**
			C	au4hkpI3Fanvz8eeBdsF2EOFZlfw0mmijIkJtUUj5X+oRwUu
			O	**1234567123456712**

Table 3. Input processing table

Table 3 illustrates that the system performs the encryption and decryption properly and check for any fault is there or not to encrypt and decrypt the confidential data.

Table 4 shows the system performs signature generation and signature verification properly to achieve the integrity, authentication and non repudiation.

Value Constraints	Value	Signature	Signature Verification
Delivery Address Line 1	VIT University	MDYCGQDaaGM3rmkP+jKZnioVBzoTTA4Oh5aX LK8CGQCQv7OE6MP4botQPJiurEW6DF0QtRN4L K8=	True
Delivery Address Line 2	Vellore -14	MDQCGCsER8N6bK1jyA1Z4+GDyP6+5vSeROP68 wIYZDuge52HySwl4/AC++yhvjL1dcsVGUOW	True
Delivery Address Line 3	Tamil Nadu	MDQCGAjhkVKLJvQRX5UB0q62bxKSxIoid9AmY AIYKcEiHWbKLR8uJ9ug8iiugGDF8BP7b2RX	True
Total Amount	16,200	a+kQv6fjF5UfbYv4eUKCz6U3iOtxOxm9yyNt5Hqto vHHcVi6C4Ym7NHiglpt/NcRuitjor5BMT4W dV0o4epjpHzEybU4Pf1l8ZO3	True

Table 4. System parameter testing table

7. Performance Analysis:

After the completion of the development phase, the performance of the e-shopping system is analyzed against the existing e-shopping system which currently uses RSA or Elgamal cryptosystem to provide the security. The Table 5 summarizes the security strength and the key length of the ECC, RSA, Elgamal and DSA. As the validity of ECC-160 is up to 2010, and now it is 2011,ECC-192 is used in this project to provide security to the e-shopping system.

ECC	RSA/DSA/Elgamal	MIPS years to attack	Protection Lifetime
160	1024	10^{12}	Up to 2010
224	2048	10^{24}	Up to 2030
256	3072	10^{28}	Beyond 2031
384	7680	10^{47}	
512	15360	10^{66}	

Table5: Summarization of Public key System[11]

Graph Comparison of key size:

From this graph, it is clear that ECC needs much less key size compared to RSA and DSA, to achieve the required level of security.

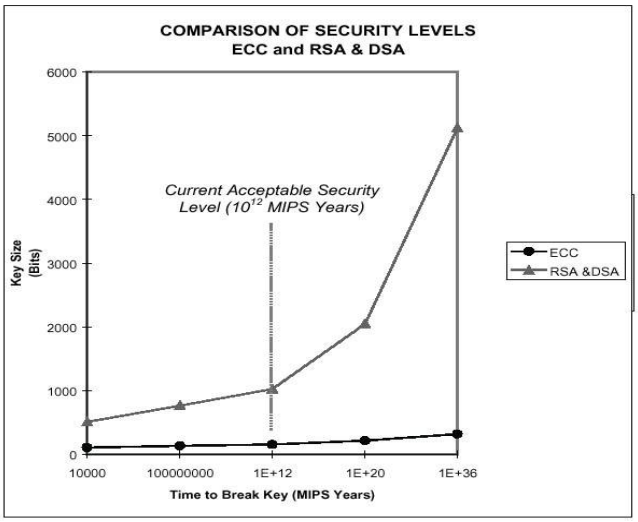


Figure 8. Comparison between ECC and RSA/DSA[10]

7.1. Analysis of the Encryption and Decryption process:

To compare the performance of the encryption and decryption process, the ECC-160, ECC-192, ECC-224, RSA-512, RSA-1024, RSA-2048, Elgmal-1024, Elgamal-1536 and Elgamal-2048 public key cryptosystems are used.

Platform: Intel Core 2 Duo processor @ 2.2 GHz with Windows XP using JAVA

The comparison table for performance analysis is given below:

	ECC-160	Elgamal-1024	RSA-1024	ECC-192	Elgamal-1536	RSA-1536	ECC-224	Elgamal-2048	RSA-2048
Execution time	4 sec	7sec	8 sec	5 sec	9 sec	12 sec	6 sec	11 sec	22 sec
Key size ratio	1: 6.4			1 : 8			1 : 9.14		

Table 6. Performance analysis of encryption and decryption process

Graph comparison of execution time between these Algorithm:

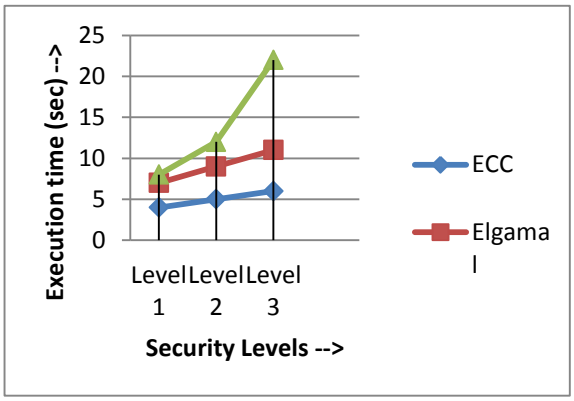


Figure 9. Execution time comparison

From the Table 6 and the above graph it is clear that ECC is much faster than RSA and Elgamal cryptosystem and also the key size ratio of the ECC is much less than the RSA and Elgamal cryptosystem and at the same time ECC provides the same level of security as RSA and Elgamal cryptosystem. Hence the performance of the ECC is much better in terms of execution time than these two public key cryptosystems.

CPU Utilization:

Platform: Intel Core 2 Duo processor @ 2.2 GHz with Windows XP using JAVA

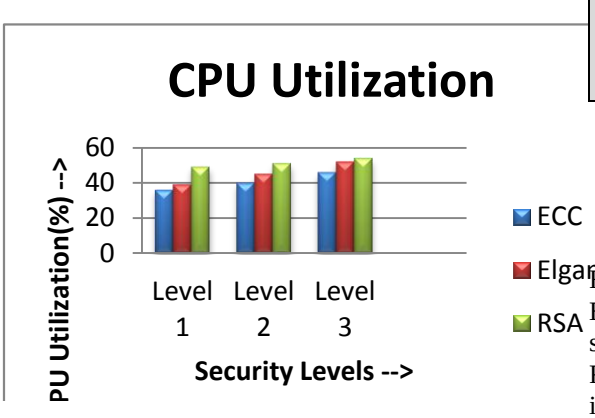


Figure 10. CPU Utilization

The CPU utilization of the ECC never exceeds 50% utilization of CPU. The other two public key algorithms

RSA and Elgamal exceeds the 50% utilization of the CPU. So ECC also uses low resources Hence the performance of the ECC is much better than these two public key cryptosystems.

7.2. Analysis of the Signature generation and Verification process:

To compare the performance of the signature generation process and verification process, SHA256 with ECDSA and SHA256 with RSADSS are used.

Platform: Intel Core 2 Duo processor @ 2.2 GHz with Windows XP using JAVA

The comparison table for performance analysis is given below:

Digital Signature Scheme	Key generation	Signature generation	Signature verification	Total time
SHA256 with ECDSA	0.4 sec	0.5 sec	0.8 sec	1.7 sec
SHA256 with RSADSS	1.1 sec	0.5 sec	0.4 sec	2.0 sec

Table7. Performance analysis of signature generation and verification process

From the Table 7 and Figure 11, it is clear that ECDSA is faster than RSADSS and also the key size ratio of the ECDSA is much less than the RSADSS . Hence the performance of the ECDSA is much ahead of RSDSS.

Graph chart of execution time:

Platform: Intel Core 2 Duo processor @ 2.2 GHz with Windows XP using JAVA

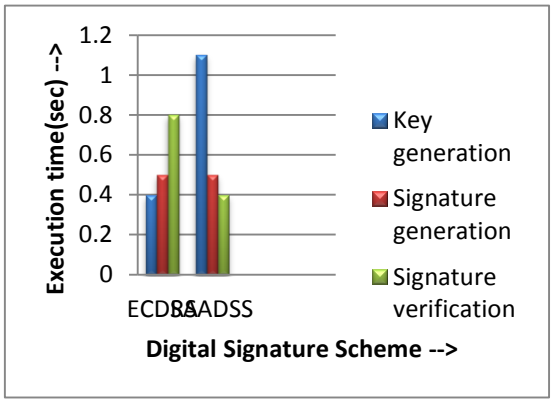


Figure 11. Graph chart of execution time of digital signature schemes

Hence, from the above analysis, it is clear that both ECC for encryption and decryption (ECIES) and ECDSA is far ahead from the other public key cryptosystem currently available. ECIES and ECDSA both use less key size, less resource, less CPU utilization and less time consuming.

8. Conclusion and Future work:

The rapid development of the Internet and Ecommerce including online shopping made it important to provide the confidentiality, integrity and non-repudiation to provide secure transactions. The above analysis suggests that *Elliptic Curve Cryptography (ECC)* is the solution of these problems and it is emerging as an attractive alternative to traditional public-key cryptosystems (*RSA*, *DSA*, *DH*). *ECC* offers equivalent security with smaller key sizes resulting in faster computations, lower power consumption, as well as memory and bandwidth savings.

In future the security of the E-shopping system can be provided using *Hyper Elliptic Curve Cryptography (HECC).* Now many mathematicians are analyzing it and this algorithm needs only 80 bit long key to achieve the required level security. So it will need less key size than ECC. So, in future, when the security packages will be available for this algorithm, the security of the E-shopping system can be applied using *Hyper Elliptic Curve Cryptography (HECC).*

9.References:

[1] Rupesh Kumar, Mario Muñoz Organero, "XML Secure Documents for a Secure e-Commerce Architecture", Global Journal of Enterprise Information System,Volume-2 Issue-1,June 2010

[2] Vikas Rattan, "E-Commerce Security using PKI approach", International Journal on Computer Science and Engineering(IJCSE),Vol. 02, No. 05, 2010, 1439-1444

[3] Dr. S.S.Riaz Ahamed, "The Influence of scope and Integrated Experimental Approach to safe Electronic Commerce ",International Journal of Engineering Science and Technology, Vol. 2(3), 2010, 448-456

[4] Ayu Tiwari,Sudip Sanyal,Ajith Abraham,Svein Knapskog,Sugata sanyal,"A MULTI-FACTOR SECURITY PROTOCOL FOR WIRELESS PAYMENT-SECURE WEB AUTHENTICATION USING MOBILE DEVICES",ISBN:978-972-8924-30-0 © 2007 IADIS

[5] I. K. Salah, A. Darwish, and S. Oqeili, "Mathematical attacks on RSA cryptosystem," Journal of Computer Science, pp. 656-671, Aug. 2006.

[6] Behrouz A. Forouzan, debdeep Mukhopadhyay, " Cryptography and Network Security", Tata McGraw-Hill , Page No.:358 © 2010 by McGra-Hill Companies.

[7] Zhang Chunhua, "Analyzing Encryption Technology Applied in Farm Product E-commerce System Security", International Conference on Electronic Measurement and instruments(ICEMI) , 2007 IEEE

[8]http://www.mgsipap.org/egov-conference/Post_Conference/conf_Papers/Papers/Jagdev_Singh.pdf

[9] Marchany, R. and Tront, J. " E-commerce Security Issues", hicss, p-193, 35th Annual Hawaii International Conference on System Sciences(HICSS'02):2002-Volume 7, IEEE.

[10] http://www.cs.umd.edu/Honors/reports/ECCpaper.pdf

[11] http://citeseerx.ist.psu.edu/viewdoc/doi=101.1.98.778

[12] http://www.trustis.com/pki/fpsia/guide/the-abc%27s-of-secure-electronic-commerce.pdf ,White paper,2001

[13] http://www.businessdictionary.com/definition/online-shopping.html

[14] http://www.bouncycastle.com

Author Biographies

Sougata Khatua has received his B.Sc (Computer Science) degree from Midnapore College under Vidyasagar

University**,** Paschim Medinipur , West Bengal, India. Currently he is a final year post graduate student of M.Sc (Computer Science) at VIT University, Vellore, T.N., India. His areas of Interest are Cryptography and Information Security.

Dr.N.Ch.S.N. Iyengar (M.Sc,M.E,Ph.D) is a Senior Professor at the School of Computing Science and Engineering at VIT University, Vellore, Tamil Nadu, India. His research interests include Agent based Distributed Computing, Data Privacy and Security, Cryptography, Intelligent computational methods and Bio informatics. He has authored several textbooks and had nearly 100 research Publications in International Journals. He chaired many international conferences and delivered invited/ technical lectures/ keynote addresses besides being International program committee member.

Image Encryption Using NTRU Cryptosystem

Ayushi[1], Dr.A.K.Mohapatra[2], Dr.Chhaya Ravikant[3]
[1]*M.Tech (IT, 6th Sem), USIT, GGSIPU, Delhi*
[2,3]*Assistant Professor, IGIT, GGSIPU, Delhi*
[1]ayushibmiet@gmail.com, [2]mohapatra.amar@gmail.com

***Abstract* - Cryptography** is the study of achieving security by encoding messages to make them non-readable. Cryptography is a process which is associated with scrambling plaintext into cipher text (encryption), then back again (known as decryption). The most common types are Secret Key Cryptography which is also known as Symmetric Key Cryptography and Public Key Cryptography which is also known as Asymmetric Key Cryptography[4].

Public Key Cryptography involves the use of two keys: one is the private key and other is public key. Both are required to encrypt and decrypt a message or transmission. The owner of the key is responsible for securing it .The public key is public. Public key cryptography intends for public keys to be accessible to all users. If a person can access anyone public key easily, then the two parties can communicate securely and with little effort, i.e. without a prior key distribution arrangement. In this, the key used for sending message to A is public key and the key used for decrypt the message by A is called private key. The main advantage of public-key cryptography has more security and convenience and so that there is little chance that an attacker can discover the keys during their transmission. In Public-key authentication, each user has sole responsibility for protecting his or her private key. This property of public-key authentication is often called non-repudiation [4].
In this paper, square binary matrix of an image is encrypted through matrix based NTRU (Nth Degree Truncated Polynomial Ring Units) to generate public key and private key for encryption and decryption.
In Public-key authentication, each user has sole responsibility for protecting his or her private key. This property of public-key authentication is often called non-repudiation.
***Keywords*—** NTRU, Private Key, Public Key, Encryption, Decryption, Modular Operation, Image Encryption.

1. Introduction to NTRU Approach

The NTRU public key cryptosystem, a relatively new cryptosystem, was developed in 1996 at Brown University. Although having the possibility of failed decryption, NTRU can be used in mobile devices and smart-cards and other mobile applications because of its features of easy generation of keys, high speed and low memory use. When it comes to the security, using the parameters recommended, NTRU is still safe for the already known attacks. Now it is already fully accepted as an IEEE P1363 standard under the specifications for lattice-based public-key cryptography [5].
The most popular public key cryptosystems like RSA and ECC are based on the complexity of number theoretic problems and their security is highly dependable to the distribution of prime numbers or based on the discrete logarithm problem on finite fields. With the development of distributed computation, grid computing and quantum computers the breaking times, even the brute force attacks, for these cryptosystems are diminished. This can be dangerous for future use of the public key cryptography. .NTRU is set up by three integers (N; p; q) such that:

- N is prime,
- p and q are relatively prime, gcd(p; q) = 1, and
- q is much much larger than p.

NTRU is based on polynomial additions and multiplications in the ring R = Z[x]/(xN-1). We use the "*" to denote a polynomial multiplication in R, which is the cyclic convolution of two polynomials. After completion of a polynomial multiplication or addition, the coefficients of the resulting polynomial need to be reduced either modulo q or p. As a side note, the key creation process also requires two polynomial inversions, which can be computed using the Extended Euclidean Algorithm [5].

1.1 Key Generation

For the public key, the user must:

- choose a secret key, a random secret polynomial f €R, with coefficients reduced modulo p,
- choose a random polynomial, g € R, with coefficients reduced modulo p, and
- Compute the inverse polynomial Fq of the secret key f modulo q.

Once the above has been completed, the public key, h, is found as h = p*Fq *g (mod q)

1.2 Encryption

The encrypted message is computed as e = r * h + m (mod q) where the message, m € R, and the random polynomial, r € R, has coefficients reduced modulo p.

1.3 Decryption

The decryption procedure requires three steps:

- a = f * e (mod q)
- shift coefficients of a to the range (-q/2,q/2)
- b=a mod p
- d = Fp *b (mod p).

The last step of decryption requires the user to compute the inverse polynomial Fp of the secret key f modulo p. The decryption process will recover the original message (d = m).

2. Description

In this paper, we are using Public key Cryptography in which we have to create two keys i.e. public key and private key. The receiver, B creates a public/private key pair. B first randomly chooses two matrices X and Y, where matrix X should be an invertible matrix (modulus p). B keeps the matrices X and Y private, since anyone who knows either one of them will be able to decrypt messages sent to B. B's next step is to compute the inverse of X modulo q and the inverse of X modulo p. Thus he computes matrix Xq and Xp which satisfies X*Xq = I (modulo q) and X*Xp = I (modulo p)..Now B computes the product H = p*Xq*Y (modulo q). B's private key is the pair
of matrices X and Xp and his public key is the matrix H [6].

2.1 Example

The example parameters are: q=32 & p=3.

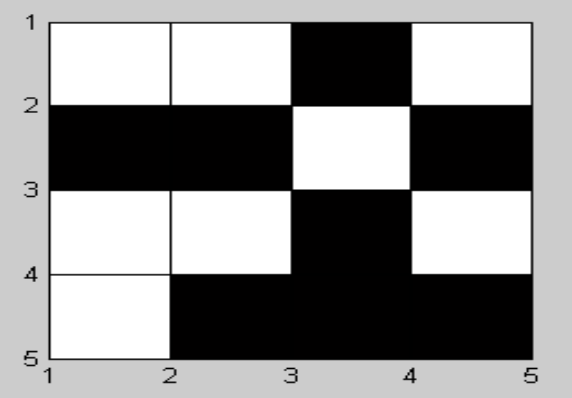


Figure 1

If this image has to be encrypted then matrix for this is given below:

$$M=\begin{pmatrix}1&1&0&1\\0&0&1&0\\1&1&0&1\\1&0&0&0\end{pmatrix}$$

Let matrix X = $\begin{pmatrix}1&-1&1&0\\0&-1&1&1\\1&0&1&-1\\1&1&0&-1\end{pmatrix}$

and matrix Y = $\begin{pmatrix}1&0&-1&1\\0&-1&0&1\\0&-1&1&0\\0&0&-1&1\end{pmatrix}$

Next B computes the inverse Xp of X modulo p and the inverse Xq of X modulo q.
He finds that: Xp = [Inverse of X] (mod p) =

$$\begin{pmatrix}1&0&-1&1\\-1&1&0&1\end{pmatrix} \qquad \begin{pmatrix}1&0&2&1\\2&1&0&1\end{pmatrix}$$

$$\begin{matrix}-1&1&1&0\\0&1&-1&1\end{matrix} \quad (\text{mod } p) = \quad \begin{matrix}2&1&1&0\\0&1&2&1\end{matrix}$$

Xq = [Inverse of X] (mod q) = $\begin{pmatrix}1&0&31&1\\31&1&0&1\\31&1&1&0\\0&1&31&1\end{pmatrix}$

B generates the public key(H)as H= (p.Xq.Y) (mod q)
=

$$\begin{pmatrix}3&-93&87&6\\93&-3&-96&99\\93&-6&-90&96\\0&-96&90&6\end{pmatrix} \text{ (mod q) } = \begin{pmatrix}3&3&26&3\\29&29&0&3\\29&26&6&0\\0&0&26&6\end{pmatrix}$$

B's private key is the pair of matrices X and Xp, and his public key is the matrix H.

2.1.1 Encryption

If a person W wants to send an image to B using B's public key H then convert the image in the form of a binary matrix M, (which is a matrix of same order as X and Y) whose elements are chosen modulo p. Next Step is to choose another matrix R of the same order as X. To send matrix M of an image, W chooses a random matrix R (which is of same order as matrix X), and B's public key H to compute the matrix. E = R*H + M (modulo q).The matrix E is the encrypted matrix which W sends to B [6].

Now, suppose W wants to send the Image matrix M to B by using B's public key.

Matrix M = $\begin{pmatrix}1&1&0&1\\0&0&1&0\\1&1&0&1\\1&0&0&0\end{pmatrix}$

She first chooses a random matrix R of same order as X, Y and M.

Matrix R = $\begin{pmatrix}-1&0&0&1\\0&1&0&-1\\1&0&-1&0\\1&0&-1&0\end{pmatrix}$

Encrypted message E = (H.R + M) (mod q)

$$= \begin{pmatrix}27&4&-29&1\\-26&29&-2&0\\-22&27&-6&4\\33&0&-32&0\end{pmatrix} \text{ (mod q)}$$

$$= \begin{pmatrix}27&4&3&1\\6&29&30&0\\10&27&26&4\\1&0&0&0\end{pmatrix}$$

W sends the encrypted Matrix E to B.

2.1.2 Decryption

Now B has received W's encrypted matrix E and he decrypt it. He begins by using his private matrix X to compute the matrix. A = X*E (modulo q). B next computes the matrix B = A (modulo p).
Finally B uses his other private matrix Xp to compute C = Xp*B (modulo p). The matrix C will be W's original message M [6].
B has received the encrypted matrix from W.

$$E = \begin{pmatrix} 27 & 4 & 3 & 1 \\ 6 & 29 & 30 & 0 \\ 10 & 27 & 26 & 4 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

He uses his private key X to compute A = X*E (modulo 32)

$$A = X.E \pmod q = \begin{pmatrix} 31 & 2 & 31 & 5 \\ 5 & 30 & 28 & 4 \\ 4 & 31 & 29 & 5 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Since B is computing A modulo q, he can choose the coefficients of A to lie between -q/2 and q/2. When B reduces the coefficients of X*E (modulo32), he chooses values lying between -15 and 16 and not between 0 and 31[6].

$$A = \begin{pmatrix} -1 & 2 & -1 & 5 \\ 5 & -2 & -4 & 4 \\ 4 & -1 & -3 & 5 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Next B reduces the coefficients of A modulo 3 and choosing the interval in [0, 1],

$$B = A \pmod p = \begin{pmatrix} -1 & -1 & -1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 0 & -1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Finally, B uses Xp, the other part of his private key, to compute C = Xp*B (modulo p)

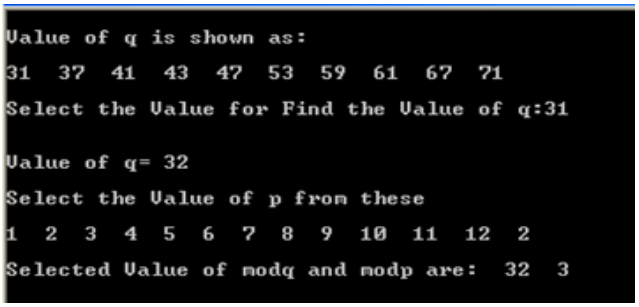
$$C = Xp.B \pmod p = \begin{pmatrix} 1 & -2 & 0 & -2 \\ -3 & 0 & -2 & 0 \\ -2 & -2 & -3 & -2 \\ 1 & 0 & 0 & 0 \end{pmatrix} \pmod p$$

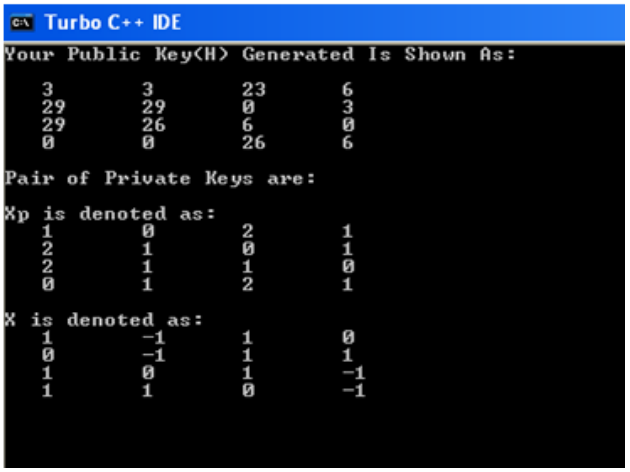
$$= \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

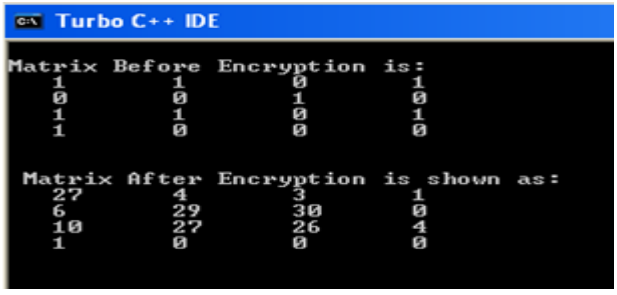
Matrix C is already in interval [0, 1], so there is no need of rearrangement.
The matrix C is W's Image Matrix M, so B has successfully decrypted W's message.

3. Results

The results for the above example as shown below:

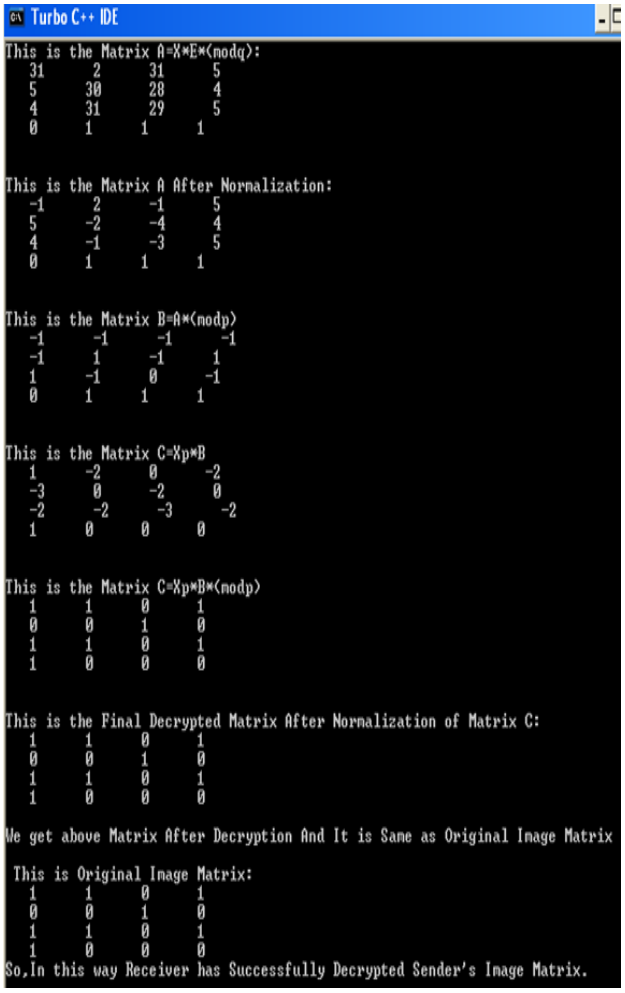






1 1 0 1

1 1 0 1
1 0 0 0



4. Conclusion

In this paper, we encrypt the image in form of binary matrix using NTRU Cryptosystem. This method is suitable for sending large images after converting them into matrix form. This is more secure method than others because we are using matrix as a key.

5. References

[1] C. Narasimham, Jayaram Pradhan "Performance Analysis of Public key Cryptographic Systems RSA and NTRU", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.8, August 2007,87-96.

[2] Priit Karu "Practical Comparison of Fast Public-key Cryptosystems", Seminar on Network Security, 2000.

[3] Qing Liu, Yunfei Li,Lin Hao,Hua Peng "Two Efficient Variants of the RSA Cryptosystem", International Conference On Computer Design And Appliations (ICCDA 2010),2010.

[4] Cryptography and Network Security by Atul Kahate.

[5] Xu-Ren Luo and Chen-Hui Jerry Lin, "Discussion on Matrix NTRU" IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011.

[6] Nayak, R. Sastry, C.V. Pradhan, J.,"A Matrix Formulation for NTRU Cryptosystem", proceedings of conference on Networks, New Delhi,2008(12-14 Dec),1-5

[7] Rodney D'Souza "The NTRU Cryptosystem: Implementation and Comparative Analysis", 2001.

[8] Ali Mersin "The Comparative Performance Analysis of Lattice Based NTRU Cryptosystem with other asymmetrical Cryptosystems" A thesis submitted for Master of Science, September 2007.

Mobile SMS Based Controller with Message Feedback

Arafat Zaidan[1], Mutamed Khatib[2] and Basim Alsayid [3]

[1]Department of Electrical Engineering, Palestine Technical University-Kadoorie (PTU), Palestine
arafatzaidan@yahoo.co.uk
[2]Department of Telecommunication Engineering and Technology, Palestine Technical University-Kadoorie (PTU), Palestine
mutamed.khatib@gmail.com
Dean, College of Engineering and Technology, Palestine Technical University-Kadoorie (PTU), Palestine
b.alsayid@ptuk.edu.ps

***Abstract*:** Due to the development in telecommunication, researchers are able now to control –almost- any device from a distance. This paper presents a controlling strategy using cellular mobile devices. The first objective is to build an interface circuit between the device to be controlled and a controlling mobile unit. This controlling mobile unit acts as a receiver of orders from any mobile or phone in order to control any device via Bluetooth. A message is then sent back as an SMS given details about the status of the system. The order is translated in the controlling mobile unit by Dual Tone Multi Frequency (DTMF) decoder as a code to the control circuit that controls the device.
This paper focuses on programming a microcontroller using a high level language. The PIC family of microcontrollers was chosen because of its low power consumption which makes this microcontroller popular in portable application. This proposed strategy provides security to the system from any fault by automatically activating an alarm SMS to the system manager informing him about the system status.

***Keywords*:** SMS, control, communication, security, mobile, PIC.

1. Introduction

The widespread use of information technology has dramatically improved both the quality and the efficiency of different services offered to people [1].
The large deployment of wireless networks and the increasing use of handheld devices like the personal digital assistant (PDA), and the mobile phone have encouraged developers to build different kind of applications and systems in all domains [2]. For example, IR remote control is an application installed in mobile phones which can be used as a remote control via Infra-red, this application can be used in a small areas and needs a line of sight. The evolution of micro-electronics and communications technologies brought many innovations in different automation areas, in particular in domestics, where the technology of industrial processes was adapted to routine domestic tasks [3].
The rapid increase in the residential demotic solutions is being noticed lately, because of the users attention for the need of personalized management for their properties and equipment available in the houses [4].
Bluetooth technology provides an unlicensed band that is ISM (Industrial Scientific Medical) band which ranges from 2.4 GHz to 2.4835 GHz enable the goals of global applicability, low power and high aggregate capacity to be met [5]. This is suitable for a wireless home or office environment and industrial applications. Bluetooth wireless technology is a short-range communications system intended to replace the cables connecting portable and/or fixed electronic devices. The key features of Bluetooth wireless technology are robustness, low power, standardized protocol, Upgradeable and low cost [6].
In this paper, a cellular mobile device is used as a controller by building an interface circuit between the device and mobile unit. This controlling mobile unit acts as a receiver of orders from any mobile or phone in order to control any device via Bluetooth [5, 6]. A message is then sent back as an SMS given details about the status of the system. The order is translated in the controlling mobile unit by Dual Tone Multi Frequency (DTMF) decoder as a code to the control circuit that controls the device [7, 8].

2. System Description

Figure 1 shows the flow of sending messages using the Global System for Mobile (GSM) module, the manager sends an SMS message from a mobile programmed previously in the PIC. When the status of any element in the system changes, the system manager receives a message from the GSM terminal.

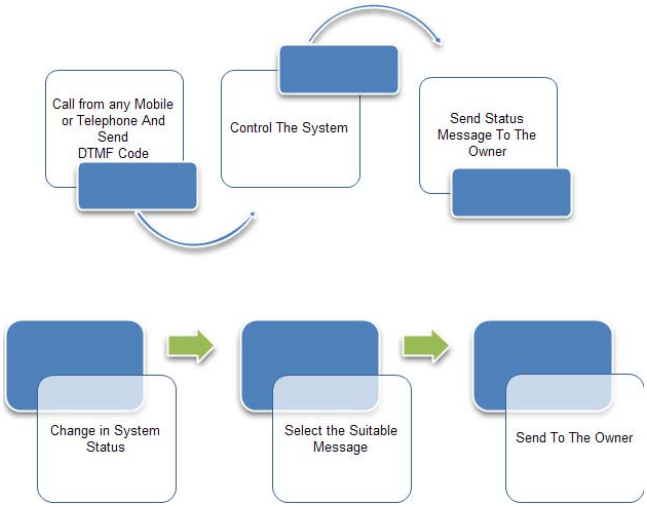


Figure 1. Flow of sending a message

The microcontroller used in this paper is the PIC 16F877A and the program was written using C language. The PIC is used as the brain of the system because it plays a major role between the sender and the controller when executing an order; it also organizes the reply from the controller to the sender. The Dual-Tone Multi-Frequency DTMF IC used in this system is the MT8870. It is used to analyze the signal that is taken from the speaker of the mobile. DTMF adds the horizontal frequencies (upper band) and vertical ones (lower band) from the keypad of a mobile. The keypad consisting of four rows and three columns, which means we need 12 keys to appoint the numbers from 0-9 in addition to (*) and (#) keys as shown in the following table:

Table 1. Frequencies of a keypad to generate a wave of DTMF

Symbol		Tone B [Hz]			
		1209	1336	1477	1633
Tone A [Hz]	697	1	2	3	A
	770	4	5	6	B
	852	7	8	9	C
	941	*	0	#	D

To generate a DTMF tune representing number (1), two frequencies one low (697Hz) and one high (1209Hz) need to be added . The output of the DTMF is a code consisting of four digits. The operating or stopping of the system depends on the arrangement of these digits. DTMF Decoder is a program used to decode DTMF dial tones found on telephone lines with touch tone phones. It is also used for receiving data transmissions over the air in amateur radio frequency bands.

A BCD to Decimal Decoder (7442-j) was used to control the signals from the DTMF, and to know which part is selected for controlling. This BCD-to-decimal decoder consists of eight inverters and four-input NAND gates. The inverters are connected in pairs to make BCD input data available for decoding by the NAND gates. Full decoding of input logic ensures that all of outputs remain off for all invalid input conditions (10–15).

A relay is used to drive the control voltage; it acts as an electrical switch. The PIC is protected from voltage spikes by photo couplers (Opto couplers). It is also used as a controlling switch and as a buffer circuit. The schematic diagram of a simple Opto-isolator is shown in Figure 2.

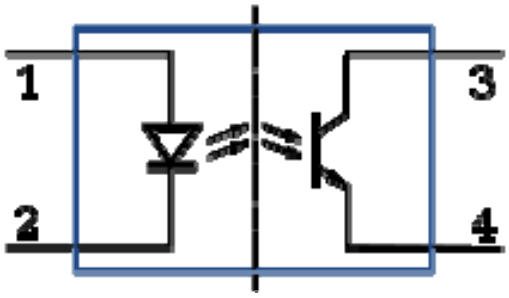


Figure 2. Schematic diagram of an opto-isolator

3. Circuits and Components

3.1 Regulated voltage

The purpose of the regulator is to insure a constant output of 5 volts.

The input goes to pin 1 in LM8050, and the output is taken from pin 2, while pin 3 is common. The output of LM8050 passes through a charge and discharge capacitor stage, and then a smoothing circuit is used to decrease the ripple voltage. The output voltage is used as the supply voltage for all the circuits in the system.

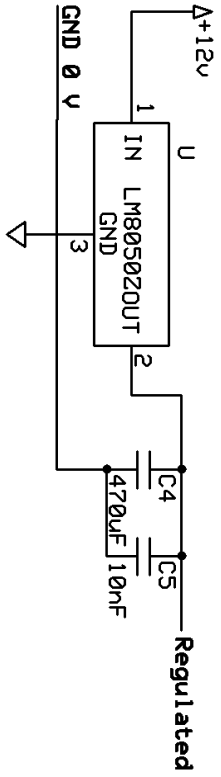


Figure 3. Regulator circuit.

3.2 DTMF circuit

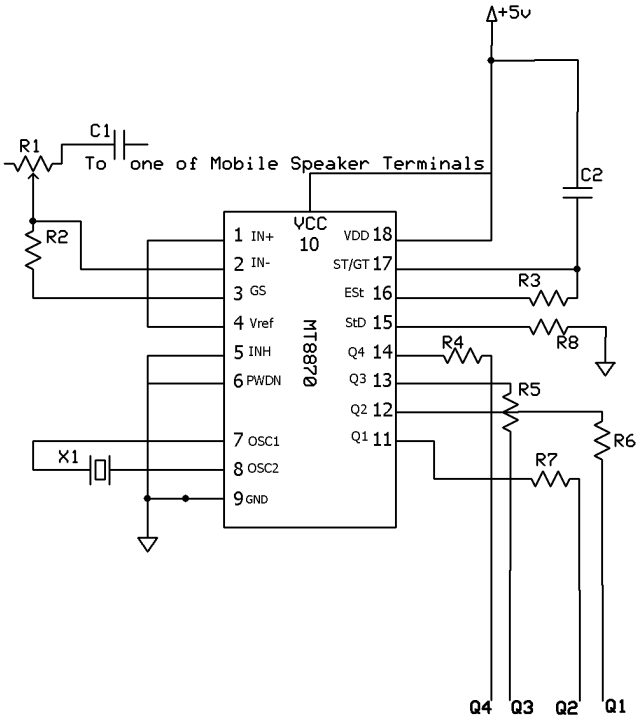


Figure 4. DTMF circuit.

Figure 4 shows a DTMF circuit diagram, the purpose of this circuit is to analyze the sound frequency which is generated from the mobile speakers when pressing any number on the keypad on the caller phone. The input of this circuit is taken from mobile speaker, and the second terminal of the speaker is connected to DC ground of the circuit. The potentiometer here is used to control the speed of the analysis and response.

After analyzing input frequency, the circuit output is taken from 4 pins, i.e., 11,12,13,14 or Q4, Q3, Q2, Q1; it is a 4 bit binary number. The frequency of the MT8870 is 3.58MHz which is generated by crystal X1.

3.3 Decoder

Figure 5 shows a 7442-J BCD to decimal decoder, the purpose of this decoder is to convert the 4 bits binary code, to active low on the pin referred to by the binary number. The inputs of this IC are the 4 bits output from DTMF circuit, connected at pins: 15, 14, 13, 12 or A0, A1, A2, A3,

Figure 5 shows that there is an indication LEDs, which is used to represent the load status, when the LED is ON, the load is connected. The 10 outputs are active low, the outputs that represent numbers: 1, 2, 3, 7, 8 and 9 were used. The control signal to drive the relays was also tracked.

3.4 Control and drive circuit

The strategy is to control any system remotely by DTMF and decoding circuit. But it should be done manually and the controller should always be on standby.

There are 3 relays to turn the loads on, with self continuity, and 3 relays to turn the first three relays off as shown in figure 6. The driving signal of the relays comes from the push-buttons, and the decoder output.

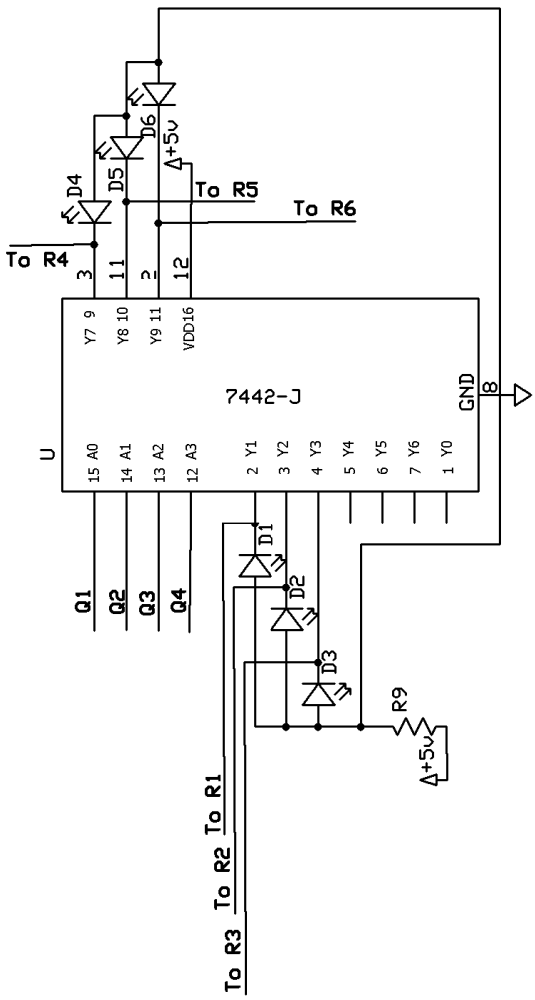
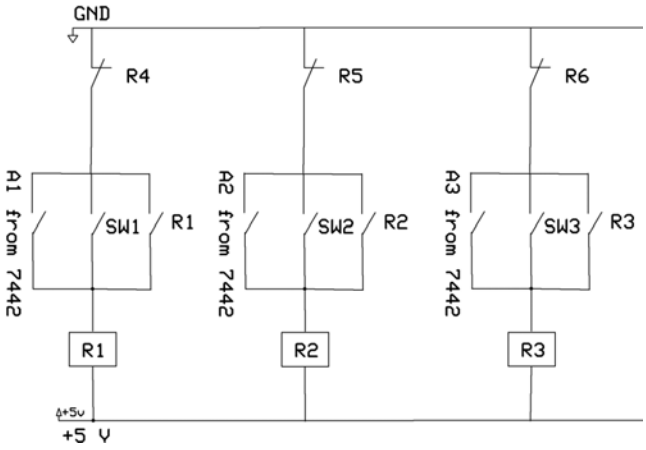


Figure 5. Decoding circuit.



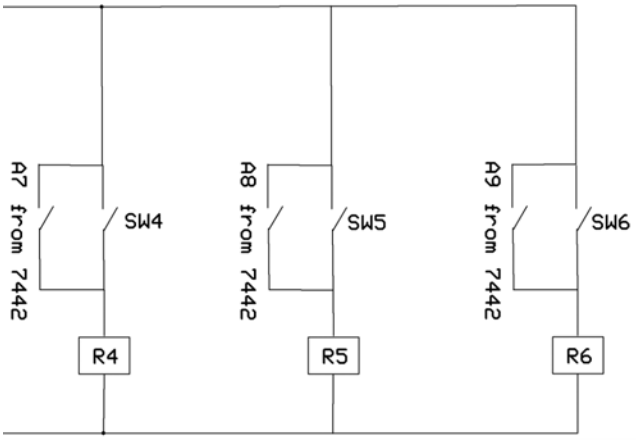


Figure 6. Block diagram of control circuit.

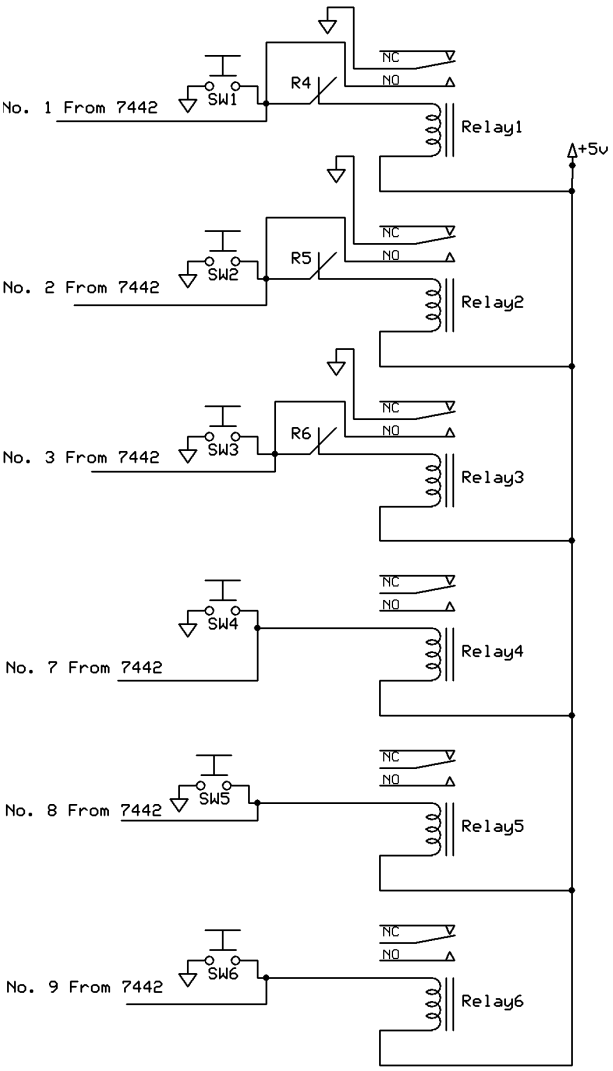


Figure 7. Control and drive circuit.

In order to make buffering between D9F communication port and the PIC, the IC MAX232 was used. Using the D9F makes it possible to program and reprogram the PIC while it is connected to the circuit, making the process faster.
The PIC operations and the registers status may be remotely monitored by connecting the circuit to the computer using the RS-232 cable, which is connected to the serial port (COM1 or COM2).
D8 is an indication LED, when the system is not working or idle, D8 flashes, while it stays ON when the system is busy.
The flashing of D7 means that the PIC is being programmed by computer, so it is not ready.

3.5 Complete schematic diagram

When a call comes to the mobile, 5 volts will appear at the terminals of the mobile's vibrator. These terminals are connected directly to Opto coupler number 8. It activates the send switch by creating a short circuit at the SEND switch, acting as an auto answer operation.
When the call is answered, the voltage at the vibrator terminals will be zero, so the opto coupler goes to the off mode thus enabling the caller to press preset numbers, to control the output, the tones of these numbers to the speakers of the mobile and from the speakers, to the DTMF input through terminal C1
Pin C1 blocks any DC voltage, and the frequented signal passes to pins 1 and 2 of the MT8870. This IC analyzes the signal, and sends the binary code to the 4 pins at the output (11, 12, 13 and 14), for example if the caller presses number 1, binary (0001) will be passed to the output pins (11, 12, 13 and 14). These outputs will be used as the inputs to the BCD-Decimal Decoder which in turn activates a single output connected to relay 1
When the Relay is active, Opto coupler 1 is active, sending a 5 volt signal to the PIC, indicating a change in the status of the system which in turn activates the appropriate message, This is done by creating a short circuit at the mobile switches.

4. System Software

Figure 9 shows a flowchart of the whole programming structure for the controllable system. The only sensor used is a simple switch that is normally open, which means it will be off all the time unless it is triggered. Once the sensor detects any instruction due to the activation of the switch or detection of motion, the PIC microcontroller receives the appropriate tunes generated by the pressing of the numbers on the keypad
of the mobile through the DTMF decoder. The generated tones are analyzed by the PIC and a message is selected and sent to a mobile number which is saved in the PIC.

The software used to design and write the programming code is C language. The code is compiled to generate hex. File which is used to program the PIC microcontroller.

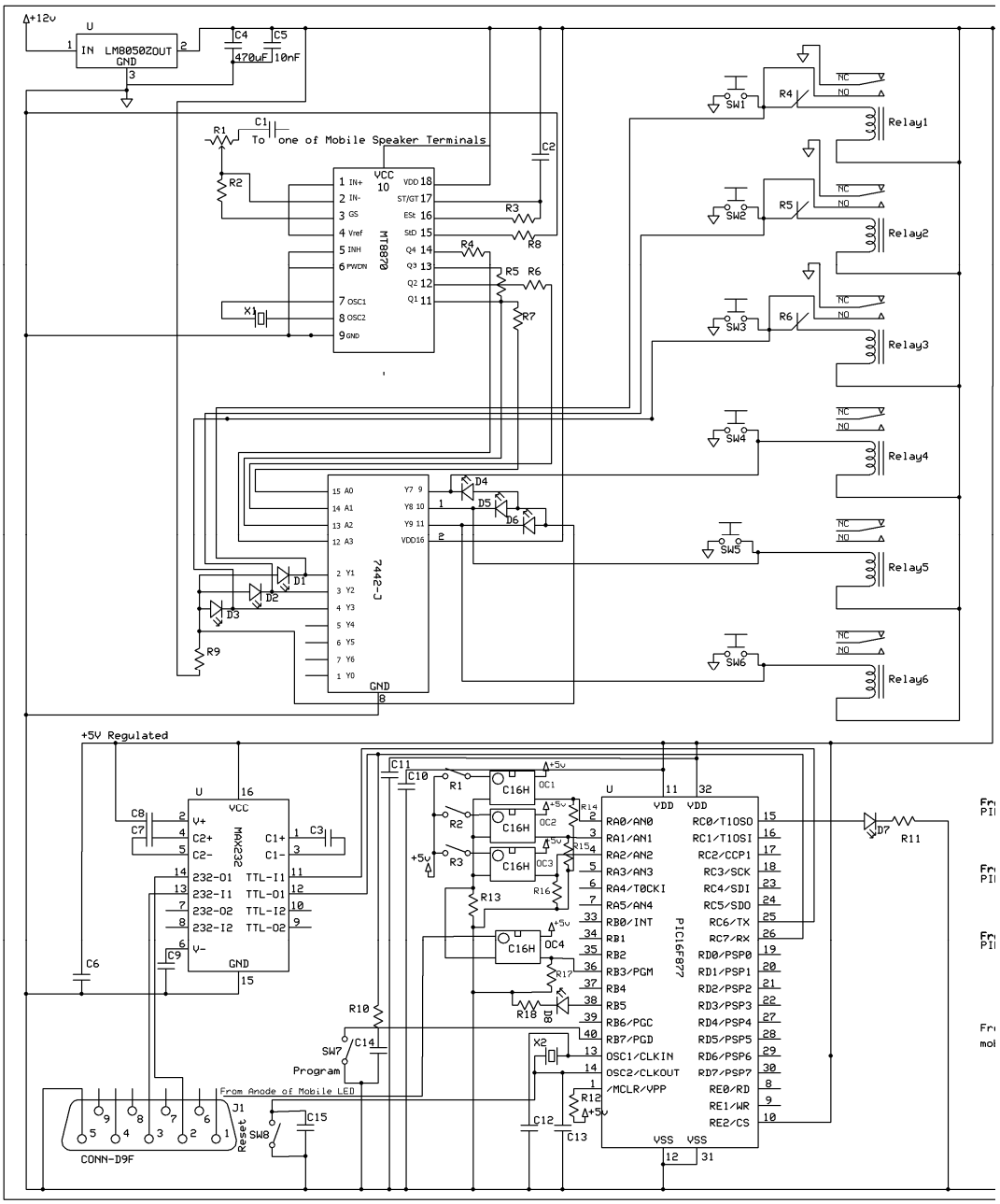


Figure 8. Schematic diagram

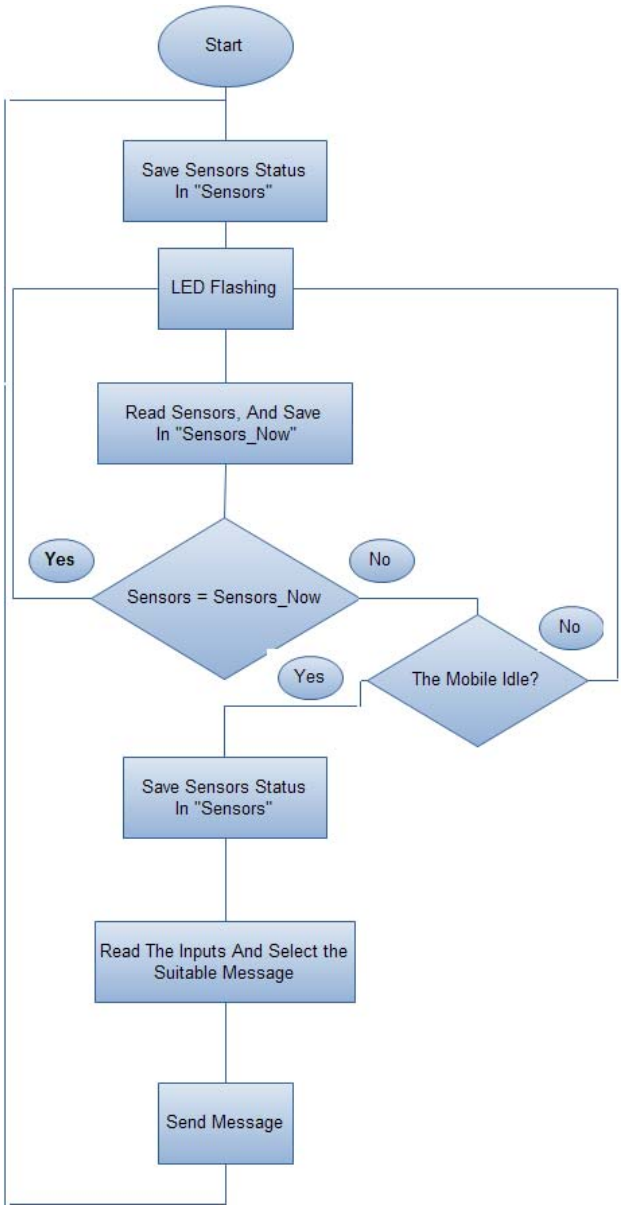


Figure 9. Flowchart of the system

5. Conclusion

An integrated System was built capable of controlling any electrical system, and also sends a feedback message in the form of an SMS showing the status of the system.

References

[1] Mutamed Khatib, Farid Ghani, "Block Transmission Systems in Synchronous Multiuser Communications", International Journal of Latest Trends in Computing IJLTC, Volume 2, Issue 1, pp. 72-79, March 2011

[2] Fontelo P, Ackerman M, Kim G, Locatis C., " The PDA as a portal to knowledge sources in a wireless setting", Telemed J E Health, Vol 9, No. 2, pp.141-147, 2003.

[3] Mafalda Seixas, João Palma, "Remote Alarm and Command System for Residential Domotics Trough GSM-SMS", 9th Spanish Portuguese Congress on Electrical Engineering, 30th June 2nd July, 2005 Marbella, Spain.

[4] Pragnell, M., Spence, L. and Moore, R., The Market Potential for Smart Homes, York Publishing Services Ltd, 2000.

[5] J. Y. Khan, J. Wall, M. A. Rashid, "Bluetooth-Based Wireless Personal Area Network for Multimedia Communication," Electronic Design, Test and Applications, IEEE International Workshop on, pp. 47, The First IEEE International Workshop on Electronic Design, Test and Applications (DELTA '02), 2002.

[6] Sailesh Rathi, "Blue Tooth Protocol Architecture," Dedicated Systems Magazine, Embedded Internet - 00q4 - p. 28 , 2000

[7] Peersman, G., Cvetkovic, S., "The Global System for mobile Communications Short Message Service", IEEE Personal Communications, June 2000, pgs 15-23.

[8] Collesei, S., Di Tria, P., Morena, G., "Short Message service based applications in the GSM network", Proc. 5th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 1994, pgs 939-943.

[9] ETSI TS 100901. Digital cellular telecommunications system (phase 2+); Technical realization of the Short Message Service (SMS) Point-to-point (PP), 3GPP TS 03.40 version 7.50 release 1998.

[10] Peacock, W., Nokia F-Bus Protocol, http://www.embedtronics.com/nokia/fbus.html

[11] Intel Corporation, MCS 51 Microcontroller Family User's Manual, 1994.

Acknowledgment

Authors would like to thank Palestine Technical University-Kadoorie (PTU) for supporting this research and allowing us to conduct this work in the university labs.
Sincere thanks to the undergraduate students: Rami Abu Sham'a, Amenah Khader, Shahd Sukkar and Mahmud Qeadan for their help in building the hardware model and performing the tests.

Author Biographies

Arafat Zaidan received his B.Eng. in Electrical & Electronic Engineering from University of Leicester in 1993, and the MPhil/PhD in Digital Control Engineering, University of Salford in 2000. The research was primarily concerned with deriving mathematical models and implementing a pole placement controller for a powered orthosis He was a control System Engineer with research experience in modern control strategies and plant supervision, and worked for five years at the Hashemite University in Jordan as an assistant professor in the department of Mechatronics. Currently working as an assistant professor in the Department of Electrical Engineering, Palestine Technical University (Kaddorie), Tul Karm, Palestine. Dr. Arafat Zaidan has a number of publications to his credit in various international journals and conference proceedings. He is a member of IEEE, Palestinian Engineers Association.

Mutamed Khatib received B.Sc. in Telecommunication Engineering from Yarmouk University, Irbid, Jordan in 1996 and M.Sc. in Electrical & Electronic Engineering from Jordan University for Science & Technology, Irbid, Jordan in 2003. He received his PhD Degree in wireless and mobile systems from University Sains Malaysia (USM), Malaysia in 2009. From 1996 to 2005, he worked as Transmission, Outside Broadcasting & Studio Engineer in Palestinian Broadcasting Corporation (PBC). From 2005 to 2009 he worked as an Instructor in the Department of Electrical Engineering, Palestine Technical University (Kadoorie), Tul Karm, Palestine. Since September 2009, Dr Mutamed Khatib is working as Assistant professor in the same university. Dr. Khatib has a number of publications to his credit in various international journals and conference proceedings. He is a member of IEEE, Palestinian Engineers Association and Arab Engineers Association.

Basim Alsayid received B.Sc. in Electrical Engineering from Studies University of Bologna, Bologna, Italy in 1991. He received his PhD Degree in Electrical Drives Engineering from University of Bologna, Bologna in 2002. From 2002 to 2007 he worked as Assistant professor in the Department of Electrical Engineering, Palestine Technical University (Kadoorie), Tul Karm – Palestine. From 2007 to 2009 he worked as the head of the electrical engineering department and from 2009 till now he is the dean of the college of engineering and technology at the same university. He is a member of IEEE, Palestinian Engineers Association. He is now involved in a 2 years research program about design and control of photovoltaic systems with a French research group.

Speech Enhancement using Kalman based Adaptive Filtering Techniques

B Raja Sekhara Reddy, Md Zia Ur Rahman, M Ajay Kumar, T Anusha, K Murali Krishna and Dr B V Rama Mohana Rao

Department of Electronics and Communication Engineering,
Narasaraopeta Engineering College, Narasaraopeta, India.
E-mail: mdzr_5@ieee.org

Abstract **-** The aim of this paper is to implement various adaptive noise cancellers (ANC) for speech enhancement based on gradient descent approach, namely the least-mean square (LMS) algorithm. While the LMS algorithm and its normalized version (NLMS), have been thoroughly used and studied. Connections between the Kalman filter and the RLS algorithm have been established however, the connection between the Kalman filter and the LMS algorithm has not received much attention. By linking these two algorithms, a new normalized Kalman based LMS (KLMS) algorithm can be derived that has some advantages to the classical one. Their stability is guaranteed since they are a special case of the Kalman filter. More, they suggests a new way to control the step size, that results in good convergence properties for a large range of input signal powers, that occur in many applications. In these paper, different algorithms based on the correlation form, information form and simplified versions of these are presented. The simplified form maintain the good convergence properties of the KLMS with slightly lower computational complexity. Finally to measure the performance of the KLMS algorithm we applied on speech signals.

Keywords: Adaptive filtering, LMS algorithm, Noise Cancellation, Speech Processing, Variable Step Size.

1. Introduction

In real time environment speech signals are corrupted by several forms of noise such as such as competing speakers, background noise, car noise, and also they are subject to distortion caused by communication channels; examples are room reverberation, low-quality microphones, etc. In all such situations extraction of high resolution signals is a key task. In this aspect filtering come in to the picture. Basically filtering techniques are broadly classified as non-adaptive and adaptive filtering techniques. In practical cases the statistical nature of all speech signals is non-stationary; as a result non-adaptive filtering may not be suitable. Speech enhancement improves the signal quality by suppression of noise and reduction of distortion. Speech enhancement has many applications; for example, mobile communications, robust speech recognition, low-quality audio devices, and hearing aids.

Many approaches have been reported in the literature to address speech enhancement. In recent years, adaptive filtering has become one of the effective and popular approaches for the speech enhancement. Adaptive filters permit to detect time varying potentials and to track the dynamic variations of the signals. Besides, they modify their behavior according to the input signal. Therefore, they can detect shape variations in the ensemble and thus they can obtain a better signal estimation. The first adaptive noise cancelling system at Stanford University was designed and built in 1965 by two students. Their work was undertaken as part of a term paper project for a course in adaptive systems given by the Electrical Engineering Department. Since 1965, adaptive noise cancelling has been successfully applied to a number of applications. Several methods have been reported so far in the literature to enhance the performance of speech processing systems; some of the most important ones are: Wiener filtering, LMS filtering [1], spectral subtraction [2]-[3], thresholding [4]-[5]. On the other side, LMS-based adaptive filters have been widely used for speech enhancement [6]–[8]. In a recent study, however, a steady state convergence analysis for the LMS algorithm with deterministic reference inputs showed that the steady-state weight vector is biased, and thus, the adaptive estimate does not approach the Wiener solution. To handle this drawback another strategy was considered for estimating the coefficients of the linear expansion, namely, the block LMS (BLMS) algorithm [9], in which the coefficient vector is updated only once every occurrence based on a block gradient estimation. A major advantage of the block, or the transform domain LMS algorithm is that the input signals are approximately uncorrelated. Recently Jamal Ghasemi et.al [10] proposed a new approach for speech enhancement based on eigenvalue spectral subtraction, in [11] authors describes usefulness of speech coding in voice banking, a new method for voicing detection and pitch estimation. This method is based on the spectral analysis of the speech multi-scale product [12].

In practice, LMS is replaced with its Normalized version, NLMS. In practical applications of LMS filtering, a key parameter is the step size. If the step size is large, the convergence rate of the LMS algorithm will be rapid, but the steady-state mean square error (MSE) will increase. On the other hand, if the step size is small, the steady state MSE will be small, but the convergence rate will be slow. Thus, the step size provides a tradeoff between the convergence rate and the steady-state MSE of the LMS algorithm. The Least Mean Squares (LMS) algorithm for adaptive filters has been extensively studied and tested in a broad range of applications [13]–[16]. In [13] and in [17] a relation between the Recursive Least Squares (RLS) and the Kalman filter [18] algorithm is determined, and in [13] the tracking convergence of the LMS, RLS and extended RLS algorithms, based on the Kalman filter, are compared. However, there is no link established between the Kalman filter and the LMS algorithm. In this paper we used the combination of LMS and Kalman filter to implement ANCs for speech enhancement. Further more some simplified versions of KLMS are also implemented. These are Information form KLMS (IKLMS) and Simplified IKLMS

(SIKLMS). Finally we applied these algorithms on speech signals to measure the performance, also signal to noise ratio improvement is measured and compared with conventional LMS adaptive filter.

2. Adaptive Algorithms

2.1. Basic Adaptive Filter Structure

Figure 1 shows an adaptive filter with a primary input that is noisy speech signal s_1 with additive noise n_1. While the reference input is noise n_2, which is correlated in some way with n_1. If the filter output is y and the filter error $e = (s_1+n_1)-y$, then

$$e^2 = (s_1 + n_1)^2 - 2y(s_1 + n_1) + y^2$$
$$= (n_1 - y)^2 + s_1^2 + 2 s_1 n_1 - 2y s_1. \quad (3)$$

Since the signal and noise are uncorrelated, the mean-squared error (MSE) is

$$E[e^2]=E[(n_1 - y)^2]+E[s_1^2] \quad (4)$$

Minimizing the MSE results in a filter error output that is the best least-squares estimate of the signal s_1. The adaptive filter extracts the signal, or eliminates the noise, by iteratively minimizing the MSE between the primary and the reference inputs. Minimizing the MSE results in a filter error output y that is the best least-squares estimate of the signal s_1.

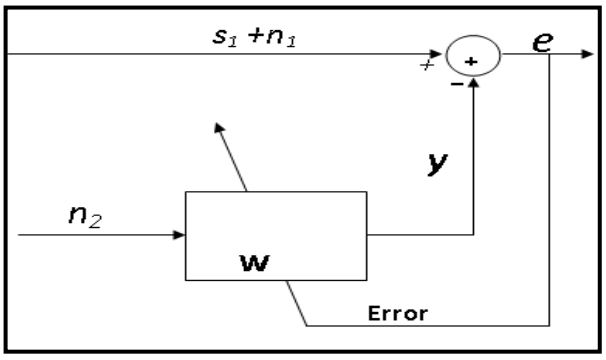


Figure 1: Adaptive Filter Structure.

2.2. Conventional LMS Algorithms

The LMS algorithm is a method to estimate gradient vector with instantaneous value. It changes the filter tap weights so that e(n) is minimized in the mean-square sense. The conventional LMS algorithm is a stochastic implementation of the steepest descent algorithm. It simply replaces the cost function $\xi(n) = E[e^2(n)]$ by its instantaneous coarse estimate.

The error estimation e(n) is

$$e(n) = \mathbf{d}(n) - \mathbf{w}(n)\,\mathbf{\Phi}(n) \quad (5)$$

Where $\mathbf{\Phi}(n)$ is input data sequence.

Coefficient updating equation is

$$\mathbf{w}(n+1) = \mathbf{w}(n) + \mu\,\mathbf{\Phi}(n)\,e(n), \quad (6)$$

Where μ is an appropriate step size to be chosen as $0 < \mu < \frac{2}{tr\,R}$ for the convergence of the algorithm.

2.3. Kalman Filter

The Kalman filter is based on a state space formulation of a continuous or discrete-time system. We will limit our discussion to discrete time. The system must be linear, but may be time variant. The Kalman filter gives an estimate of the state of the system given a set of outputs. For the case of Gaussian signals, and given the assumed linear model, the state estimate is optimum in the sense that it minimizes the norm of the difference between the estimate and the actual state. The system is described by the equations,

$$\mathbf{x}(n+1) = \mathbf{F}(n)\,\mathbf{x}(n) + \mathbf{n}(n) \quad (7)$$
$$\mathbf{z}(n) = \mathbf{H}^T(n)\,\mathbf{x}(n) + \mathbf{v}(n). \quad (8)$$

The system state vector is $\mathbf{x}(n)$, and the measured signal vector is given by $\mathbf{z}(n)$. The state transition matrix is $\mathbf{F}(n)$, $\mathbf{n}(n)$ is the state noise, $\mathbf{H}(n)$ is the observation matrix and $\mathbf{v}(n)$ is the measurement noise. The state noise and measurement noise are Gaussian random variables with known autocorrelation functions. The autocorrelation of the state noise is $\mathbf{Q}_{nn}(n)$ and of the measurement noise is $\mathbf{Q}_{vv}(n)$ as in,

$$Q_{vv}(n) = E[v(n)v^T(n)] \quad (9)$$
$$Q_{nn}(n) = E[n(n)n^T(n)] \quad (10)$$

The state estimate is given by $\bar{X}_{|n}(n)$ in Table 1. This table represents the Kalman filter algorithm. The estimate is calculated recursively based on the estimate at the previous time instant, $\bar{X}_{|\,n-1}(n-1)$ Along with the state estimate, the algorithm updates the state covariance matrix, $\sum_{x|n}(n)$.

Table 1: Kalman Filter.

Initialize

$$\bar{x}_{|\,0}(0) = \bar{x}_{0|\,0} \quad (11)$$
$$\sum_{x|0}(0) = \mathbf{\Sigma}_{x|\,0} \quad (12)$$

do a time update for n=0

Iterate from $n = 1$ to ...

$$\alpha(n) = z(n) - H^T(n)\bar{x}_{|n-1}(n) \quad (13)$$

Order update

$$K(n) = \sum_{x|n-1}(n)H(n) \quad (14)$$
$$(H^T(n)\ \sum_{x|n-1}(n)H(n) + Q_{vv}(n))^{-1}$$
$$\bar{x}_{|\,n}(n) = \bar{x}_{|\,n-1}(n) + K(n)\alpha(n) \quad (15)$$

$$\sum_{x|n}(n) = \sum_{x|n-1}(n) - K(n)H^T(n)\sum_{x|n-1}(n) \quad (16)$$

Time update

$$\bar{x}_{|\,n}(n+1) = F(n)\,\bar{x}_{|\,n}(n) \quad (17)$$
$$\sum_{x|n}(n+1) = F(n)\sum_{x|n}(n)F^T(n) + Q_{vv}(n) \quad (18)$$

2.3.1. Derivation of the Kalman Based LMS

The Kalman filter can be used in adaptive filtering by making a number of correspondences. The adaptive filtering problem is reformulated as a state estimation problem, where the state vector corresponds to the filter coefficients vector. Since the state estimate is the state that minimizes the square of the error at each coefficient, it will also minimize the

output error of the filter [18]. The optimal filter variation in time is modelled as a Markov model with white noise input, **n**(n), and state transition matrix, **F**(n) = λ **I** with λ close to one. The measured signal $d(n)$ is related to the state through the reference signal vector **u**(n) plus an additional measurement noise $v(n)$. This is summarized in Table 2.

Table 2: Correspondences from the Kalman Filter Variables to Adaptive Filter Variables (KLMS).

Kalman	Kalman LMS
z(n)	d(n)
H(n)	u(n)
$\bar{\boldsymbol{x}}_{\mid \mathbf{n}}(\mathbf{n})$	w(n)
$\sum_{\boldsymbol{x\mid n-1}}(\boldsymbol{n})$	$\sum_{w}(n)$
$\boldsymbol{Q_{nn}(n)}$	$Q_{nn}(n)$
$\boldsymbol{Q_{vv}(n)}$	$q_n(n)$
F**(n)**	λI

The resulting algorithm is then,

$$\alpha(n) = d(n) - u^T(n)w(n) \quad (19)$$

$$w(n+1) = \lambda w(n) + \lambda \frac{\sum_w(n)u(n)\alpha(n)}{u^T(n)\sum_w(n)u(n)+q_v(n)} \quad (20)$$

$$\sum_w(n+1) = \lambda^2 \sum_w(n) + -\lambda^2 \frac{\sum_w(n)u(n)u^T(n)\sum_w(n)}{u^T(n)\sum_w(n)u(n)+q_v(n)} + Q_{nn}(n) \quad (21)$$

The signal $\alpha(n)$ is the same as $e(n)$ and is used to be consistent with the Kalman filter notation. The variance matrix $\Sigma_w(n)$ can be made diagonal by carefully selecting the state noise autocorrelation matrix $\mathbf{Q}_{nn}(n)$ at each iteration. More, this can be done without changing the state noise total power, tr{$\mathbf{Q}_{nn}(n)$}, where tr{} stands for the trace of the matrix.

The procedure is not feasible if the state noise is to low.
To do this one simply makes $\mathbf{\Sigma}_w(n) = \sigma_w^2(n)\,\mathbf{I}$ and tr{$\mathbf{Q}_{nn}(n)$} = $N\,q_n(n)$ and apply the trace operator to (21). The resulting algorithm is the Kalman based LMS algorithm (KLMS) and is represented in Table 3. Note that tr{$\mathbf{u}(n)\ \mathbf{u}(n)^T$} = $\mathbf{u}(n)^T\mathbf{u}(n)$. The actual algorithm presented in Table 3 has been modified to allow complex signals. Namely, in the calculation of the power and in the coefficients update, $\mathbf{u}(n)^*$, the conjugate of $\mathbf{u}(n)$, is used in its place.

Table 3: Normalized LMS Based on the Kalman Filter, KLMS

Initialize

$$w(0) = w_0 \quad (22)$$

$$\sigma_w^2(o) = \sigma_{w0}^2 \quad (23)$$

Iterate from $n=0$ to ...

$$P(n) = u^H(n)u(n) \quad (24)$$

$$\alpha(n) = d(n) - u^T(n)w(n \quad (25)$$

$$w(n+1) = w(n) + \frac{u(n)^*\alpha(n)}{P(n)+q_v(n)/\sigma_w^2(n)} \quad (26)$$

$$\sigma_w^2(n+1) = \sigma_w^2(n)(1 - \frac{P(n)/N}{P(n)+q_v(n)/\sigma_w^2(n)}) + q_v(n) \quad (27)$$

2.3.2. Choosing the State Noise Variance

The model for the state variation is,

$$w_j(n+1) = \lambda w_j(n) + n_j(n). \quad (28)$$

Each coefficient corresponds to a low frequency signal, with time constant given by $\tau = T/\ln(\lambda)$ where T is the sampling period. This can be approximated by $\tau = T/(1-\lambda)$ if λ is close to one. So one has, $\lambda \approx (1 - T/\tau)$. The variance of each coefficient is easily calculated as,

$$\sigma_w^2 = \frac{q_n}{1-\lambda^2} \quad (29)$$

This should be equal to the value chosen to initialize the algorithm $\sigma_w^2 = \sigma_{w0}^2$. It follows that the state noise can be chosen as,

$$q_n = \sigma_{w0}^2(1 - \lambda^2 \approx 2\sigma_{w0}^2 \frac{T}{\tau}) \quad (30)$$

where the last approximation is valid for large τ , where τ is the time constant of the under laying model, as previously discussed.

2.4. Information form Kalman Based LMS Algorithm

If the state noise is low or zero (21) can be written as,

$$\sum_w^{-1}(n+1) = \sum_w^{-1}(n) + \frac{u(n)u^T(n)}{q_v(n)} \quad (31)$$

The matrix $\sum_w^{-1}(n+1)$ can be approximated by a diagonal matrix if the reference signal autocorrelation is narrow. Doing this and applying the trace operator results,

$$\sigma_w^{-2}(n+1) = \sum_w^{-1}(n) + \frac{P(n)}{Nq_v(n)} \quad (32)$$

by defining the total power up to (but not counting) time n, $P_T(n)$, by the equation,

$$P_T(n+1) = P_T(n) + P(n) \quad (33)$$

one can prove that,

$$\sigma_w^{-2}(n) = \frac{P_T(n)+Nq_v(n)/2\sigma_{w0}^2}{Nq_v(n)} \quad (34)$$

with, $P_T(0) = 0$, resulting in the algorithm presented in Table 4. Note that this algorithm is equivalent to the KLMS for the case $N = 1$.

Table 4: Information form Kalman Based LMS (IKLMS)

Initialize

$$w(0) = w_0 \quad (35)$$

$$P_T(0) = \sigma_{w0}^2 \quad (36)$$

Iterate from $n=0$ to ...

$$\alpha(n) = d(n) - u^T(n)w(n) \quad (37)$$

$$P(n) = u^H(n)u(n) \quad (38)$$

$$w(n+1) = w(n) + \frac{u(n)^*\alpha(n)}{P(n)+P_T(n)/N+q_v/\sigma_{w0}^2} \quad (39)$$

$$P_T(n+1) = P_T(n) + P(n) \quad (40)$$

2.5. Simplification of the Algorithm

If one is not interested in the initial convergence, then the algorithm in Table III can be simplified. The coefficients estimation error standard deviation $\sigma_w^2(n)$ converges to a steady state value, resulting that $q_v(n)/\sigma_w^2(n)$ converges to,

$$q_v(\infty)/\sigma_w^2(\infty) = \frac{P}{2}(-1+\sqrt{1+\frac{4q_v}{NPq_v}}) \quad (41)$$

This can be used in place of $q_v(n)/\sigma_w^2(n)$. The value of the state noise can be calculated as in (30). The algorithm in IV can also be simplified. The time varying quantity $P_T(n+1)$ is replaced by an estimate of its value at time M, resulting in,

$$w(n+1) = w(n) + \frac{u(n)^*\alpha(n)}{(\frac{N+M-1}{N})u^H(n)u(n)+q_v/\sigma_{w0}^2} \quad (42)$$

We call this algorithm the Simplified Information Form Kalman LMS (SIKLMS). The quantity M is the step sample time.

3. Simulation Results

To show that KLMS and SIKLMS algorithms are appropriate for speech enhancement we have used real speech signals with noise. In the figure *number of samples* is taken on *x-axis* and *amplitude* is taken on *y-axis*. The convergence curves for various algorithms is shown in Figure 2. In order to test the convergence performance we have simulated a sudden noise spike at 4000th sample. From the figure it is clear that the performance of the implemented KLMS algorithms is better than the conventional LMS, NLMS, IKLMS and SIKLMS algorithm. To prove the concept of filtering we have considered five speech samples contaminated with various real noises. These noises are random noise, high voltage murmuring, battle field noise, helicopter noise and crane noise. The noisy speech signal is given as in put to the adaptive filter structure shown in Figure 1, signal somewhat correlated with noise is given as reference signal. As the number of iterations increases error decreases and clean signal can be extracted from the output of the filter. These simulation results are shown in Figures 3, 4, 5, 6 and 7. To evaluate the performance of the algorithms SNRI is measured and tabulated in Tables I, II, III, IV and V.

4. Conclusion

In this paper the problem of noise removal from speech signals using Variable Step Size based adaptive filtering is presented. For this, the same formats for representing the data as well as the filter coefficients as used for the LMS algorithm were chosen. As a result, the steps related to the filtering remains unchanged. The proposed treatment, however exploits the modifications in the weight update formula for all categories to its advantage and thus pushes up the speed over the respective LMS-based realizations. Our simulations, however, confirm that the ability of SIKLMS and IKLMS algorithms is better than conventional LMS and KLMS algorithms in terms of computational complexity, where as KLMS is better than other in terms if SNRI and convergence rate. But the difference in SNRI between KLMS and IKLMS, SIKLMS is little when compared to computational complexity.Hence these algorithms are acceptable for all practical purposes.

References

[1] B. Widrow, J. Glover, J. M. McCool, J. Kaunitz, C. S. Williams, R. H.Hearn, J. R. Zeidler, E. Dong, and R. Goodlin,"Adaptive noise cancelling: Principles and applications ", Proc. IEEE, vol. 63, pp.1692-1716, Dec. 1975.
[2] B. L. Sim, Y. C. Tong, J. S. Chang and C. T. Tan, "A parametric formulation of the generalized spectral subtraction method," IEEE Trans. On Speech and Audio Processing, vol. 6, pp. 328-337, 1998.
[3] I. Y. Soon, S. N. Koh, and C. K. Yeo, "Noisy speech enhancement using discrete cosine transform," Speech Communication, vol. 24, pp. 249-257, 1998.
[4] H. Sheikhzadeh, and H. R. Abutalebi, "An improved wavelet-based speech enhancement system," Proc. of the Eurospeech, 2001.
[5] S. Salahuddin, S. Z. Al Islam, M. K. Hasan, M. R. Khan, "Soft thresholding for DCT speech enhancement," Electron. Letters, vol. 38, no.24, pp. 1605-1607, 2002.
[6] J. Homer, "Quantifying the convergence speed of LMS adaptive filter with autoregressive inputs," Electronics Letters, vol. 36, no. 6, pp. 585– 586, March 2000.
[7] H. C. Y. Gu, K. Tang and W. Du, "Modifier formula on mean square convergence of LMS algorithm," Electronics Letters, vol. 38, no. 19, pp. 1147 –1148, Sep 2002.
[8] M. Chakraborty and H. Sakai, "Convergence analysis of a complex LMS algorithm with tonal reference signals," IEEE Trans. on Speech and Audio Processing, vol. 13, no. 2, pp. 286 – 292, March 2005.
[9] S. Olmos , L. Sornmo and P. Laguna, ``Block adaptive filter with deterministic reference inputs for event-related signals:BLMS and BRLS," IEEE Trans. Signal Processing, vol. 50, pp. 1102-1112, May.2002.
[10] Jamal Ghasemi and Mohammad Reza Karami Mollaei, "A New Approach for Speech Enhancement Based On Eigenvalue Spectral Subtraction", Signal Processing: An International Journal, vol. 3, Issue. 4, pp. 34-41.
[11] Mohamed Anouar Ben Messaoud, Aïcha Bouzid and Noureddine Ellouze," A New Method for Pitch Tracking and Voicing Decision Based on Spectral Multi-scale Analysis", Signal Processing: An International Journal, vol. 3, Issue. 5, pp. 144-152.
[12] M.Satya Sai Ram, P. Siddaiah and M. Madhavi Latha," USEFULNESS OF SPEECH CODING IN VOICE BANKING", Signal Processing: An International Journal, vol. 3, Issue. 4, pp. 42-52.
[13] S. Haykin, *Adaptive Filter Theory*. Prentice-Hall, Inc., 1996.
[14] J. Homer, "Quantifying the convergence speed of LMS adaptive FIR filter with autoregressive inputs," *Electronics Letters*, vol. 36, no. 6, pp. 585– 586, March 2000.
[15] Y. Gu, K. Tang, H. Cui, and W. Du, "Modifier formula on mean square convergence of LMS algorithm," *Electronics Letters*, vol. 38, no. 19, pp. 1147 – 1148, September 2002.
[16] M. Chakraborty and H. Sakai, "Convergence analysis of a complex LMS algorithm with tonal reference signals," *IEEE Trans. Speech Audio Process.*, vol. 13, no. 2, pp. 286 – 292, March 2005.
[17] A. Sayed and T. Kailath, "A state-space approach to adaptive RLS filtering," *IEEE Signal Process. Mag.*, vol. 11, no. 3, pp. 18 – 60, July 1994.
[18] B. D. O. Anderson, *Optimal Filtering*. Dover Publications, 2005.

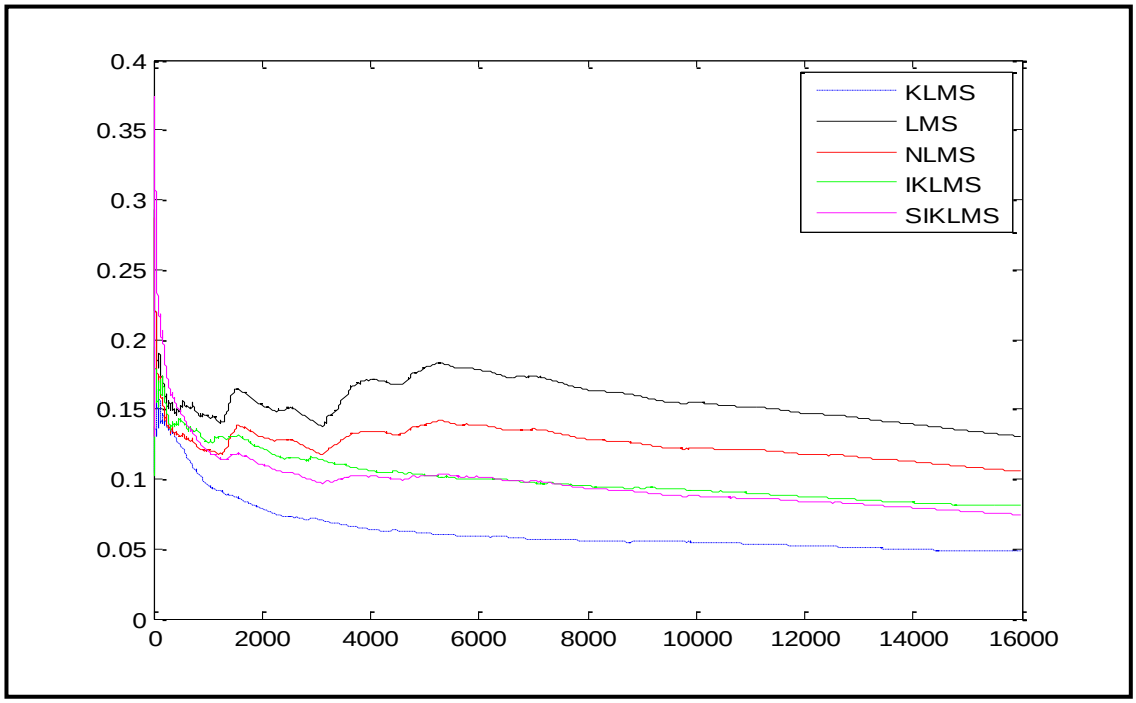


Figure 2: Convergence Characteristics of Various Algorithms.

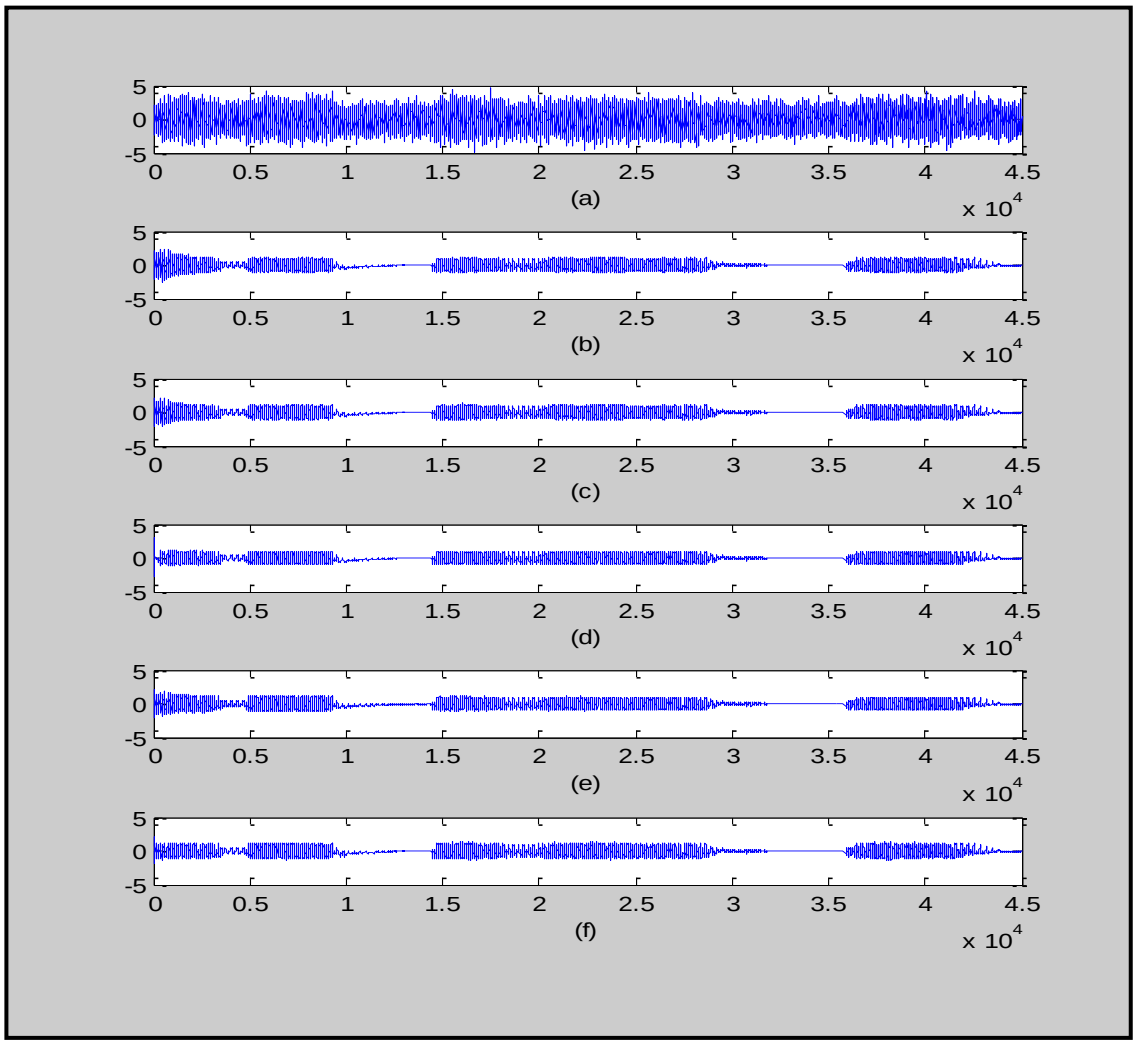


Figure 3: Typical filtering results of random noise removal (a) Speech Signal with real noise, (b) recovered signal using LMS algorithm, (c) recovered signal using NLMS algorithm, (d) recovered signal using KLMS algorithm, (e) recovered signal using IKLMS algorithm, (f) recovered signal using SIKLMS algorithm.

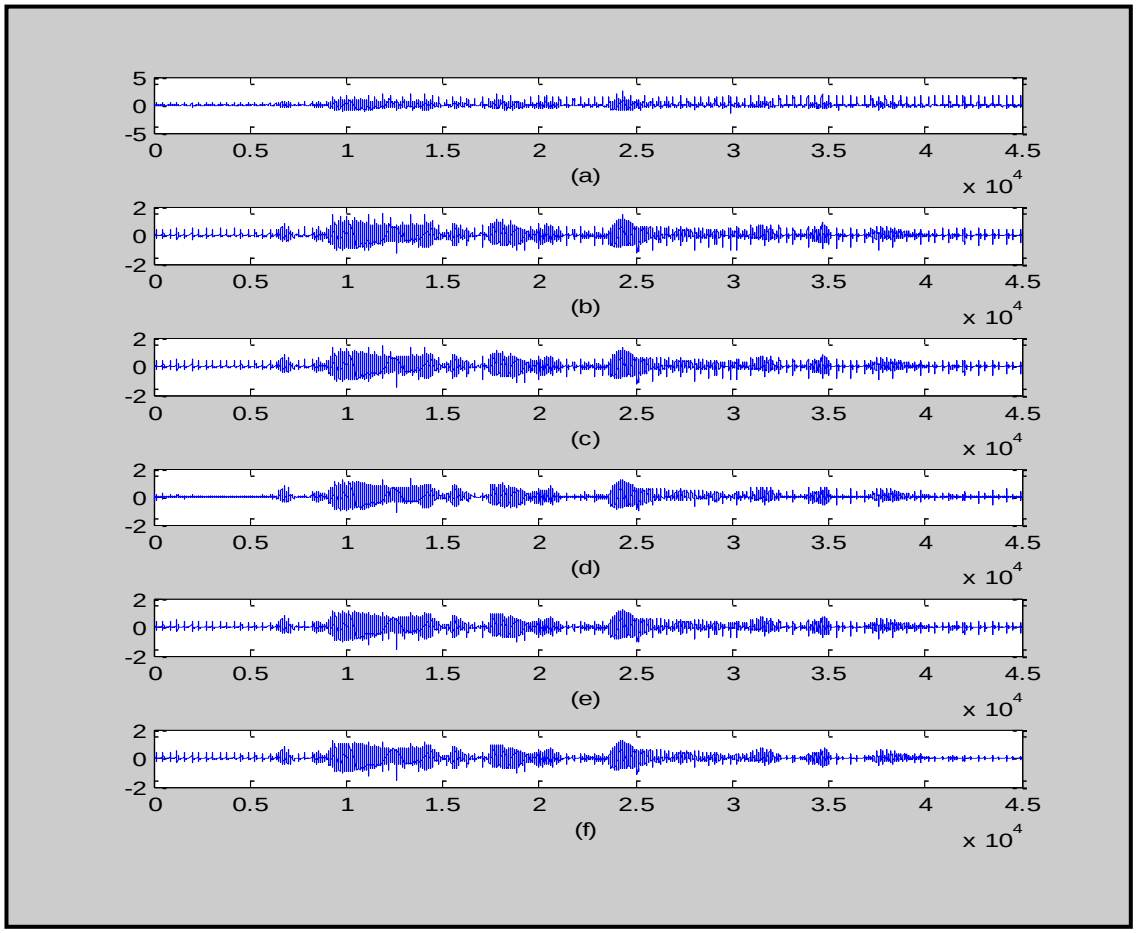


Figure 4: Typical filtering results of high voltage murmuring removal (a) Speech Signal with real noise, (b) recovered signal using LMS algorithm, (c) recovered signal using NLMS algorithm, (d) recovered signal using KLMS algorithm, (e) recovered signal using IKLMS algorithm, (f) recovered signal using SIKLMS algorithm.

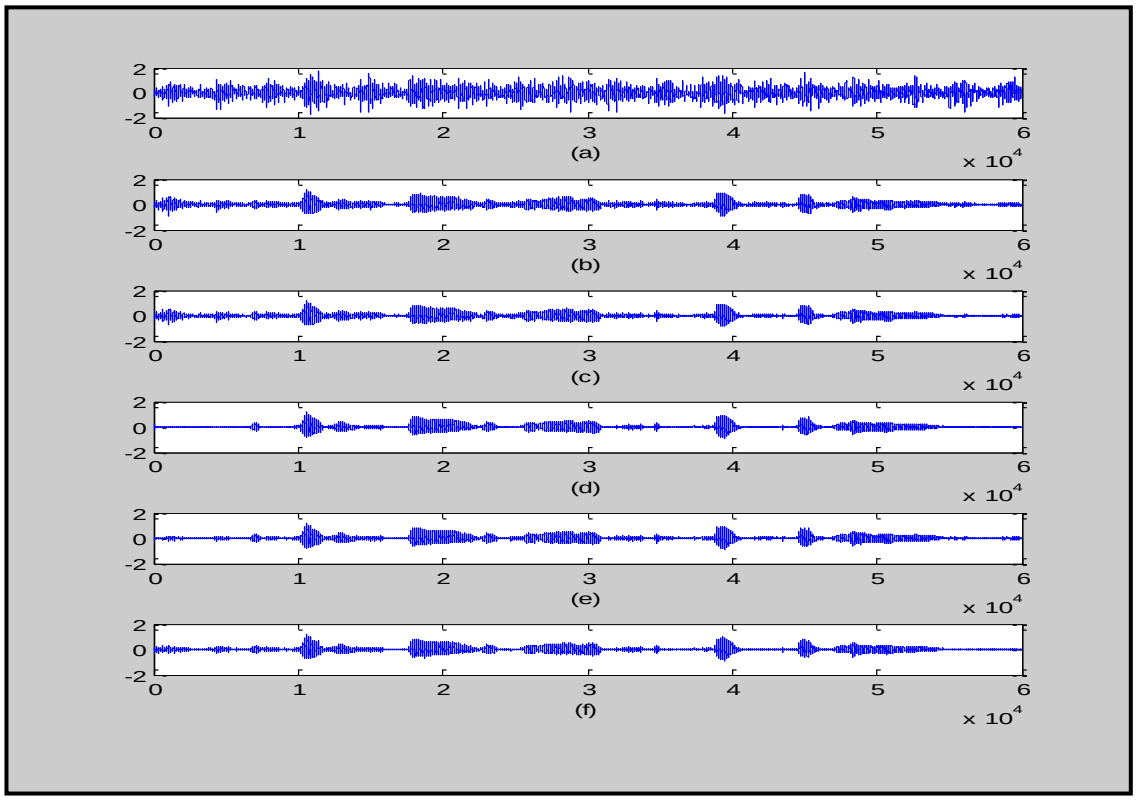


Figure 5: Typical filtering results of helicopter noise removal (a) Speech Signal with real noise, (b) recovered signal using LMS algorithm, (c) recovered signal using NLMS algorithm, (d) recovered signal using KLMS algorithm, (e) recovered signal using IKLMS algorithm, (f) recovered signal using SIKLMS algorithm.

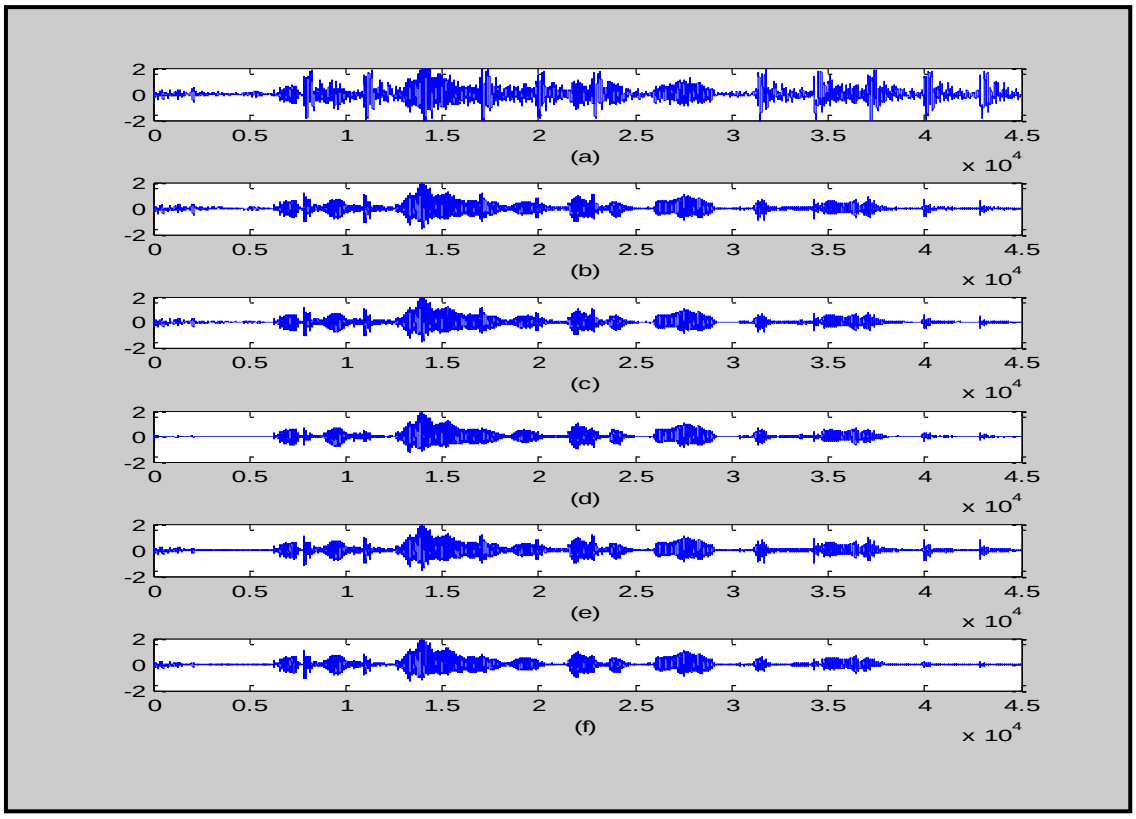


Figure 6: Typical filtering results of battle field noise removal (a) Speech Signal with real noise, (b) recovered signal using LMS algorithm, (c) recovered signal using NLMS algorithm, (d) recovered signal using KLMS algorithm, (e) recovered signal using IKLMS algorithm, (f) recovered signal using SIKLMS algorithm.

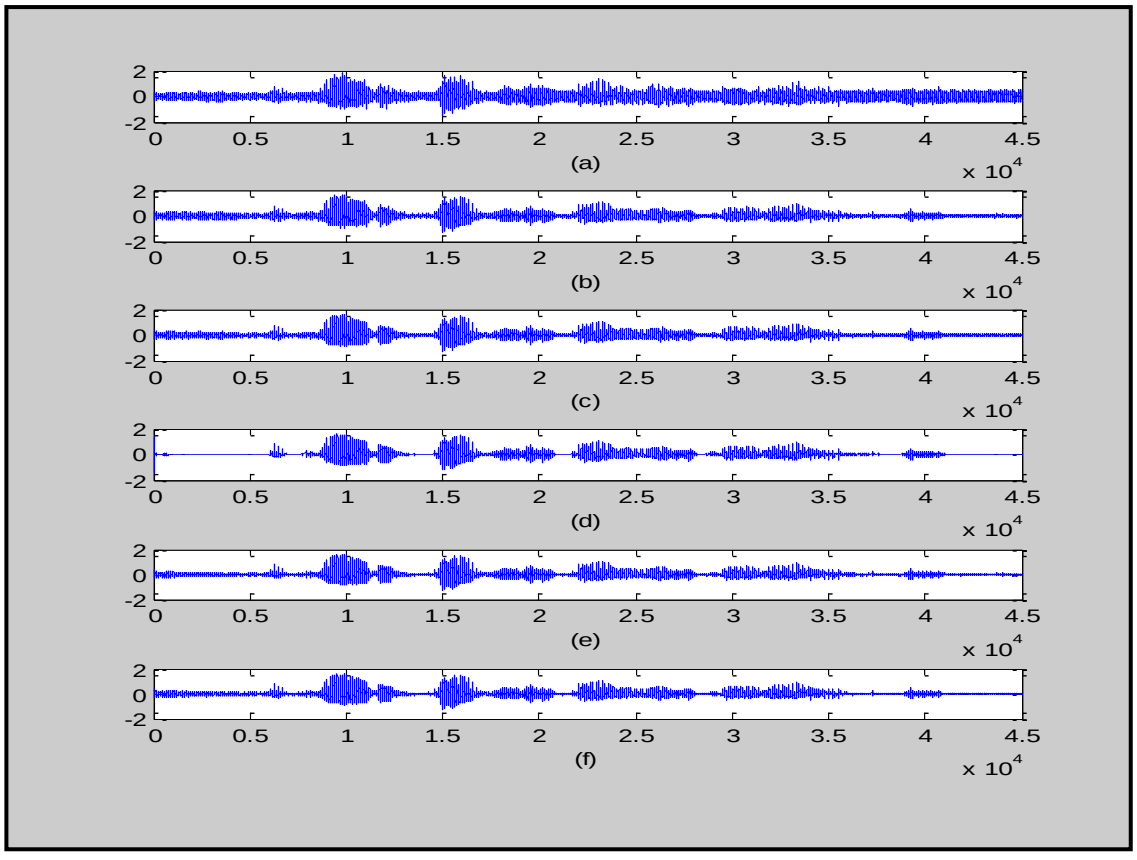


Figure 7: Typical filtering results of crane noise removal (a) Speech Signal with real noise, (b) recovered signal using LMS algorithm, (c) recovered signal using NLMS algorithm, (d) recovered signal using KLMS algorithm, (e) recovered signal using IKLMS algorithm, (f) recovered signal using SIKLMS algorithm.

Sl.No	Sample No	Before filtering	LMS		NLMS		KLMS		IKLMS		SIKLMS	
			After	Imp.	After	Imp.	After	Imp.	After	Imp.	After	Imp.
1	I	-2.913	7.4744	10.3874	8.2001	11.1131	10.6238	13.5368	8.7554	11.6684	8.7428	11.6558
2	II	-7.0875	2.6889	9.7764	3.5997	10.6872	7.5682	14.6557	6.0778	13.1653	5.6322	12.4095
3	III	-6.6262	3.1348	9.761	4.0368	10.663	7.9222	14.5484	6.5001	13.1263	5.9827	12.6089
4	IV	-8.6313	1.7558	10.3871	2.6707	11.302	6.5182	15.1495	5.1424	13.7737	4.7525	13.3838
5	V	-6.9159	2.8605	9.7764	3.7738	10.6897	7.651	14.5669	5.4121	12.328	5.757	12.6729
Average Improvement			10.01766		10.891		14.49146		12.81234		12.54618	

Table 1: SNR Contrast for Random noise removal.

Sl.No	Sample No	Before filtering	LMS		NLMS		KLMS		IKLMS		SIKLMS	
			After	Imp.	After	Imp.	After	Imp.	After	Imp.	After	Imp.
1	I	4.3536	8.6414	4.2878	9.1469	4.7933	10.6632	6.3096	9.3742	5.0206	9.8448	5.4912
2	II	-0.54077	3.7539	4.29467	4.3198	4.86057	9.1212	9.66197	5.7078	6.24857	6.282	6.82277
3	III	-0.07949	4.3428	4.422293	4.8245	4.903993	7.5772	7.656693	5.9704	6.049893	6.5194	6.598893
4	IV	-0.41585	2.962	3.37785	3.5832	3.99905	9.3965	9.81235	4.9095	5.32535	5.4285	5.84435
5	V	1.3917	4.5746	3.1829	5.2853	3.8936	14.0313	12.6396	6.0645	4.6728	6.7319	5.3402
Average Improvement			3.9131026		4.4901026		9.2160426		5.4634426		6.0194826	

Table 2: SNR Contrast for High voltage murmuring removal.

Sl.No	Sample No	Before filtering	LMS		NLMS		KLMS		IKLMS		SIKLMS	
			After	Imp.	After	Imp.	After	Imp.	After	Imp.	After	Imp.
1	I	4.621	9.2021	4.5811	9.8872	5.2662	10.7157	6.0947	10.1455	5.5245	9.7827	5.1617
2	II	-0.2734	4.3164	4.5898	5.2809	5.5543	8.6715	8.9449	6.4597	6.7331	6.3532	6.6266
3	III	0.18787	4.7884	4.60053	5.8061	5.61823	9.1652	8.97733	6.9943	6.80643	7.0431	6.85523
4	IV	-2.1688	3.1101	5.2789	4.0095	6.1783	10.3226	12.4914	4.6602	6.829	5.1163	7.2851
5	V	-0.10189	4.5081	4.60999	5.4251	5.52699	8.4963	8.59819	5.8726	5.97449	6.3622	6.46409
Average Improvement			4.732064		5.628804		9.020044		6.373504		6.478544	

Table 3: SNR Contrast for Crane noise removal.

Sl.No	Sample No	Before filtering	LMS		NLMS		KLMS		IKLMS		SIKLMS	
			After	Imp.	After	Imp.	After	Imp.	After	Imp.	After	Imp.
1	I	-0.4285	4.6733	5.1018	5.8808	6.3093	8.3735	8.802	7.2711	7.6996	6.639	7.0675
2	II	-3.562	2.6637	6.2257	3.2592	6.8212	9.2386	12.8006	4.0723	7.6343	5.4378	8.9998
3	III	-3.1007	3.0572	6.1579	3.5837	6.6844	7.2519	10.3526	4.4229	7.5236	5.1077	8.2084
4	IV	-5.1435	2.5601	7.7036	3.042	8.1855	9.4467	14.5902	6.0676	11.2111	5.3656	10.5091
5	V	-3.3905	3.803	7.1935	4.3376	7.7281	7.8091	11.1996	4.2185	7.609	6.2536	9.6441
Average Improvement			6.4765		7.1457		11.549		8.33552		8.88578	

Table 4: SNR Contrast for Gun noise removal.

Sl.No	Sample No	Before filtering	LMS		NLMS		KLMS		IKLMS		SIKLMS	
			After	Imp.	After	Imp.	After	Imp.	After	Imp.	After	Imp.
1	I	1.3799	5.583	4.2031	6.6885	5.3086	10.1614	8.7815	7.7909	6.411	7.0215	5.6416
2	II	-2.5454	1.404	3.9494	2.5186	5.064	7.1994	9.7448	5.3638	7.9092	5.8853	8.4307
3	III	-2.0841	1.9504	4.0345	3.0563	5.1404	9.3233	11.4074	5.7652	7.8493	6.2045	8.2886
4	IV	-3.6722	2.9146	6.5868	3.7377	7.4099	9.4879	13.1601	6.1745	9.8467	6.2762	9.9484
5	V	-1.5821	4.4353	6.0174	5.2948	6.8769	8.7096	10.2917	5.3554	6.9375	6.6555	8.2376
Average Improvement			4.95824		5.95996		10.6771		7.79074		8.10938	

Table 5: SNR Contrast for Helicopter noise removal.

Performance Analysis of Robust Adaptive Algorithms in Speech Processing

M. Ajay Kumar, K. Prameela, Md Zia Ur Rahman *, T.Srikantha Reddy[1] and Dr. B V Rama Mohana Rao

Dept. of E.C.E., Narasaraopeta Engg. College, Narasaraopeta, A.P., India
E-mail : mdzr_5@ieee.org,
** Corresponding Author. [1] Dept. of E.C.E., Nalanda Institute of Technology, Sattenapalli, A.P., India*

Abstract **-** The aim of this paper is to implement various adaptive noise cancellers (ANC) for speech enhancement based on gradient descent approach, namely the least-mean square (LMS) algorithm and then enhanced to variable step size strategy. In practical application of the LMS algorithm, a key parameter is the step size. As is well known, if the step size is large, the convergence rate of the LMS algorithm will be rapid, but the steady-state mean square error (MSE) will increase. On the other hand, if the step size is small, the steady state MSE will be small, but the convergence rate will be slow. Thus, the step size provides a trade-off between the convergence rate and the steady-state MSE of the LMS algorithm. An intuitive way to improve the performance of the LMS algorithm is to make the step size variable rather than fixed, that is, choose large step size values during the initial convergence of the LMS algorithm, and use small step size values when the system is close to its steady state, which results in Variable Step Size LMS (VSSLMS) algorithms. By utilizing such an approach, both a fast convergence rate and a small steady-state MSE can be obtained. By using this approach various forms of VSSLMS algorithms are implemented. These are robust variable step-size LMS (RVSSLMS) algorithm providing fast convergence at early stages of adaptation and modified robust variable step-size LMS (MRVSSLMS) algorithm. The performance of these algorithms is compared with conventional LMS and Kowngs VSSLMS algorithm. Finally we applied these algorithms on speech enhancement application. Simulation results confirms that the implemented RVSSLMS and MRVSSLMS are superior than conventional algorithms in terms of convergence rate and signal to noise ratio improvement (SNRI).

Keywords: Adaptive filtering, LMS algorithm,Noise Cancellation, Speech Processing, Variable Step Size.

1. Introduction

In real time environment speech signals are corrupted by several forms of noise such as such as competing speakers, background noise, car noise, and also they are subject to distortion caused by communication channels; examples are room reverberation, low-quality microphones, etc. In all such situations extraction of high resolution signals is a key task. In this aspect filtering come in to the picture. Basically filtering techniques are broadly classified as non-adaptive and adaptive filtering techniques. In practical cases the statistical nature of all speech signals is non-stationary; as a result non-adaptive filtering may not be suitable. Speech enhancement improves the signal quality by suppression of noise and reduction of distortion. Speech enhancement has many applications; for example, mobile communications, robust speech recognition, low-quality audio devices, and hearing aids.

Many approaches have been reported in the literature to address speech enhancement. In recent years, adaptive filtering has become one of the effective and popular approaches for the speech enhancement. Adaptive filters permit to detect time varying potentials and to track the dynamic variations of the signals. Besides, they modify their behavior according to the input signal. Therefore, they can detect shape variations in the ensemble and thus they can obtain a better signal estimation. The first adaptive noise cancelling system at Stanford University was designed and built in 1965 by two students. Their work was undertaken as part of a term paper project for a course in adaptive systems given by the Electrical Engineering Department. Since 1965, adaptive noise cancelling has been successfully applied to a number of applications. Several methods have been reported so far in the literature to enhance the performance of speech processing systems; some of the most important ones are: Wiener filtering, LMS filtering [1], spectral subtraction [2]-[3], thresholding [4]-[5]. On the other side, LMS-based adaptive filters have been widely used for speech enhancement [6]–[8]. In a recent study, however, a steady state convergence analysis for the LMS algorithm with deterministic reference inputs showed that the steady-state weight vector is biased, and thus, the adaptive estimate does not approach the Wiener solution. To handle this drawback another strategy was considered for estimating the coefficients of the linear expansion, namely, the block LMS (BLMS) algorithm [9], in which the coefficient vector is updated only once every occurrence based on a block gradient estimation. A major advantage of the block, or the transform domain LMS algorithm is that the input signals are approximately uncorrelated. Recently Jamal Ghasemi et.al [10] proposed a new approach for speech enhancement based on eigenvalue spectral subtraction, in [11] authors describes usefulness of speech coding in voice banking, a new method for voicing detection and pitch estimation. This method is based on the spectral analysis of the speech multi-scale product [12].

In practice, LMS is replaced with its Normalized version, NLMS. In practical applications of LMS filtering, a key parameter is the step size. If the step size is large, the convergence rate of the LMS algorithm will be rapid, but the steady-state mean square error (MSE) will increase. On the other hand, if the step size is small, the steady state MSE will be small, but the convergence rate will be slow. Thus, the step size provides a tradeoff between the convergence rate and the steady-state MSE

of the LMS algorithm. The performance of the LMS algorithm may be improved by making the step size variable rather than fixed. The resultant approach with variable step size is known as variable step size LMS (VSSLMS) algorithm [13]. By utilizing such an approach, both a fast convergence rate and a small steady-state MSE can be obtained. Many VSSLMS algorithms are proposed during recent years [14]-[17]. In this paper, we considered the problem of noise cancellation in speech signals by effectively modifying and extending the framework of [1], using VSSLMS algorithms mentioned in [14]-[17]. For that, we carried out simulations on various real time speech signals contaminated with real noise. The simulation results show that the performances of the VSSLMS based algorithms are comparable with LMS counterpart to eliminate the noise from speech signals. Recently in [18] Karthik et.al demonstrated speech enhancement using variable step size LMS (VSSLMS) algorithms, in [19], [20] Rahman et.al presented speech filtering using variable step size least mean fourth based treatment and unbiased and normalized adaptive filtering techniques.

2. Adaptive Algorithms

2.1. Basic Adaptive Filter Structure

Figure 1 shows an adaptive filter with a primary input that is noisy speech signal s_1 with additive noise n_1. While the reference input is noise n_2, which is correlated in some way with n_1. If the filter output is y and the filter error $e = (s_1+n_1)-y$, then

$$e^2 = (s_1 + n_1)^2 - 2y(s_1 + n_1) + y^2$$
$$= (n_1 - y)^2 + s_1^2 + 2 s_1 n_1 - 2y s_1. \quad (1)$$

Since the signal and noise are uncorrelated, the mean-squared error (MSE) is

$$E[e^2]=E[(n_1 - y)^2]+E[s_1^2] \quad (2)$$

and

$$(3)$$

Minimizing the MSE results in a filter error output that is the best least-squares estimate of the signal s_1. The adaptive filter extracts the signal, or eliminates the noise, by iteratively minimizing the MSE between the primary and the reference inputs. Minimizing the MSE results in a filter error output y that is the best least-squares estimate of the signal s_1.

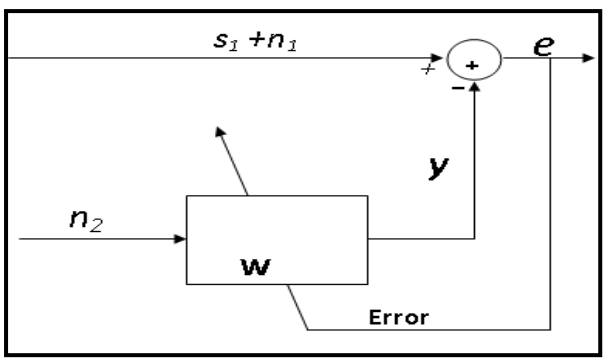


Figure 1: Adaptive Filter Structure.

2.2. Conventional LMS Algorithms

The LMS algorithm is a method to estimate gradient vector with instantaneous value. It changes the filter tap weights so that e(n) is minimized in the mean-square sense. The conventional LMS algorithm is a stochastic implementation of the steepest descent algorithm. It simply replaces the cost function $\xi(n) = E[e^2(n)]$ by its instantaneous coarse estimate.

The error estimation e(n) is

$$e(n) = \mathbf{d}(n) - \mathbf{w}(n)\,\mathbf{\Phi}(n) \quad (3)$$

Where $\mathbf{\Phi}(n)$ is input data sequence.

Coefficient updating equation is

$$\mathbf{w}(n+1) = \mathbf{w}(n) + \mu\,\mathbf{\Phi}(n)\,e(n), \quad (4)$$

Where μ is an appropriate step size to be chosen as $0 < \mu < \frac{2}{tr\,R}$ for the convergence of the algorithm.

2.3. Kwong's VSSLMS algorithm

The LMS type adaptive algorithm is a gradient search algorithm which computes a set of weights w_k that seeks to minimize $E(d_k - X^T_k W_k)$ The algorithm is of the form

$$W_{k+1} = W_k + \mu_k X_k \epsilon_k$$

Where $\epsilon_k = d_k + X^T_k W^*_k$

and μ_k is the step size. In the standard LMS algorithm μ_k is a constant. In this μ_k is time varying with its value determined by the number of sign changes of an error surface gradient estimate. Here the new variable step size or VSS algorithm, for adjusting the step size μ_k yields :

$$\mu'_{k+1} = \alpha\mu_k + \gamma\epsilon^2_k \qquad 0 < \alpha < 1,\ \gamma > 0$$

$$\mu_{k+1} = \begin{cases} \mu_{max} & \text{if } \mu'_{k+1} > \mu_{max} \\ \mu_{min} & \text{if } \mu'_{k+1} < \mu_{min} \\ \mu'_{k+1} & \text{otherwise} \end{cases}$$

where $0 < \mu_{min} < \mu_{max}$. The initial step size μ_0 is usually taken to be μ_{max}, although the algorithm is not sensitive to the choice. The step size μ_k , is always positive and is controlled by the size of the prediction error and the parameters α and γ. Intuitively speaking, a large prediction error increases the step size to provide faster tracking. If the prediction error decreases, the step size will be decreased to reduce the misadjustment. The constant μ_{max} is chosen to ensure that the mean-square error (MSE) of the algorithm remains bounded. A sufficient condition for μ_{max}

$$\mu_{max} \leq 2/(3\ tr\ (R)) \quad (6)$$

μ_{min} is chosen to provide a minimum level of tracking ability. Usually, μ_{min} will be near the value of μ that would be chosen for the fixed step size (FSS) algorithm.

α must be chosen in the range (0, 1) to provide exponential forgetting.

2.4. Robust Variable Step-Size LMS (RVSSLMS) algorithm

A number of time-varying step-size algorithms have been proposed to enhance the performance of the conventional LMS algorithm. Simulation results comparing the proposed algorithm to current variable step-size algorithms clearly indicate its superior performance for cases of stationary environments. For non-stationary environments, our algorithm performs as well as other variable step-size algorithms in providing performance equivalent to that of the regular LMS algorithm [17].

The adaptation step size is adjusted using the energy of the instantaneous error. The weight update recursion is given by

$$w(n+1)= w(n)+\mu(n)e(n)X(n)$$

And updated step-size equation is

$$\mu(n+1)=\alpha\mu(n)+\gamma e^2(n) \quad (7)$$

where $0<\alpha<1, \gamma>0$, and $\mu(n+1)$ is set to or when it falls below or above these lower and upper bounds, respectively. The constant μ_{max} is normally selected near the point of instability of the conventional LMS to provide the maximum possible convergence speed. The value of μ_{max} is chosen as a compromise between the desired level of steady state misadjustment and the required tracking capabilities of the algorithm. The parameter γ controls the convergence time as well as the level of misadjustment of the algorithm. At early stages of adaptation, the error is large, causing the step size to increase, thus providing faster convergence speed. When the error decreases, the step size decreases, thus yielding smaller misadjustment near the optimum. However, using the instantaneous error energy as a measure to sense the state of the adaptation process does not perform as well as expected in the presence of measurement noise. The output error of the identification system is

$$e(n)=d(n)-X^T(n)W(n) \quad (8)$$

where d(n) is the desired signal is given by

$$d(n)=X^T(n)W^*(n)+\xi(n) \quad (9)$$

$\xi(n)$ is a zero-mean independent disturbance, and $W^*(n)$ is the time-varying optimal weight vector. Substituting (8) and (9) in the step-size recursion, we get

$$\mu(n+1)=\alpha\mu(n)+\gamma V^T(n)X(n)X^T(n)V(n)+\gamma\xi^2(n)-2\gamma\xi(n)V^T(n)X(n) \quad (10)$$

Where $V(n)=W(n)-W^*(n)$ is the weight error vector. The input signal autocorrelation matrix, which is defined as $R=E\{X(n)X^T(n)\}$, can be expressed as $R=Q\Lambda Q^T$, where Λ is the matrix of eigen values, and Q is the model matrix of R. using $\tilde{V}(n)=Q^TV(n)$ and $X'(n) = Q^TX(n)$, then the statistical behavior of $\mu(n+1)$ is determined.

$$E\{\mu(n+1)\}=\alpha E\{\mu(n)\}+\gamma(E\{\xi^2(n)\}+E\{\tilde{V}^T(n)\Lambda\tilde{V}(n)\})$$

where we have made use of the common independence assumption of $\tilde{V}(n)$ and $X'(n)$. Clearly, the term $E\{\tilde{V}^T(n)\Lambda X'(n)\}$ influences the proximity of the adaptive system to the optimal solution, and $\mu(n+1)$ is adjusted accordingly. However, due to the presence of $E\{\xi^2(n)\}$, the step-size update is not an accurate reflection of the state of adaptation before or after convergence. This reduces the efficiency of the algorithm significantly. More specifically, close to the optimum, $\mu(n)$ will still be large due to the presence of the noise term $E\{\xi^2(n)\}$. The step size can be rewritten as

$$\mu(n+1)=\alpha\mu(n)+\gamma[E\{V^T(n)X(n)X^T(n-1)V(n-1)\}]^2 \quad (11)$$

It is also clear from above discussion that the update of $\mu(n)$ is dependent on how far we are from the optimum and is not affected by independent disturbance noise. Finally, the considered algorithm involves two additional update equations compared with the standard LMS algorithm. Therefore, the added complexity is six multiplications per iteration. These multiplications can be reduced to shifts if the parameters α,β,γ, are chosen as powers of 2.

2.5. Modified Robust Variable Step-Size LMS (MRVSSLMS) algorithm

From the frame work of step size parameter of LMS algorithm, Kwongs and RVSSLMS algorithms the step size of MRVSS is given:

$$\mu(n+1)=\begin{cases}\mu_{max}; if\ \mu(n+1)>\mu_{max}\\ \mu_{min}; if\ \mu(n+1)<\mu_{min}\\ \alpha\mu(n)+\gamma p^2(n)\end{cases} \quad (12)$$

$$p(n+1) = (1-\beta(n))\,p(n) +\beta(n)e(n)e(n-1) \quad (13)$$

$$\beta(n+1)=\begin{cases}\beta_{max}; if\ \beta(n+1)>\beta_{max}\\ \beta_{min}; if\ \beta(n+1)<\beta_{min}\\ \eta\beta(n)+\lambda e^2(n)\end{cases} \quad (14)$$

where the parameters $0<\alpha,\eta<1$, $\gamma, \lambda > 0$. The $p(n)$ is the time average of the error signal correlation at iteration time n and n+1, and the $\beta(n)$ is the time average of the square error signal, which is used to control the sensitivity of $p(n)$ to the instantaneous error correlation. min max $0 < \mu_{min} < \mu_{max}$; $0 < \beta_{min} < \beta_{max} <1$. The upper bound of step size μ_{max} satisfied the mean square stability condition. The lower bound of the step size μ_{min} is used to guarantee the excess MSE under the tolerant level. The parameter β should be less than 1 and larger than zero.

That is to say, when the algorithm is convergent, the instantaneous error power is very small and the error signal correlation is not sensitive to instantaneous error, and the accuracy of error signal correlation is enhanced. If the system is suddenly changed, the instantaneous error signal power is increased, which result to the enlargement of the correlation function of the error

signal and the instantaneous error signal correlation, therefore the algorithm has a good tracking ability. In one word, the MRVSS have good tracking ability and good anti-noise ability, which are the advantages of algorithm proposed in reference [15][17]. Using these strategies different adaptive noise cancellers are implemented to remove diverse form of noises from speech signals.

3. Simulation Results

To show that RVSSLMS and MRVSSLMS algorithms are appropriate for speech enhancement we have used real speech signals with noise. In the figure *number of samples* is taken on *x-axis* and *amplitude* is taken on *y-axis*. The convergence curves for various algorithms is shown in Figure 2. In order to test the convergence performance we have simulated a sudden noise spike at 4000^{th} sample. From the figure it is clear that the performance of the implemented RVSSLMS and MRVSSLMS algorithms is better than the conventional LMS and Kwongs VSSLMS algorithm. To prove the concept of filtering we have considered five speech samples contaminated with various real noises. These noises are random noise, high voltage murmuring, battle field noise, helicopter noise and crane noise. The noisy speech signal is given as in put to the adaptive filter structure shown in Figure 1, signal somewhat correlated with noise is given as reference signal. As the number of iterations increases error decreases and clean signal can be extracted from the output of the filter. These simulation results are shown in Figures 3, 4, 5, 6 and 7. To evaluate the performance of the algorithms SNRI is measured and tabulated in Tables I, II, III, IV and V.

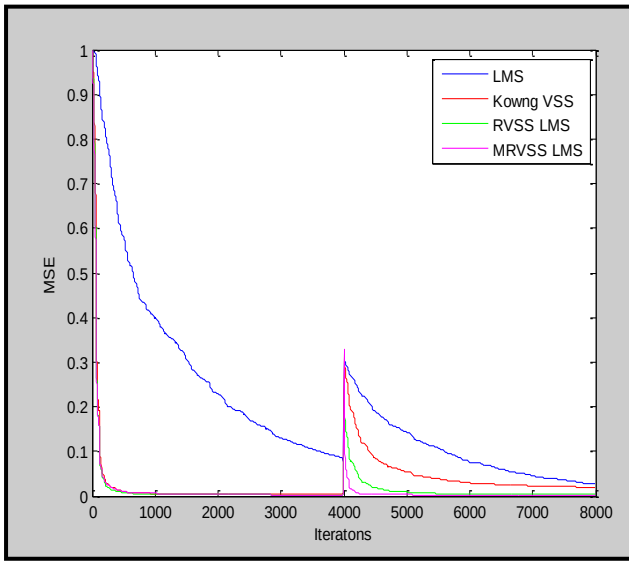


Figure 2: Convergence Characteristics of Various Algorithms.

4. Conclusion

In this paper the problem of noise removal from speech signals using Variable Step Size based adaptive filtering is presented. For this, the same formats for representing the data as well as the filter coefficients as used for the LMS algorithm were chosen. As a result, the steps related to the filtering remains unchanged. The proposed treatment, however exploits the modifications in the weight update formula for all categories to its advantage and thus pushes up the speed over the respective LMS-based realizations. Our simulations, however, confirm that the ability of MRVSSLMS and RVSSLMS algorithms is better than conventional LMS and Kowngs VSSLMS algorithms in terms of SNR improvement and convergence rate. Hence these algorithm is acceptable for all practical purposes.

References

[1] B. Widrow, J. Glover, J. M. McCool, J. Kaunitz, C. S. Williams, R. H.Hearn, J. R. Zeidler, E. Dong, and R. Goodlin,"Adaptive noise cancelling: Principles and applications ", Proc. IEEE, vol. 63, pp.1692-1716, Dec. 1975.
[2] B. L. Sim, Y. C. Tong, J. S. Chang and C. T. Tan, "A parametric formulation of the generalized spectral subtraction method," IEEE Trans. On Speech and Audio Processing, vol. 6, pp. 328-337, 1998.
[3] I. Y. Soon, S. N. Koh, and C. K. Yeo, "Noisy speech enhancement using discrete cosine transform," Speech Communication, vol. 24, pp. 249-257, 1998.
[4] H. Sheikhzadeh, and H. R. Abutalebi, "An improved wavelet-based speech enhancement system," Proc. of the Eurospeech, 2001.
[5] S. Salahuddin, S. Z. Al Islam, M. K. Hasan, M. R. Khan, "Soft thresholding for DCT speech enhancement," Electron. Letters, vol. 38, no.24, pp. 1605-1607, 2002.
[6] J. Homer, "Quantifying the convergence speed of LMS adaptive filter with autoregressive inputs," Electronics Letters, vol. 36, no. 6, pp. 585– 586, March 2000.
[7] H. C. Y. Gu, K. Tang and W. Du, "Modifier formula on mean square convergence of LMS algorithm," Electronics Letters, vol. 38, no. 19, pp. 1147 –1148, Sep 2002.
[8] M. Chakraborty and H. Sakai, "Convergence analysis of a complex LMS algorithm with tonal reference signals," IEEE Trans. on Speech and Audio Processing, vol. 13, no. 2, pp. 286 – 292, March 2005.
[9] S. Olmos , L. Sornmo and P. Laguna, ``Block adaptive filter with deterministic reference inputs for event-related signals:BLMS and BRLS," IEEE Trans. Signal Processing, vol. 50, pp. 1102-1112, May.2002.
[10] Jamal Ghasemi and Mohammad Reza Karami Mollaei, "A New Approach for Speech Enhancement Based On Eigenvalue Spectral Subtraction", Signal Processing: An International Journal, vol. 3, Issue. 4, pp. 34-41.
[11] Mohamed Anouar Ben Messaoud, Aïcha Bouzid and Noureddine Ellouze," A New Method for Pitch Tracking and Voicing Decision Based on Spectral Multi-scale Analysis", Signal Processing: An International Journal, vol. 3, Issue. 5, pp. 144-152.
[12] M.Satya Sai Ram, P. Siddaiah and M. Madhavi Latha," USEFULNESS OF SPEECH CODING IN VOICE BANKING", Signal Processing: An International Journal, vol. 3, Issue. 4, pp. 42-52.
[13] Yonggang Zhang, Ning Li, Jonathon A. Chambers, and Yanling Hao, "New Gradient-Based Variable Step Size LMS Algorithms," EURASIP Journal on Advances in Signal Processing vol. 2008, Article ID 529480, 9 pages, doi:10.1155/2008/529480.
[14] S. Karni and G. Zeng, "A new convergence factor for adaptive filters," *IEEE Transactions on Circuits and Systems*, vol. 36, no. 7, pp. 1011–1012, 1989.
[15] R. H. Kwong and E.W. Johnson, "A variable step-size LMS algorithm," *IEEE Transactions on Signal Processing*, vol. 40, no. 7, pp. 1633–1642, 1992.
[16] V. J. Mathews and Z. Xie, "A stochastic gradient adaptive filter with gradient adaptive step-size," *IEEE Transactions on Signal Processing*, vol. 41, no. 6, pp. 2075–2087, 1993.
[17] T. Aboulnasr and K.Mayyas, "A robust variable step-size LMStype algorithm: analysis and simulations," *IEEE Transactions on Signal Processing*, vol. 45, no. 3, pp. 631–639, 1997.
[18] G.V.S. Karthik, M.Ajay Kumar, Md.Zia Ur Rahman, "Speech Enhancement Using Gradient Based Variable Step Size Adaptive Filtering Techniques", International Journal of Computer Science &

Emerging Technologies, UK, (E ISSN: 2044-6004), Volume 2, Issue 1, February 2011, pp. 168-177.
[19] Md. Zia Ur Rahman, K.Murali Krishna, G.V.S. Karthik, M. John Joseph and M.Ajay Kumar, " Non Stationary Noise Cancellation in Speech Signals using an Efficient Variable step size higher order filter", International Journal of Research and Reviews in Computer Science, UK, Vol. 2, No. 1, 2011.
[20] Md Zia Ur Rahman et al., "Filtering Non Stationary noise in Speech signals using Computationally efficient unbiased and Normalized Algorithm", International Journal on Computer Science and Engineering, ISSN : 0975-3397 Vol. 3 No. 3 Mar 2011, pp. 1106-1113.

Table I: SNR Contrast for Random noise removal.

S.No	Sample No	Before Filtering	LMS		Kowngs VSSLMS		RVSSLMS		MRVSSLMS	
			After	Imp	After	Imp	After	Imp	After	Imp
1	I	0.7523	5.907	5.1553	6.514	5.7621	9.0738	8.3214	10.106	9.3542
2	II	-2.1468	4.1468	6.6975	5.710	8.2610	6.661	9.2154	7.923	10.473
3	III	-4.1554	1.4826	5.6380	1.539	5.6944	3.1546	7.3100	4.760	8.9163
4	IV	-3.6941	1.921	5.6154	2.041	5.7358	3.568	7.2623	5.143	8.8372
5	V	-5.6992	0.544	6.2435	2.333	8.0329	2.692	8.3912	3.853	9.5531
Average Improvement				5.8699		6.6972		8.1000		9.4269

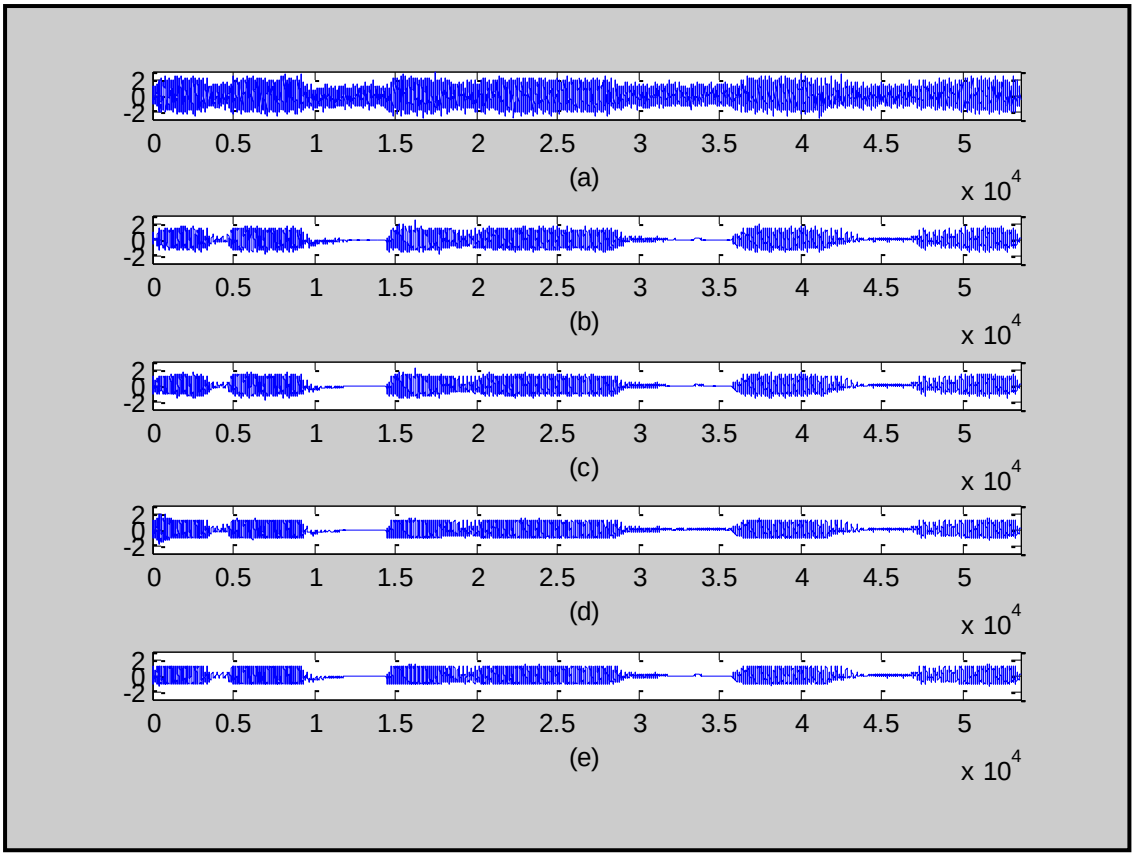


Figure 3**:** Typical filtering results of random noise removal (a) Speech Signal with real noise, (b) recovered signal using LMS algorithm, (c) recovered signal using Kowngs VSSLMS algorithm, (d) recovered signal using RVSSLMS algorithm, (e) recovered signal using MRVSSLMS algorithm.

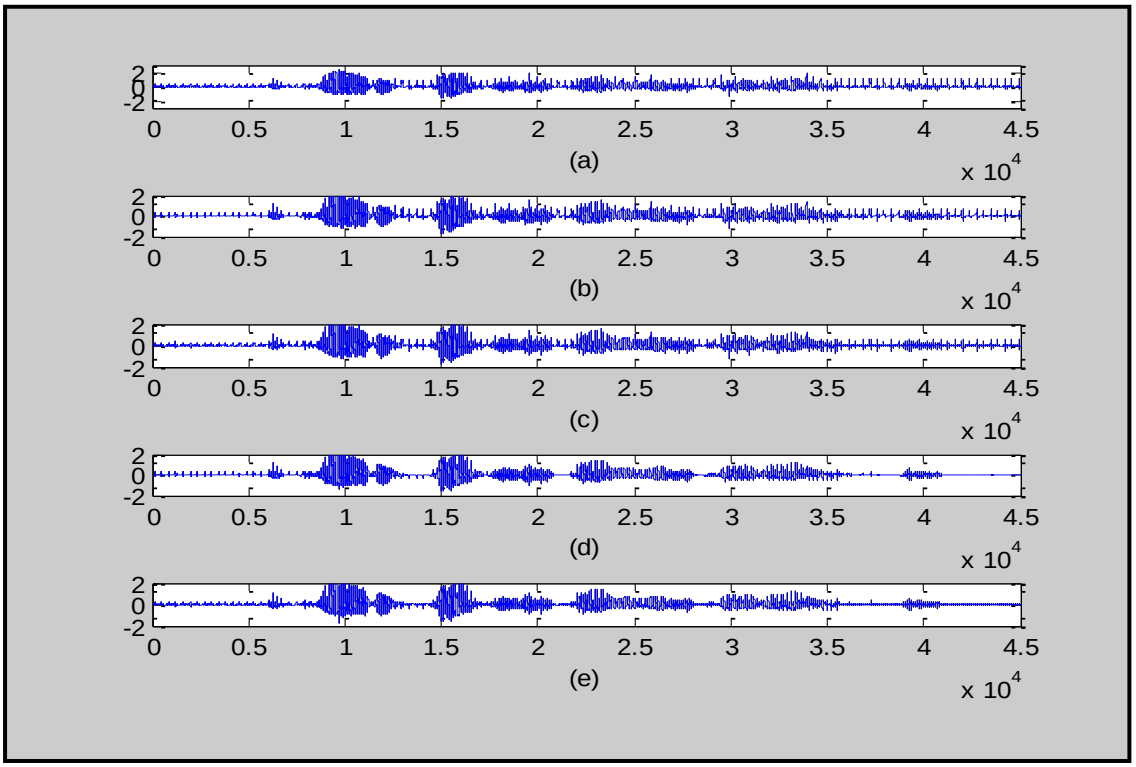


Figure 4**:** Typical filtering results of high voltage murmuring removal (a) Speech Signal with real noise, (b) recovered signal using LMS algorithm, (c) recovered signal using Kowngs VSSLMS algorithm, (d) recovered signal using RVSSLMS algorithm, (e) recovered signal using MRVSSLMS algorithm.

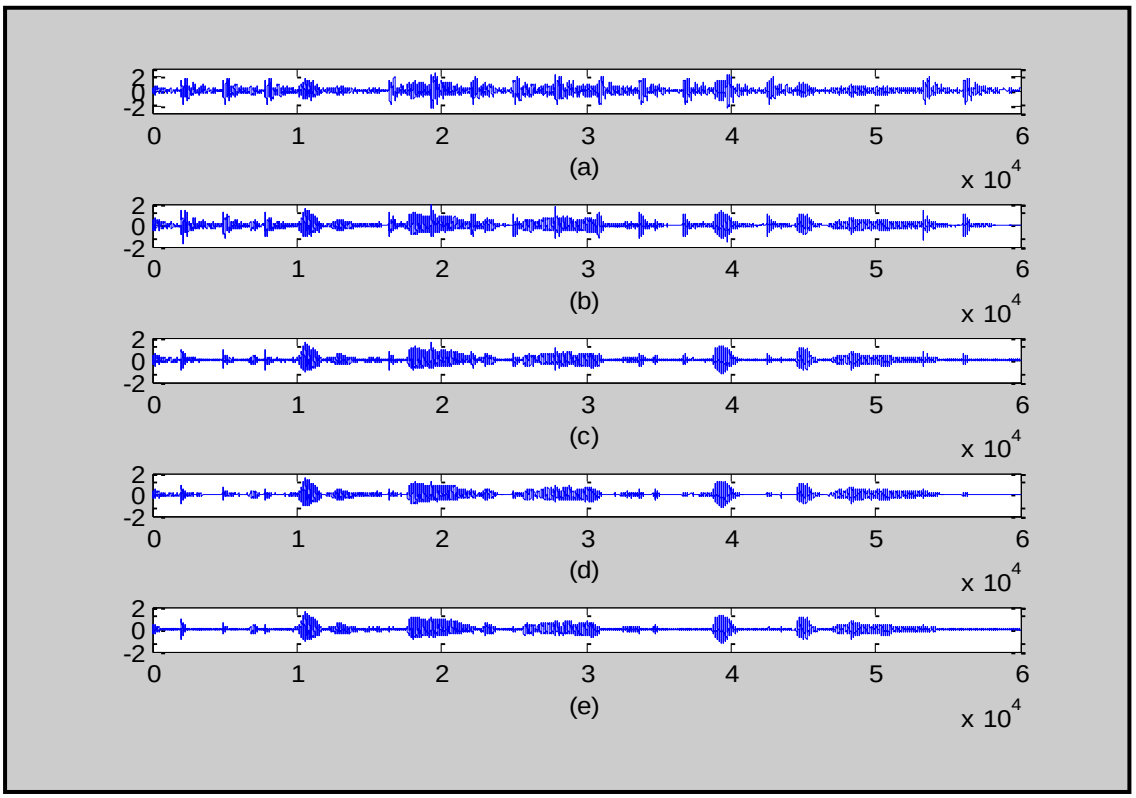


Figure 5**:** Typical filtering results of battle field noise removal (a) Speech Signal with real noise, (b) recovered signal using LMS algorithm, (c) recovered signal using Kowngs VSSLMS algorithm, (d) recovered signal using RVSSLMS algorithm, (e) recovered signal using MRVSSLMS algorithm.

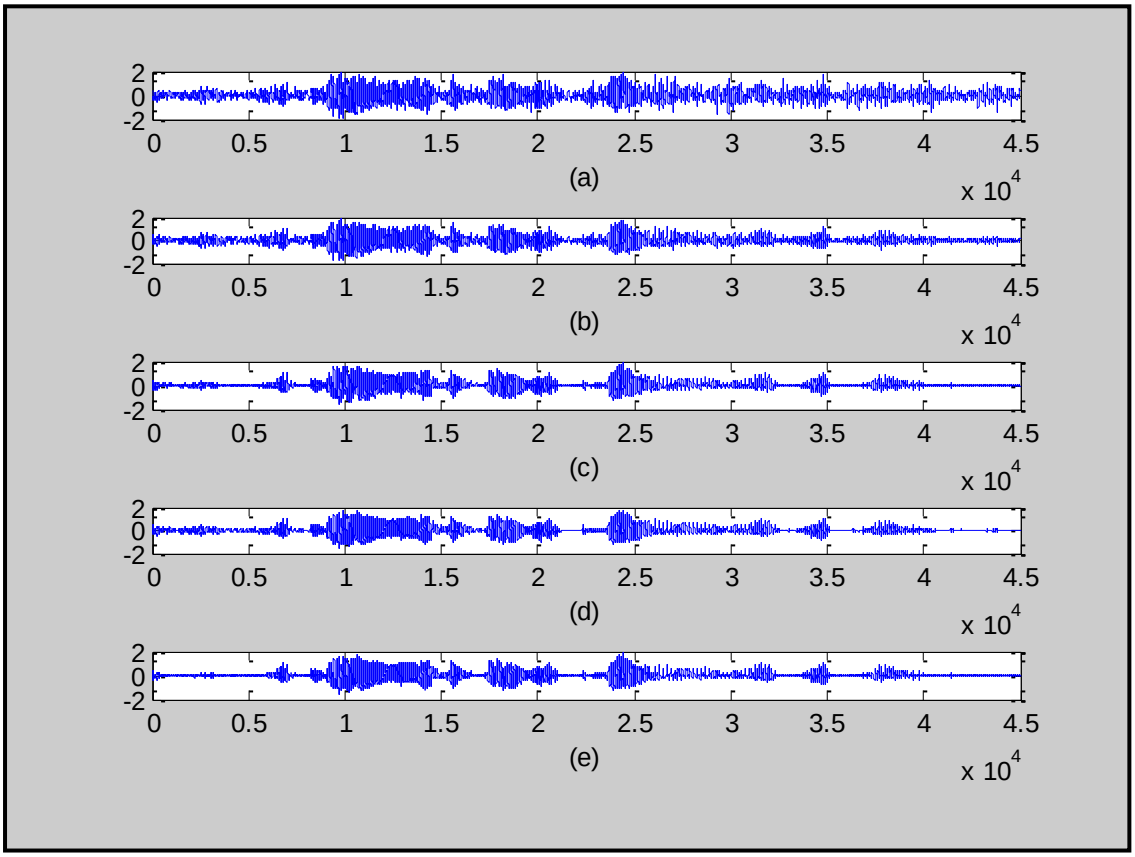


Figure 6: Typical filtering results of helicopter noise removal (a) Speech Signal with real noise, (b) recovered signal using LMS algorithm, (c) recovered signal using Kowngs VSSLMS algorithm, (d) recovered signal using RVSSLMS algorithm, (e) recovered signal using MRVSSLMS algorithm.

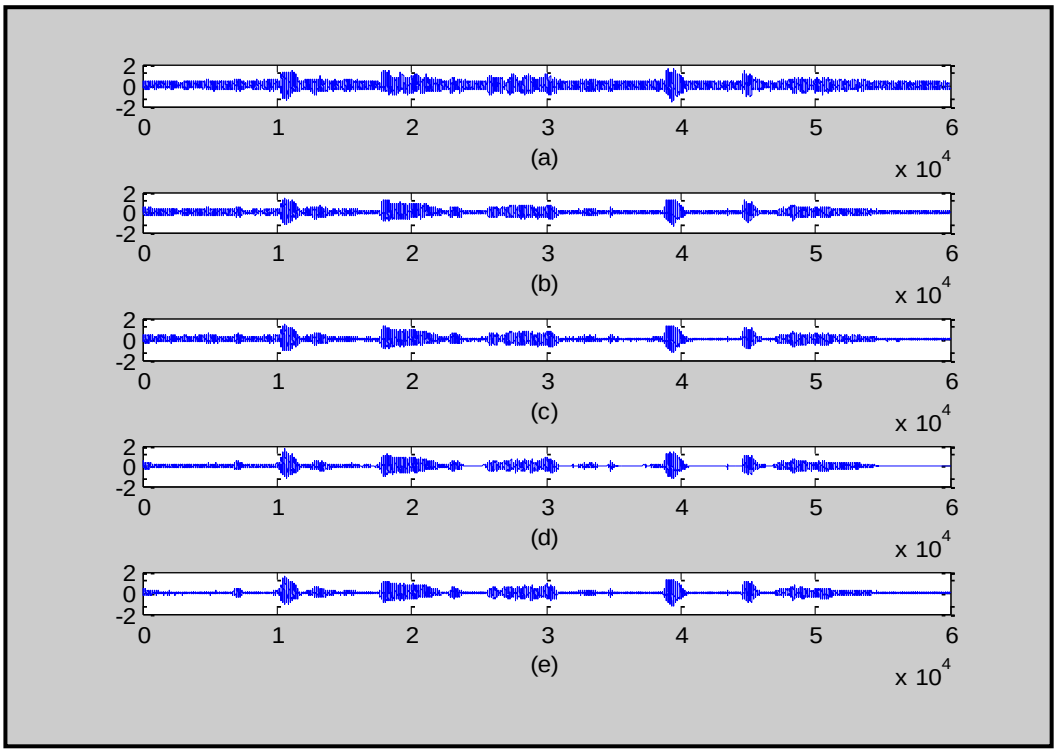


Figure 7: Typical filtering results of crane noise removal (a) Speech Signal with real noise, (b) recovered signal using LMS algorithm, (c) recovered signal using Kowngs VSSLMS algorithm, (d) recovered signal using RVSSLMS algorithm, (e) recovered signal using MRVSSLMS algorithm.

Table II: SNR Contrast for High voltage murmuring removal.

S.No	Sample No	Before Filtering	LMS		Kowngs VSSLMS		RVSSLMS		MRVSSLMS	
			After	Imp	After	Imp	After	Imp	After	Imp
1	I	-1.5937	2.0034	3.5971	3.0735	4.6672	4.2078	5.8015	4.6311	6.2248
2	II	0.0705	1.7646	1.6940	1.9657	1.8951	5.9283	5.8577	6.5044	6.4338
3	III	2.6032	4.3508	1.7476	5.5225	2.9193	7.4302	4.8270	7.9161	5.3129
4	IV	3.0644	4.9673	1.9029	6.6277	3.5633	7.4096	4.3452	8.5129	5.4485
5	V	0.9671	2.8560	1.8888	3.0758	2.1086	7.1156	6.1484	7.9817	7.0145
Average Improvement				2.1660		3.0307		5.3959		6.0869

Table III: SNR Contrast for Battle field noise removal.

S.No	Sample No	Before Filtering	LMS		Kowngs VSSLMS		RVSSLMS		MRVSSLMS	
			After	Imp	After	Imp	After	Imp	After	Imp
1	I	2.2974	3.3847	1.0873	4.6287	2.3313	6.2601	3.9627	7.2928	4.9954
2	II	-3.4698	2.3609	5.8307	3.1695	6.6393	3.7577	7.2275	4.4719	7.9417
3	III	-0.3705	3.9806	4.3511	4.0248	4.3953	4.3109	4.6814	4.8196	5.1901
4	IV	0.1689	2.8943	2.7253	5.7864	5.6174	5.9778	5.8088	6.6614	6.4924
5	V	-2.2891	1.0904	3.3795	5.0618	7.3509	5.5578	7.8469	7.1885	9.4776
Average Improvement				3.4747		5.2668		5.9054		6.8194

Table IV: SNR Contrast for Helicopter noise removal.

S.No	Sample No	Before Filtering	LMS		Kowngs VSSLMS		RVSSLMS		MRVSSLMS	
			After	Imp	After	Imp	After	Imp	After	Imp
1	I	-0.9230	2.4582	3.3821	5.1360	6.0596	6.2503	7.1733	6.5314	7.4544
2	II	3.8058	4.9874	1.1816	5.2488	1.4430	5.5993	1.7935	7.9834	4.1776
3	III	1.1096	4.0840	2.9644	4.5105	3.4009	5.1851	4.0755	6.2739	5.1643
4	IV	1.5709	4.5591	2.9882	5.1484	3.5772	5.9130	4.3421	9.1449	7.5736
5	V	-0.7858	2.9730	3.7588	3.4963	4.2821	5.1573	5.9431	6.2262	7.0120
Average Improvement				2.8550		3.7525		4.6655		6.2764

Table V: SNR Contrast for Crane noise removal.

S.No	Sample No	Before Filtering	LMS		Kowngs VSSLMS		RVSSLMS		MRVSSLMS	
			After	Imp	After	Imp	After	Imp	After	Imp
1	I	0.5244	3.2108	2.6863	4.1024	3.5770	4.2822	3.7577	4.6914	4.1669
2	II	-1.8459	3.2714	5.1173	5.7327	7.5786	6.0373	7.8832	6.7004	8.5463
3	III	-2.1790	3.3691	5.5481	4.2556	6.4346	4.3284	6.5074	4.9409	7.1199
4	IV	-1.6394	2.3560	3.9954	4.2422	5.8816	4.4689	6.1083	5.1134	6.7528
5	V	-3.6823	0.7695	4.4518	4.9700	8.6523	5.8311	9.5134	6.7282	10.410
Average Improvement				4.3597		6.4250		6.7540		7.3993

Analysis of OFDM System using a novel MIMO Technique

D. Ashok Kumar[1], B. Manjula, Md Zia Ur Rahman, K. Murali Krishna and Dr. B. V. Rama Mohana Rao

Department of Electronics and Communication Engineering, Narasaraopeta Engineering College, Narsaraaopeta, India.

[1] ashokd92@ymail.com

***Abstract*— A study of the MIMO (Multiple Input and Multiple Output) OFDM (Orthogonal Frequency Division Multiplexing) and MIMO CI (Carrier Interferometry) OFDM system that are based on the SFBC (Space Frequency Block Coding) coding is done in this project. We evaluate and compare the performances of MIMO OFDM and MIMO CI OFDM systems in both the AWGN (Additive White Gaussian Noise) channel and the Rayleigh fading channel. In CI OFDM, CI code spreading/de-spreading operation and carrier allocation/de-allocation are separately processed by simple IFFT/FFT (Inverse Fast Fourier Transform/ Fast Fourier Transform) type operation. From the simulation results, it is shown that MIMO SFBC CI-OFDM reduces PAPR (Peak to Average Power Ratio) significantly compared with MIMO SFBC-OFDM system. The out-of band re-growth of signal spectrum in MIMO SFBC CI-OFDM system is much smaller than MIMO SFBC OFDM. In the NBI (Narrow Band Interference) channel MIMO SFBC CI-OFDM system achieves considerable BER improvement, compared with the MIMO SFBC-OFDM system in which error floor occurs in most of SNR (Signal to Noise Ratio) range. So, it can be expected that MIMO SFBC CI-OFDM system is very useful for the high speed communication system in the situation of nonlinear HPA (High Power Amplifier) and NBI channel.**

1. INTRODUCTION

OFDM technique has been adopted as the standards in the several high data rate applications, such as Europe DAB/DVB (Digital Audio and Video Broadcasting) system, high-rate WLAN (Wireless Local Area Networks) such as IEEE802.11x, HIPERLAN II and MMAC (Multimedia Mobile Access Communications), and terrestrial DMB (Digital Multimedia Broadcasting) system. OFDM system transmits information data by many sub-carriers, where sub carriers are orthogonal to each other and sub-channels are overlapped so that the spectrum efficiency may be enhanced. OFDM can be easily implemented by the IFFT and FFT process in digital domain, and has the property of high-speed broadband transmission and robustness to multi-path interference in frequency selective fading. However, OFDM signal has high PAPR because of the superimposition of multi-carrier signals with large number of sub-carriers. The high PAPR makes the signal more sensitive to the nonlinearities of the HPA, and these results in signal distortion when the peak power exceeds the dynamic range of the amplifier. To transmit the high PAPR signal without distortion requires more expensive power amplifier with high linearity and wider dynamic range. Besides, the non-linear distortions due to clipping and amplification effects in the transmitted signal will lead to both in-band and out-of band emissions. The former provokes BER degradation whereas the later results in spectral spreading.

Recently, a new kind of technique called CI-OFDM has been widely studied in the multi-carrier communication system [2-5]. In the CI-OFDM technique, each information symbol is sent simultaneously over all carriers and the each carrier for the symbol is assigned a corresponding orthogonal CI spreading code. This CI OFDM system not only can reduce PAPR problem significantly but also achieve frequency diversity gains without any loss in the communication throughput. Besides, a great deal attention has been devoted to MIMO antenna array systems and space-time-frequency processing [6-8]. MIMO diversity technique which exist diversity gain and coding gain can resolve the high link budget problem in the high data rate transmission, especially in the multi-path fading channel. Besides, the space-time-frequency processing, especially Alamouti's diversity technique offers significant increase in performance at a low decoding complexity. Alamouti's STBC (Space Time Block Coding) method is very efficient when delay spread is big or channel's time variation is very small during the coded continuous OFDM symbols and OFDM sub carrier number is small. On the other hand, when Doppler spread is big or channel's time variation is large and channel is non frequency selective, so the inter-sub carrier's channel frequency response is nearly constant in the OFDM system with many sub carriers,

the SFBC (Space Frequency Block Coding) method is more efficient for the high quality transmission.

In this paper, we focused on the two transmit (Tx) / one receive (Rx) antenna, and two Tx / two Rx antenna configuration. We evaluated the performance of MIMO OFDM and MIMO CI OFDM system on the basis of MIMO technique theoretical analysis when HPA nonlinearity or NBI are existed. SFBC coding is applied in both MIMO OFDM system and MIMO CI OFDM system [1]. In CI OFDM realization, CI code spreading/de-spreading operation and carrier allocation/de-allocation are separately processed by simple IFFT/FFT type operation [8, 9].We simulated these systems with both the AWGN and Rayleigh fading channels. We have shown that in both cases (AWGN and Rayleigh fading channel) MIMO CI OFDM system outperforms MIMO OFDM significantly in the existence of both HPA non-linearity and NBI.

2. SYSTEM DESCRIPTION

SFBC transmit diversity technique is applied into the OFDM system. Simply, the 2Tx/1Rx and 2Tx/2Rx antenna configuration are considered to compare the system performance of the MIMO OFDM and MIMO CI-OFDM system. First, we discuss the traditional MIMO SFBC OFDM structure with 2Tx/1Rx and 2Tx/2Rx antenna.

2.1 Alamouti's with $2T_x$-$1R_x$ antennas

Alamouti's introduced a very simple scheme of Space Frequency Block Coding (SFBC) allowing transmissions from two antennas with the same data rate as on a single antenna, but increasing the diversity at the receiver from one to two in a flat fading channel. As shown in Figure 1, the Alamouti's algorithm uses the space and the frequency domain to encode data, increasing the performance of the system by coding the signals over the different transmitter branches. Thus, the Alamouti's code achieves diversity two with full data rate as it transmits two symbols in two frequency slots.

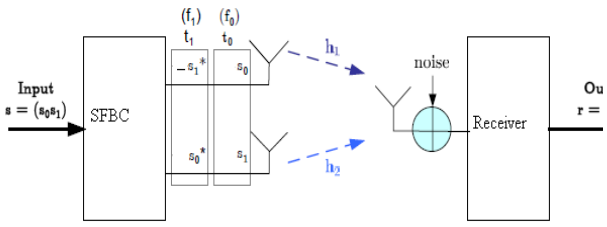


Figure 1: 2×1 Alamouti's SFBC scheme

In the first frequency slot, transmit antennas T_{x1} and T_{x2} are sending symbols s0 and s1, respectively. In the next frequency slot, symbols $-s_1^*$ and s_0^* are sent, where $(\cdot)^*$ denotes complex conjugation. Furthermore, it is supposed that the channel, which has transmission coefficients h_1 and h_2, remains constant and frequency flat over the two consecutive time steps.

The received vector, r, is formed by stacking two consecutive received data samples in frequency, resulting in

$$\mathbf{r} = \mathbf{Sh} + \mathbf{n} \quad (1)$$

Where $\mathbf{r} = [r_0, r_1]^T$ represents the received vector, $\mathbf{h} = [h_1, h_2]^T$ is the complex channel vector, $\mathbf{n} = [n_0, n_1]^T$ is the noise at the receiver, and **S** defines the SFBC:

$$\mathbf{S} = \begin{pmatrix} s_0 & s_1 \\ -s_1^* & s_0^* \end{pmatrix}$$

The vector equation in (1) can be read explicitly as

$$r_0 = s_0 h_1 + s_1 h_2 + n_0 \quad (2)$$

$$r_1 = -s_1^* h_1 + s_0^* h_2 + n_1 \quad (3)$$

At the receiver, the vector **y** of the received signal is formed according to $\mathbf{y} = [r_0, r_1^*]^T$ which is equivalent to

$$r_0 = s_0 h_1 + s_1 h_2 + n_0 \quad (4)$$

$$r_1^* = s_0 h_2^* - s_1 h_1^* + n_1^* \quad (5)$$

The above (4&5) can be rewritten in a matrix system as specified in Equation 3.12:

$$\begin{pmatrix} r_0 \\ r_1^* \end{pmatrix} = \begin{pmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \end{pmatrix} + \begin{pmatrix} n_0 \\ n_1^* \end{pmatrix} \quad (6)$$

The short notation for this system is the following:

$$\mathbf{y} = \mathbf{H}_v \mathbf{s} + \tilde{\mathbf{n}} \quad (7)$$

where $\tilde{\mathbf{n}}$ represents the new noise vector obtained after the conjugation of the second equation, $\tilde{\mathbf{n}} = [n_0, n_1^*]^T$

The estimated transmitted signal is then calculated from the formula

$$\hat{\mathbf{s}} = \mathbf{H}_v^H \mathbf{y} \quad \text{Where } \mathbf{y} = [r_0, r_1^*]^T \quad (8)$$

where $\mathbf{H}_v^H = \begin{pmatrix} h_1^* & h_2 \\ h_2^* & -h_1 \end{pmatrix}$ is Hermitian of the virtual channel matrix $\mathbf{H}_v$.

$$\hat{\mathbf{s}} = \begin{pmatrix} \hat{s}_0 \\ \hat{s}_1 \end{pmatrix} = \mathbf{H}_v^H \mathbf{H}_v \begin{pmatrix} s_0 \\ s_1 \end{pmatrix} + \mathbf{H}_v^H \begin{pmatrix} n_0 \\ n_1^* \end{pmatrix} \quad (9)$$

The resulting virtual (2 × 2) channel matrix $\mathbf{H}_v$ is orthogonal, i.e.

$$\mathbf{H_v}^H \mathbf{H_v} = \mathbf{H_v}\mathbf{H_v}^H = h^2\,\mathbf{I_2}$$

Due to this orthogonality, the Alamouti's scheme decouples the MISO channel into two virtually independent channels with channel gain h^2 and diversity d = 2.

The channel gain mentioned is deduced from (10), which specifies that transmitted symbols can be estimated at the receiver as the result of multiplying the received signals by the Hermitian of the virtual channel matrix. After performing the corresponding operations it results in a signal with a gain of h^2 plus some modified noise.

$$\hat{\mathbf{s}} = h^2\mathbf{I_2}\mathbf{s} + \hat{\mathbf{n}} \qquad (10)$$

Where, **s** is the transmitted signal,

$\mathbf{I_2}$ is the 2×2 identity matrix,

$h^2 = |h_1|^2 + |h_2|^2$ is the power gain of the channel, and

$\hat{\mathbf{n}} = \begin{pmatrix} h_1^* n_0 + h_2 n_1^* \\ h_2^* n_0 - h_1 n_1^* \end{pmatrix}$ is some modified noise.

2.2 Alamouti's with $2T_x$ - $2R_x$ Antennas

A system with two transmitting antennas and two receive antennas as the one depicted in Figure 2, is analyzed next. The already explained steps are applied to each of the receive antennas, denoting the received signal in the first and second time slot as $\mathbf{r}_1$ and $\mathbf{r}_2$, respectively.

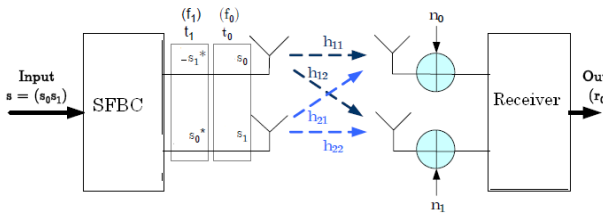


Figure 2 : 2×2 Alamouti's SFBC scheme

The received signal from a 2 × 2 Alamouti's scheme, as depicted above, is

$$\mathbf{y} = \begin{pmatrix} r_0(1) \\ r_0(2) \\ r_1^*(1) \\ r_1^*(2) \end{pmatrix} = \begin{pmatrix} h_{11} & h_{21} \\ h_{12} & h_{22} \\ h_{21}^* & -h_{11}^* \\ h_{22}^* & -h_{12}^* \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \end{pmatrix} + \begin{pmatrix} n_0(1) \\ n_0(2) \\ n_1^*(1) \\ n_1^*(2) \end{pmatrix} \qquad (11)$$

The estimated transmitted signal can be calculated from $\hat{\mathbf{s}} = \mathbf{H_v}^H \mathbf{y}$ where $\mathbf{y} = \left[r_0(1), r_0(2), r_1^*(1), r_1^*(2)\right]^T$ and $(.)^H$ represents the Hermitian operation.

The virtual channel matrix, $\mathbf{H_v}$ is expressed as

$$\mathbf{H_v} = \begin{pmatrix} h_{11} & h_{21} \\ h_{12} & h_{22} \\ h_{21}^* & -h_{11}^* \\ h_{22}^* & -h_{12}^* \end{pmatrix} \quad \textit{Therefore}$$

$$\mathbf{H_v}^H = \begin{pmatrix} h_{11}^* & h_{12}^* & h_{21} & h_{22} \\ h_{21}^* & h_{22}^* & -h_{11} & -h_{12} \end{pmatrix}$$

The obtained result for the process of estimating the transmitted symbols is

$$\hat{\mathbf{s}} = h^2\mathbf{I_2}\mathbf{s} + \hat{\mathbf{n}}$$

(12)

Where, $\mathbf{I_2}$ is the 2×2 identity matrix,

s is the transmitted signal,

$h^2 = |h_{11}|^2 + |h_{21}|^2 + |h_{12}|^2 + |h_{22}|^2$ is the power gain of the channel, and

$$\hat{\mathbf{n}} = \begin{pmatrix} h_{11}^* n_0(1) + h_{12}^* n_0(2) + h_{21} n_1^*(1) + h_{22} n_1^*(2) \\ h_{21}^* n_0(1) + h_{22}^* n_0(2) - h_{11} n_1^*(1) - h_{12} n_1^*(2) \end{pmatrix}$$

represents some modified noise.

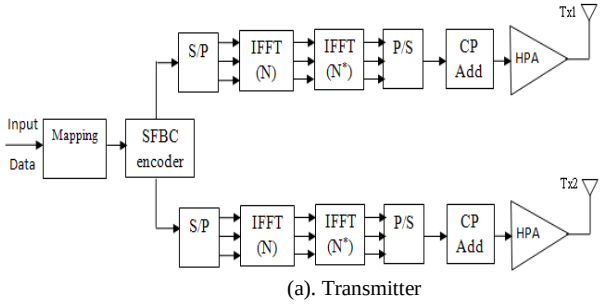
3. MIMO SFBC CI OFDM SYSTEM

3.1 Configuration of the MIMO SFBC CI OFDM

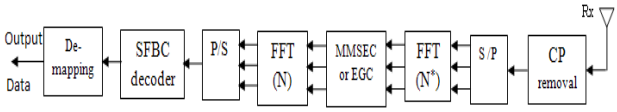
The transmitter incorporates SFBC, symbol mapping which is accomplished by Quadrature Amplitude modulation (QAM), high power amplifier (HPA). The first IFFT accomplishes the CI spreading and the second IFFT performs the typical OFDM modulation. A cyclic prefix is also appended as a guard interval to the CI OFDM symbol in order to combat the inter symbol interference (ISI) induced by multipath delay spread in the selective fading channel. At receiver, two FFTs are used to demodulate and de-spread the signals respectively. Different diversity combining techniques are easy to implement based on this system structure. Equal gain combining (EGC) is an optimal combining technique in an AWGN channel, while other methods such as minimum mean square error combining (MMSEC) and maximum ratio combining (MRC) are used to eliminate ISI in the selective fading channel environment. By using diversity combination, the output signal of the receiver corresponds to

$$\hat{s} = \sum_{k=0}^{N-1}\sum_{i=0}^{N-1} w_i r e^{-j\frac{2\pi}{N}ki} e^{-j\frac{2\pi}{N}ni} = DFT[w.DFT(r)] \quad (13)$$

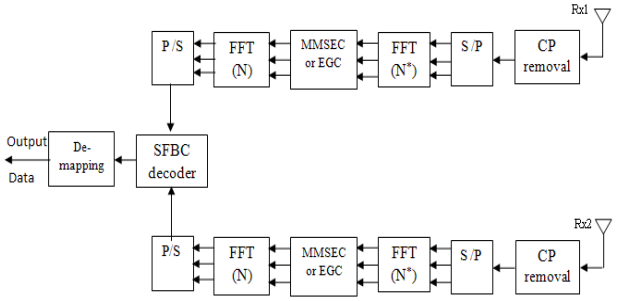
Where **w** = $(w_0, w_{1,\ldots,} w_{N-1})$ is weight used in diversity combining scheme.



(a). Transmitter



(b). Receiver in $2T_x$-$1R_x$



(c) Receiver in $2T_x$-$2R_x$

Figure 3: MIMO SFBC CI OFDM Transceiver (a) Transmitter, (b) Receiver in $2T_x$-$1R_x$ and (c) Receiver in $2T_x$-$2R_x$

The input vector of the second IFFT in Figure 3 (a) could correspond to

$$\boldsymbol{\rho}' = (\underbrace{\rho_0, \rho_1, \ldots, \rho_{N/2-1}}_{N/2}, \underbrace{0,0,\ldots 0}_{(L-1)*N}, \underbrace{\rho_{N/2}, \rho_{N/2+1}, \ldots, \rho_{N-1}}_{N/2})$$

$$\text{or } \boldsymbol{\rho}' = (\underbrace{\rho_0, \rho_1, \ldots, \rho_{N-1}}_{N}, \underbrace{0,0,\ldots 0}_{(L-1)*2N}, \underbrace{0,0,\ldots 0}_{N})$$

where, L is oversampling factor of the second IFFT.

Before passing through nonlinear HPA, the l^{th} Tx transmitted signal for one entire MIMO SFBC CI OFDM symbol is as follows

$$S^l(t) = \sum_{k=0}^{N-1}\sum_{i=0}^{N-1} x_k^l . e^{j2\pi k \Delta f t} . e^{jk\Delta\theta_i} . e^{j2\pi f_c t} . p(t) \quad (14)$$

$$S^l(t) = e^{j2\pi f_c t} . \sum_{k=0}^{N-1} s_k^l . e^{j2\pi k \Delta f t} . p(t) \quad (15)$$

where, x_k^l is the time domain SFBC coded data on the k carrier and l^{th} Tx antenna, f_c is the centre frequency and $P(t)$ is the pulse shaping for the bit duration T_b. Besides, here, $\sum_{i=0}^{N-1} x_i^l . e^{jk\Delta\theta_i}$ is defined as s_k^l.

Theoretically, in the MIMO SFBC CI-OFDM receiver side, the j^{th} Rx received signal can be expressed as follows

$$R^j(t) = e^{j2\pi f_c t} . \sum_{l=1}^{L}\sum_{k=0}^{N-1} h_k^{lj} . s_k^l . e^{j2\pi k\Delta f t} + n^{lj}(t) + I^{lj}(t) \quad (16)$$

$$R^j(t) = e^{j2\pi f_c t} . \sum_{l=1}^{L}\sum_{k=0}^{N-1} \alpha_k^{lj} . s_k^l . e^{j2\pi k\Delta f t} . e^{j\phi_k^{lj}} + n^{lj}(t) + I^{lj}(t) \quad (17)$$

$$R^j(t) = e^{j2\pi f_c t} . \sum_{l=1}^{L}\sum_{k=0}^{N-1}\sum_{i=0}^{N-1} \alpha_k^{lj} x_k^l . e^{j2\pi k\Delta f t} . e^{jk\Delta\theta_i} . e^{jkf_c t} + n^{lj}(t) + I^{lj}(t) \quad (18)$$

where L is the total transmit antenna number (L = 2 in our case), $R^j(t)$ is the j^{th} Rx antenna received signal, h_k^{lj} is the time domain channel response of the k^{th} carrier from l^{th} Tx antenna to j^{th} Rx antenna when channel is frequency selective fading channel, α_k^{lj} and ϕ_k^{lj} are the fade parameter and phase offset of h_k^{lj} respectively, and $n^{lj}(t)$ is the AWGN (Additive White Gaussian Noise) with a power spectral density equal to $N_0/2$ and $I^{lj}(t)$ is the narrow band interference noise from l^{th} Tx antenna to j^{th} Rx antenna.

In an AWGN or a flat fading channel, i.e., $\alpha_k^{lj} = C_k$ where C is a constant, a simple equal gain combining across carriers (index k) is an optimal combining technique. However, in a frequency selective fading channel, a carefully designed combiner (across carriers) needs to be employed to counter the loss of orthogonality between CI spreading codes (due to the

carrier dependent gain α_k^{lj}). The general form of the combiner corresponds to

$$R_C{}^j = \sum_{k=0}^{N-1} W_k \cdot R_k^j(t)$$

(19)

The weights W_k *is* based on Minimized Mean Square Error Combining (MMSEC) since this scheme has been shown (in the MIMO OFDM for wireless LAN, [9]) (1) to exploit the frequency diversity available in a frequency-selective fading channel and (2) to jointly minimize the inter-symbol interference, the additive noise (the second term in (18)) and the narrow band interference (the third term in (18)). It is easy to show that the combining weight vector, derived via the MMSE criteria, corresponds to

$$W = \left(\alpha \mathrm{I}_N + \mathrm{H}^H \mathrm{H}\right)^{-1} \mathrm{H}^H$$

(20)

Where, $\alpha = \sigma_n^2 / \sigma_s^2$. (σ_s^2 and σ_n^2 are variances of the signal and noise).

H is the channel matrix, I_N is the $N \times N$ identity matrix.

3.2 Mapping and De-Mapping

Serial binary data is converted into complex numbers representing constellation points. This one maps the time domain amplitude coefficients into frequency domain coefficients at the transmitter and Vs at the receiver. Generally digital modulation techniques such as BPSK, QPSK, 16QAM etc., are used. In this project 16QAM is used. Mapping itself is called as serial to parallel converter.

3.3 Peak to Average Power Ratio (PAPR)

Consider the MIMO OFDM system with *L* transmit antennas that uses *N* sub-carriers. In the case of two transmit antennas, the each of *N*-dimensional OFDM symbol is transmitted from antenna 1 and antenna 2 respectively. Generally, the PAPR of the transmitted OFDM signal is defined as

$$PAPR^l = \frac{\max_{0 \le t \le T} \left| S^l(t) \right|^2}{E\left[\left| S^l(t) \right|^2 \right]}$$

(21)

where *l* means the transmit antenna number and *E*[•] means the expectation operation.

When calculating PAPR using discrete sampled signals, we cannot find the accurate PAPR because the true peak of continuous time OFDM signal may be missed in the Nyquist sampling. So, we use 4 times over-sampling to improve accuracy of discrete PAPR. Besides, to show statistical characteristics of PAPR, we use CCDF (Complementary Cumulative Distribution Function), which is the probability that PAPR of OFDM/CIOFDM signal exceeds a certain threshold $PAPR_0$. The CCDF is defined as

$$\begin{aligned} CCDF^l &= \Pr\left(PAPR^l > PAPR_0\right) \\ &= 1 - \Pr\left(PAPR^l \le PAPR_0\right) \\ &= 1 - \prod_{n=1}^{N} \left[1 - \exp\left(- PAPR_0 \times \frac{P_{avg}^l}{P_n^l} \right) \right] \\ &= 1 - \left(1 - \exp\left(- PAPR_0\right)\right)^{\alpha N} \end{aligned}$$

(22)

where P_n^l is the average sample power of l^{th} transmit antenna signal, $P_{avg}^l = (1/T)\int_0^T \left| S^l(t) \right|^2 dt$ is the average power of l^{th} transmit antenna signal, here, when oversampling is done, $P_n^l = P_{avg}^l$ is nearly satisfied. Commonly, α is 2.8 in most cases.We define the observed CCDF of MIMO transmitter is

$$CCDF = \max_{0 < l \le L} \left(CCDF^l \right) \qquad (23)$$

4. RESULTS AND DISCUSSIONS

Based on the above theoretical analysis, in order to compare the transmission performance both in the MIMO SFBC OFDM and MIMO SFBC CI-OFDM system, we evaluated the PAPR, Spectrum and BER of MIMO SFBC OFDM and MIMO SFBC CI-OFDM when SSPA is used as each transmitter's HPA or/and NBI is inserted to the data carriers. 2Tx-1Rx and 2Tx-2Rx MIMO scheme is considered. HPA back off values are supposed to be 2, 3 and 6. JSR (or ISR) of NBI is supposed to be 0dB or 1dB. AWGN and Rayleigh fading channels are considered through the whole evaluation. The total sub carrier number is supposed to be 1024 and 16QAM modulation is used in the whole simulation.

The PAPR benefit of CI OFDM can translate to an increase in transmission range. Specifically, assume that clipping (due to saturation of the transmit power amplifier) must occur no more than 10% of the time. In this case, referring to *Figure 4***,** we must not clip any OFDM symbols with PAPR ≤ 10.24 (any OFDM symbol with PAPR > 10.24 may be clipped). Therefore, assuming a peak (max) power of 100 *mW*, the average power = peak power/10.24 = 9.7656 *mW*. For CI OFDM systems (with clipping permitted no more than 10% of the time), a CI OFDM symbol with PAPR ≤ 8.167 must experience no clipping (any CI OFDM symbol with

PAPR > 8.167 may be clipped). Therefore, (again assuming a peak (max) power = 100 *mW*) the average power = peak power/8.167 = 12.24 *mW*.

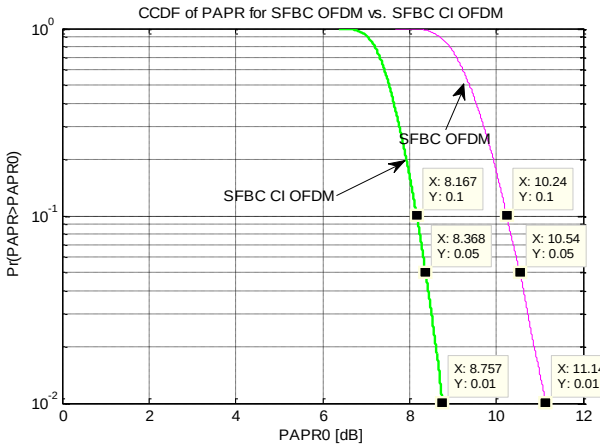


Figure 4: PAPR in MIMO SFBC OFDM & CI OFDM

By direct comparison, we observe that, at a fixed clipping percentage of l0%, a CI OFDM system may operate with an average power of ***12.24mW***, whereas an OFDM system must operate at ***9.7656mW***. That is, CI OFDM enjoys a 2.07 dB gain in transmit power.

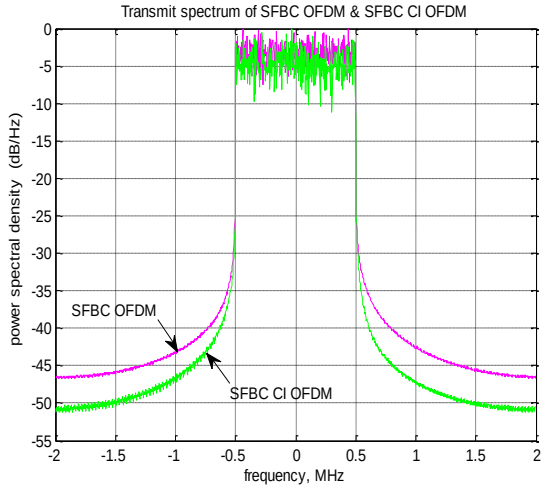


Figure 5: Spectrum in MIMO SFBC OFDM & CI OFDM

Besides, the transmit signal in CI OFDM systems will be received at a signal power of 2.07dB more than that of OFDM. Therefore, if we consider that power decreases as a function of $\mathbf{r}^2$, i.e., as a function of 201og(r), additional range equates 20log(r) = 2.07, i.e., CI OFDM offers a range-increase-factor of 1.27**.** If OFDM demonstrates a range of 100 m (Meters), CI OFDM demonstrates a range of 127 m. If OFDM can operate at 150 m, CI OFDM operates at 190.5 m.

Besides, the out of band spectrum re-growth is reduced significantly in the MIMO SFBC CI-OFDM system compared with MIMO SFBC OFDM system as seen in *Figure 5.*

Bit Error Rate (BER) Comparison Under Awgn Channel

Figure 6 is the BERs of MIMO SFBC OFDM and MIMO SFBC CI-OFDM when SSPA with 2 back off is considered as the transmitter HPA. As seen in Figure *6*, about 21dB and 18.5dB SNR are required at 10^{-4} of BER in the 2Tx-1Rx SFBC CI-OFDM and 2Tx-2Rx SFBC CI-OFDM system, but worse than 10^{-2} of BERs are achieved at SNR of 21dB both in the 2Tx-1Rx SFBC OFDM and 2Tx-2Rx SFBC OFDM system, and error floors occur in the two kinds of MIMO SFBC OFDM systems.

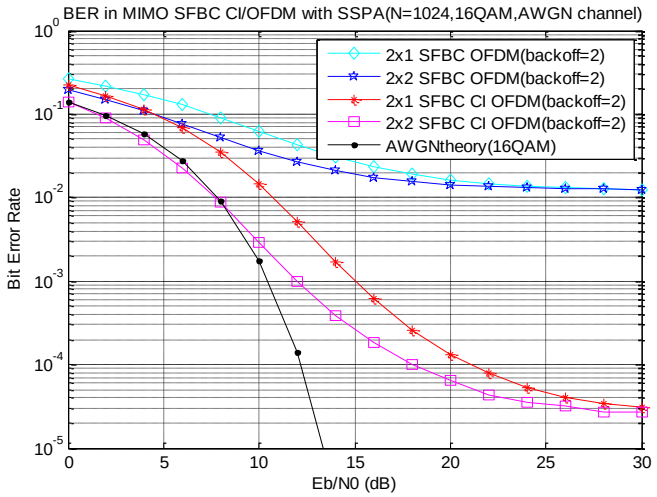


Figure 6: BER in MIMO SFBC OFDM & CI OFDM with HPA (back off=2)

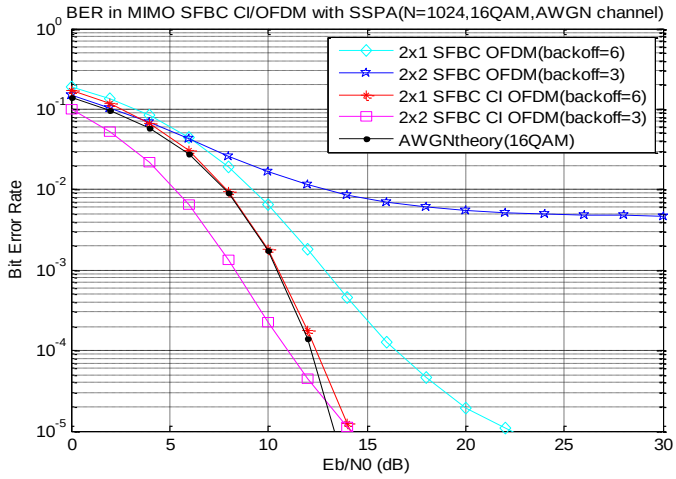


Figure 7: BER in MIMO SFBC OFDM & CI OFDM with HPA (back off=3 or 6)

Figure 7 is the BER of MIMO SFBC OFDM and MIMO SFBC CI-OFDM when SSPA with certain back-off is considered as transmitter HPA. As seen in Figure 7, when back off of 6 and 3 are supposed respectively in the 2Tx-1Rx SFBC CI-OFDM and 2Tx-2Rx SFBC CI-OFDM system, SSPA nonlinearity is almost compensated completely. However, in 2Tx-1Rx SFBC OFDM system, about 4dB SNR penalty is

observed at BER of10^{-4}, and in the 2Tx-2Rx SFBC OFDM system, error floor occurs even if at SNR of 30dB.

Figure 8 is the BER of MIMO SFBC OFDM and MIMO SFBC CI-OFDM when NBI is inserted to the data carriers. As seen from the figure, MIMO SFBC CI-OFDM system can nearly compensate all the NBI affect when JSR is 0 or 1 respectively. Only About 3.5dB SNR penalty is observed at BER of 10^{-4} in the 2Tx-1Rx SFBC CI-OFDM system, and even if 2dB SNR gain is observed in the 2Tx-2Rx SFBC CI-OFDM system compared with theory without NBI. However, worse than ~10^{-3} of BER are achieved in the 2Tx-1Rx SFBC OFDM and 2Tx-2Rx SFBC OFDM system, and error floors occur in the both of MIMO SFBC OFDM systems.

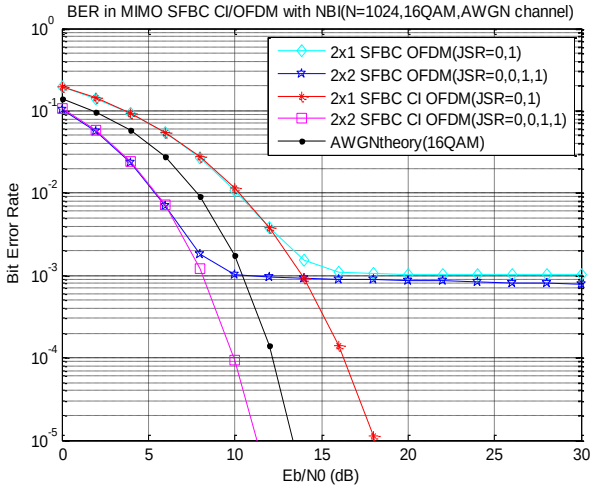


Figure 8: BER in MIMO SFBC OFDM & CI OFDM with NBI

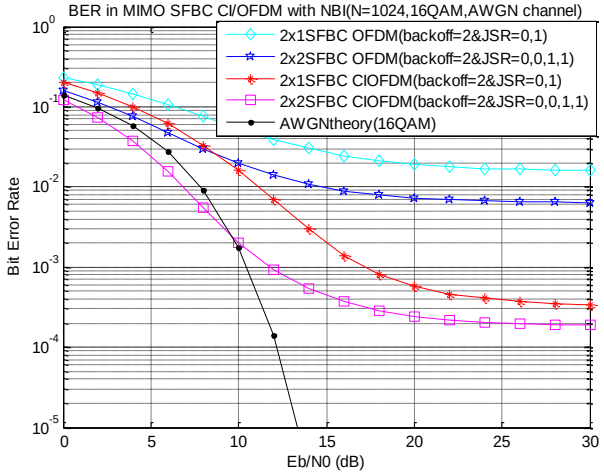


Figure 9: BER in MIMO SFBC OFDM & CI OFDM with HPA and NBI

Figure 9 is the BER of MIMO SFBC OFDM and MIMO SFBC CI-OFDM when SSPA with 2 back off is considered as transmitter HPA and also NBI is inserted to the data carriers. As seen from the figure, about 17dB and 12dB SNR are required at 10^{-3} of BER in the 2Tx-1Rx SFBC CI-OFDM and 2Tx-2Rx SFBC CI-OFDM system respectively, but worse than 2×10^{-2} and 10^{-2} of BER are achieved in the 2Tx-1Rx SFBC OFDM and 2Tx-2Rx SFBC OFDM system, and error floors occur in the both of MIMO SFBC OFDM systems.

BER Comparison under Rayleigh Fading & AWGN Channel

Figure 10 is the BER of MIMO SFBC OFDM and MIMO SFBC CI-OFDM when SSPA back off 2 is considered as the transmitter HPA. As seen in Figure *10*, about 35dB and 30dB SNR are required at $2x10^{-3}$ of BER in the 2Tx-1Rx SFBC CI-OFDM and 2Tx-2Rx SFBC CI-OFDM system, but worse than 10^{-2} of BERs are achieved even at SNR of 40dB both in the 2Tx-1Rx SFBC OFDM and 2Tx-2Rx SFBC OFDM system, and error floors occur in the two kinds of MIMO SFBC OFDM systems.

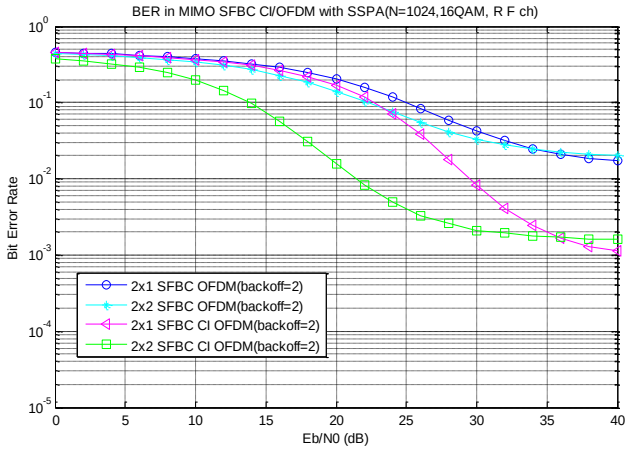


Figure 510: BER in MIMO SFBC OFDM & CI OFDM with HPA (back off=2)

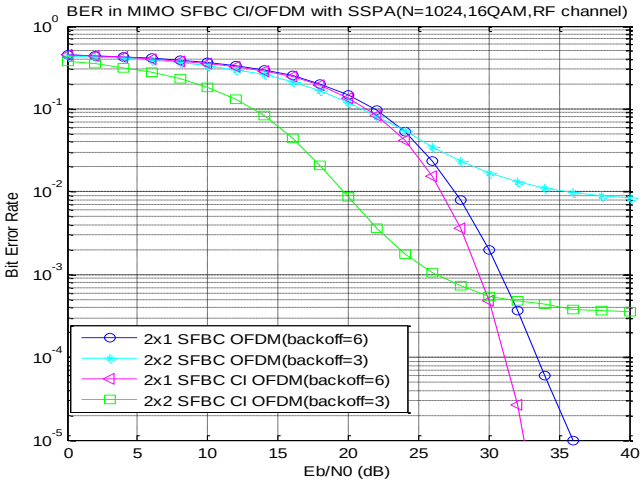


Figure 11: BER in MIMO SFBC OFDM & CI OFDM with HPA (back off=3 & 6)

Figure 11 is the BER of MIMO SFBC OFDM and MIMO SFBC CI-OFDM when SSPA with certain back-off is considered as transmitter HPA. As seen in Figure 11, when back off of 6 and 3 are supposed respectively in the 2Tx-1Rx SFBC CI-OFDM and 2Tx-2Rx SFBC CI-OFDM system, SSPA nonlinearity is almost compensated completely. However, in 2Tx-1Rx SFBC OFDM system, about 2dB SNR penalty is observed than 2Tx-1Rx SFBC CI OFDM at BER of 10^{-4}, and in the 2Tx-2Rx SFBC OFDM system, gives BER of 10^{-2} even at SNR of 40dB.

Figure 12 is the BER of MIMO SFBC OFDM and MIMO SFBC CI-OFDM when NBI is inserted to the data carriers. As seen from the figure, MIMO SFBC CI-OFDM system can nearly compensate all the NBI affect when JSR is 0 or 1 respectively. Only About 27dB and 33.5dB are required at BER of 10^{-4} in the 2Tx-2Rx SFBC CI-OFDM and 2Tx-1Rx SFBC CI-OFDM system respectively.. However, worse than $7x10^{-3}$ of BER are achieved in the 2Tx-1Rx SFBC OFDM and 2Tx-2Rx SFBC OFDM system, and error floors occur in the both of MIMO SFBC OFDM systems.

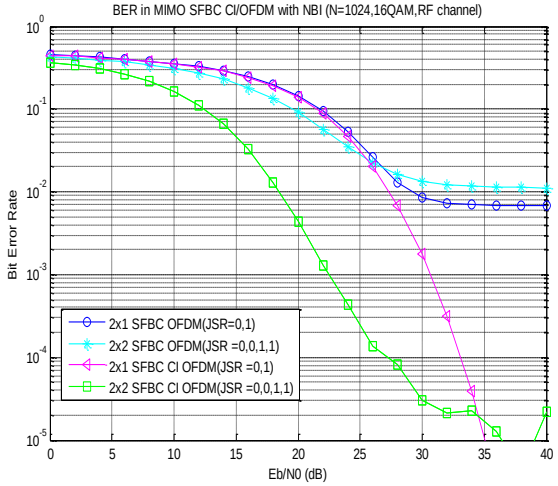


Figure 12: BER in MIMO SFBC OFDM & CI OFDM with NBI

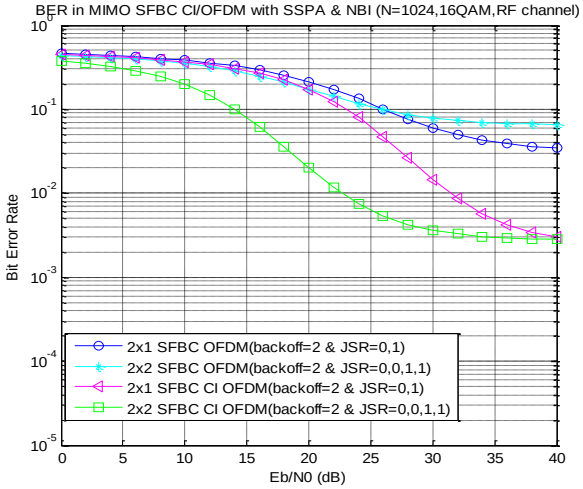


Figure 13: BER in MIMO SFBC OFDM & CI OFDM with HPA (back off=2) and NBI

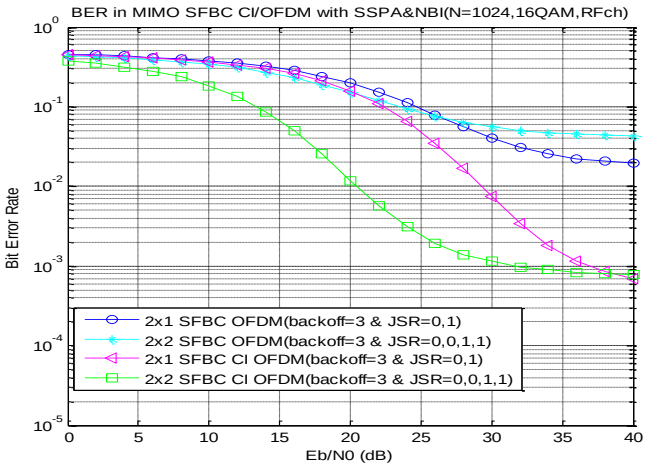


Figure 14: BER in MIMO SFBC OFDM & CI OFDM with HPA (back off=3) and NBI

Figure 13 & Figure 14 are the BER of MIMO SFBC OFDM and MIMO SFBC CI-OFDM when SSPA with back off 2 & 3 respectively is considered as transmitter HPA and also NBI is inserted to the data carriers. As seen from the Figure 13 & Figure 14, about 31.5dB & 31dB and 22.5dB & 37dB SNR are required at 10^{-2} &$10^{-3}$of BER in the 2Tx-1Rx SFBC CI-OFDM and 2Tx-2Rx SFBC CI-OFDM system respectively, but worse than 2×10^{-2} & 10^{-2} of BER are achieved in the 2Tx-1Rx SFBC OFDM and 2Tx-2Rx SFBC OFDM system, and error floors occur in the both of MIMO SFBC OFDM systems.

5. CONCLUSION

We evaluated the performance of MIMO SFBC OFDM and MIMO SFBC CI OFDM system on the basis of MIMO technique, and focused on the two Tx/one Rx antenna and two Tx/two Rx antenna configurations under both AWGN and Rayleigh fading channel. SFBC coding is applied in both MIMO OFDM system and MIMO CI-OFDM system, in which CI codes spreading operation and carrier allocation are separately processed by simple IFFT type operation.

1. From the simulation results, it is found that MIMO SFBC CI OFDM reduces PAPR significantly compared with MIMO SFBC-OFDM system.
2. The out-of band re-growth of signal spectrum in MIMO SFBC CI OFDM system is much smaller than MIMO SFBC OFDM.
3. When the Narrow band interference exists, MIMO SFBC CI OFDM system achieves considerable BER improvement compared with the MIMO SFBC OFDM system in which error floor occurs even in high SNR. It is because that CI OFDM method has frequency diversity benefit so that it brings robustness to the narrow band interference.

4. Much better system performance is obtained by using MIMO SFBC CI-OFDM method than MIMO SFBCOFDM in the situation of existing both nonlinear HPA and NBI.

Overall, MIMO SFBC CI-OFDM system outperforms MIMO SFBC OFDM significantly when system is interrupted by the HPA nonlinearity or NBI under both AWGN and Rayleigh fading channel. Therefore, the MIMO SFBC CI OFDM method can be further applicable to the any kinds of MIMO type multi-carrier communication systems with many sub-carriers.

REFERENCES

[1]. Heung-Gyoon Ryu *Member, IEEE*: "System Design and Analysis of MIMO SFBC CI-OFDM System against the Nonlinear Distortion and Narrowband Interference", IEEE Transactions on Consumer Electronics, Vol. 54, No. 2, May 2008.
[2]. Carl R. Nassar, B. Natarajan, Z. Wu D. Wiegandt, S. A. Zekavat, "Multi-Carrier Technologies for Wireless Communication", 2002.
[3]. Zhiqiang Wu, Zhijin Wu, Wiegandt, D.A. and Nassar, C.R., "Highperformance 64-QAM OFDM via carrier interferometry spreading codes," *IEEE 58th Vehicular Technology Conference, 2003 VTC 2003- Fall*, Vol. 1, pp.557 – 561, 6-9 Oct. 2003.
[4]. Wiegandt, D.A., Nassar, C.R., and Wu, Z., "The elimination of peak-toaverage power ratio concerns in OFDM via carrier interferometry spreading codes: a multiple constellation analysis," *Proceedings of the Thirty-Sixth Southeastern Symposium on System Theory, 2004*, pp.323 –327, 2004.
[5]. Zhiquang Wu, Nassar, C.R. and Xiaoyao Xie, "Narrowband interference rejection in OFDM via carrier interferometry spreading codes," *Global Telecommunications Conference, 2004 GLOBECOM '04. IEEE*, Vol.4, pp.2387– 2392, 29 Nov.– 3 Dec. 2004.
[6]. Wiegandt, D.A., Wu, Z. and Nassar, C.R.; "High-performance carrier interferometry OFDM WLANs: RF testing," *ICC '03. IEEE International Conference on Communications*, Vol. 1, pp.203 – 207, 11- 15 May 2003.
[7]. Anwar.K and Yamamoto.H., "A new design of carrier interferometry OFDM with FFT as spreading codes," 2006 IEEE Radio and Wireless Symposium, pp.543-546,17-19 Jan. 2006.
[8]. Xu, Fang; Xu, Ru and Sun, Haixin, "Implementation of Carrier Interferometry OFDM by Using Pulse Shaping Technique in Frequency Domain," *2007 IEEE International Workshop on Anti-counterfeiting, Security, Identification*, pp.319–323, 16-18 April 2007.
[9]. Albert van Zelst, "MIMO OFDM for wireless LANs", April-2004.

Edge Colour Moments: An Enhanced Feature Descriptor for Content Based Image Retrieval

S.Selvarajah [1] and S.R. Kodituwakku [2]

[1] *Department of Physical Science, Vavuniya Campus of the University of Jaffna, Vavuniya, Sri Lanka*
[2] *Department of Statistics & Computer Science, University of Peradeniya, Sri Lanka,*
{shakeelas@mail.vau.jfn.ac.lk, salukak@pdn.ac.lk}

***Abstract*: Colour is one of the important features used in Content Based Image Retrieval (CBIR) systems. Colour moment is one such widely used feature. Image indexing using colour moments does not take spatial information of an image into account. This paper presents an enhanced colour moment for content based image retrieval. This method takes edge information into account. Colour distribution of image pixels are analyzed for three types of edges: two directional edges and one non-directional edge. Three distance measures are computed based on the colour distribution of each edge type and they are combined to obtain a similarity measurement for retrieval. The method is tested with publicly available image databases. Experimental results show improvement of retrieval quality as compared to that of traditional colour moments. It could be used to achieve good retrieval performance for CBIR.**

***Keywords*:** Image Retrieval, Colour moments, Directional edges, Non-directional edges.

1. Introduction

Content Based Image Retrieval (CBIR) has been an active research area in the last two decades. Traditional systems represent image contents only by text annotations and this approach has several limitations. CBIR combines digital image processing techniques with database techniques to retrieve images.

In CBIR systems, images are automatically indexed by summarizing their visual features. A feature is a characteristic that can capture a certain visual property of an image either globally for the entire image or locally for regions or objects. Color, texture and shape are commonly used features in CBIR systems. Although some new methods such as the relevance feedback have been proposed to improve the performance of CBIR systems, low-level features still play an important role [1-5].

A key function in any CBIR system is the feature extraction. Mapping the image pixels into the feature space is known as feature extraction. Extracted features are used to represent images for searching, indexing and browsing images in an image database. Use of feature space is more efficient in terms of storage and computation.

Most of the CBIR systems represent the feature space as a feature vector. Once the features are represented as a vector it can be used to determine the similarity between images. CBIR systems use different techniques to measure similarity.

In retrieval stage, query image is also represented as a feature vector and the similarity between the query vector and stored feature vectors is computed. The similarly measure is used to determine the distance between the query image and stored images. After that images are ranked according to the distance and retrieved.

A very basic issue in designing a CBIR system is to select the most effective image features to represent image contents. Many low-level features have been researched so far. Among those visual features, colour is considered as the most dominant and distinguish feature. The use of object-specific information of images is essential for efficient image retrieval. Many object feature based approaches use colour feature as an object internal feature [6]. Edge is a local shape feature and it captures the general shape information in the image [7]. Therefore, edge information is another frequently used feature in image retrieval.

Since colour and shape features capture different aspects of images, their combination could be useful in representing the image contents. Therefore, some pioneer works attempted to characterize the colour and shape information of an image in one feature representation. However, despite many research efforts, the existing low-level features are still not powerful enough to represent image content. Currently, the shape features along with colour have been intensively researched [8]. In this experiment, the colour distribution of pixels that belong to the edges is considered as an internal feature of edge shape descriptor.

This paper proposes an enhanced low-level feature, named edge colour moments, for representing image contents. It integrates the colour and shape characteristics of an image in to one compact form by combining edge information and colour information.. Three categories of colour moments are computed: two for directional edges and one for non-directional edge that is the combination of horizontal and vertical edges. Preliminary experimental results show that the proposed feature achieves better performance than many existing low-level features.

2. Methods and Materials

In order to develop an enhanced feature descriptor low-level image descriptors are considered.

2.1 *Materials*

To develop an enhanced feature the following low-level descriptors are analyzed.

2.1.1 Colour moments for image retrieval

According to the probability theory, a probability distribution is uniquely characterized by its moments. If the colour distribution is interpreted, the colour distribution can be characterized by its moments [9]. Moreover, most of the colour distribution information can be captured by the low-order moments. Using only the first and second moments is a good approximation and has been proved to be efficient and effective in representing colour distribution of images [10]. The mean, standard deviation, and skewness of an image are known as colour moments. Following equations define the mean and standard deviation of an image of size $n \times m$.

$$mean = \sum_{i=1}^{n}\sum_{j=1}^{m} x_{ij} / mn \qquad (1)$$

$$stdev = \sqrt{\frac{1}{nm}\sum_{i=1}^{n}\sum_{j=1}^{m}\left(X_{ij} - mean\right)^2} \qquad (2)$$

where X_{ij} is the Pixel value of the i^{th} row and j^{th} column.
These colour moments do not involve local relationships among the neighboring pixels.

2.1.2 Colour distribution around the edges

Edge is a local shape feature and it captures the general shape information in the image [7, 9]. The changes of colour in an image occur at the colour edges. Therefore, the colour distribution on the pixels around colour edge is very similar to that of entire image. So the colour distribution of pixels around edges could be used in describing image instead of considering all pixels in an image.

2.1.3 Similarity measurements

Eight similarity measurements have been proposed and used [11]. In this work, Sum-of-Absolute Differences (SAD) method is used. The Sum-of-Absolute Differences is defines as follows.

$$SAD\left(f_q, f_t\right) = \sum_{i=o}^{n-1}\left(1 f_q[i] - f_t[i]\right) \qquad (3)$$

Where f_q and f_t represent query feature vector and database feature vectors, and n is the number of features in each vector.

2.2 Methodology

The first step in computing edge colour moments is to find directional and non-directional edges in an image. The edges from colour image are detected by using the method proposed in [12].

First the colour image is transformed to the HIS colour space and then the hue channel is neglected. The other two channels are convolved with the vertical and horizontal Sobel operators. Next the resulting gradient images are threshold to binary images by a suitable threshold value for each channel. The threshold value for intensity gradient image is manually fixed to 15% of the maximum gradient value. For the saturation image the threshold value is fixed to 30% of the maximum gradient value. These manually fixed threshold values are selected by testing several threshold and the same threshold values are used for all images.

The directional gradient edge image is computed in two steps. First, the thresholded horizontal components of the intensity gradient image and saturation gradient image are combined by the logical OR operator. Then the same procedure followed to the vertical components of the intensity gradient image and saturation gradient image. Next the non-directional gradient edge image is computed by adding the directional gradient edge images. These three binary edge images are dilated one time by taking pixels on both sides of the edges into account. Finally colour moments, mean and standard deviation, are computed by considering only the pixels whose intensity value is 1 on the previously computed binary edge images. The extracted features are stored in a database.

Using the Euclidean distance given in equation (3) three distance measures are computed based on the colour distribution of each edge type and they are combined to obtain a similarity measurement for retrieval. When a query image is given, its mean and standard deviation are extracted and stored in a feature vector. They are compared against features stored in the feature database. The difference between the query features and target features are calculated and stored in a database. All the images are indexed according to the difference between query features and database features.

A general purpose image database consists of 1000 images is used for experimentation [13]. The database consists of different categories such as Africans and villages, Beaches, Buildings, Buses, Dinosaurs, Elephants, Flowers, Horses, Mountains and glaciers, and Food. All the categories are used for retrieval. These images are stored in JPEG format with size 384x256 and 256x384. Each image is represented with RGB colour space. In order to measure retrieval effectiveness for an image retrieval system, precision values are computed. Ten different images of each category are used as query images. These images are selected so that some of them have uniform colour distribution, some others have non-uniform colour distribution and the other having average colour distribution. In this experiment, only the top 50 images are chosen as the retrieval results.

3. Results and Discussion

The experimental results for different categories of images with traditional moments and the proposed descriptor are given in Table 1.

Table 1: An average retrieval accuracy of colour moments & Edge colour moments

Category	Average Precision	
	Colour Moments	Edge Colour Moments
Africans and villages	0.28	0.60
Beaches	0.32	0.52
Buildings	0.16	0.40
Buses	0.28	0.34
Dinosaurs	0.84	0.96
Elephants	0.04	0.32
Flowers	0.82	0.98
Foods	0.60	0.78
Horses	0.44	0.54
Mountains and glaciers	0.30	0.66

4. Conclusions

In this paper, an enhanced image descriptor, edge colour moments, is proposed. It investigates colour statistics for the pixels of three types of edges: two directional edges and one non-directional edge. The proposed image descriptor captures more information by considering the colour feature and local shape feature.

Experimental results show that proposed edge colour moments descriptor outperforms traditional colour moments. Performance could be further improved by considering four directional edges or eight directional edges. The proposed edge colour moments are efficient and could be used in many applications where traditional colour moments are applied.

Reference

[1]. Chang S.K., and Hsu A. (1992), "Image information systems: where do we go from here?" IEEE Trans. On Knowledge and Data Engineering, Vol. 5, No. 5, pp. 431-442.

[2]. February, (1995), Smulders A.M.W., Worring M., Santini, A. S., Gupta, and R. Jain (2000), "Content-based image retrieval at the end of the early years," IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol.22, No. 12, pp. 1349-1380.

[3]. W. Y. Ma, H. J. Zhang, (1998), "Content-based Image Indexing and Retrieval", In Handbook of Multimedia Computing, Borko Furht. Ed., CRC Press.

[4]. Faloutsos C. et. al. (1994), "Efficient and effective querying by image content, "Journal of intelligent information systems, Vol.3, pp.231-262.

[5].Rui Y. and Huang T. S (1997), Image retrieval: Past, Present, and Future, Journal of Visual Communication and Image Representation.

[6]. Sami Brandt, Jorma Laaksonen and Erkki Oja, (2000), "Statistical Shape Features in Content Based Image Retrieval", Proceddings of 15th International Conference on Pattern Recognition, Vol.2, , pp1062-1065.

[7]. A.K. Jain and A.Vailaya, (1996), "Image Retrieval Using Color and Shape", Pattern Recognition, 29(8), pp.1233-1244.

[8]. M.Swain and D.Ballard, (1991), "Color indexing", International Journal of Computer Vision, 7(1):11-32.

[9]. M. Stricker and M. Orengo, (1995), "Similarity of color images", Proc. SPIE on Storage and Retrieval for Image and Video Databases, Vol. 2420, pp. 381-392, San Jose, USA,

[10]. W. Y. Ma and H. J. Zhang, (1998), "Content-based Image Indexing and Retrieval", In Handbook of Multimedia Computing, Borko Furht. Ed., CRC Press.

[11]. Dengsheng Zhang and Guojun Lu, (2003), "Evaluation of similarity measurement for image retrieval", IEEE Int. Conf. Neural Networks & Signal Processing Nanjing, China, December 14-17.

[12]. International Organization for Standardization Organization Internationale De Normalization ISO/IEC JTC1/SC29/WG11 Coding of Moving Pictures and Audio, ISO/IEC JTC1/SC29/WG11 N4031, Singapore, March 2001.

[13]. http://wang1.ist.psu.edu/, Accessed on 30/12/2010.

Author Biographies

Saluka Ranasinghe Kodituwakku is an associate professor at the Statistics and Computer Science Department, University of Peradeniys, Sri Lanka. His research interests are database systems, distributed computing and software engineering.

S. Selvarajah is a lecturer at the Department of Physical Science, Vavuniya Campus of the University of Jaffna, Vavuniya, Sri Lanka and a MPhil student at the Postgraduate Institute, university of Peradeniya, Sri Lanka.

Shape Detection Model for Redrawing of Basic Geometric Objects

Aihab Khan[1], Javeria Sadaf[1], Malik Sikandar Hayat Khiyal[1],
Saba Bashir[2], Farhan Hassan Khan[2]

[1]*Dept. of Computer Science, Fatima Jinnah Women University, Rawalpindi, Pakistan*
[2]*Computer Engineering Dept., National University of Science and Technology, Islamabad, Pakistan*
aihabkhan@yahoo.com,javeria.sadaf@hotmail.com,m.sikandarhayat@yahoo.com,
saba.bashir3000@gmail.com,mrfarhankhan@gmail.com

Abstract: Object extraction is very useful due to great momentum in computer technology and especially in the field of image processing. It is used in many object related image processing applications such as object recognition. Printed data becomes discolored with the passage of time and graphical data gets deteriorated. Recognition and then redrawing through classification technique has been used to overcome these problems. Flow charts have been used to derive out the basic geometric objects. Extraction of the geometric objects has been accomplished by the proposed algorithm. The proposed research has presented a shape detection model that can be acquainted with the basic geometric objects. Recognition of objects is carried out by observing different features of the geometric objects. Classification of the objects is carried out by the proposed algorithm. The proposed model is competent of recognizing the objects and it is applicable on basic geometric objects in two dimensional images.

Keywords: *geometric objects, object extraction, object recognition, rectangularity.*

1. Introduction

Image processing is often referred to as digital image processing. It is any form of signal processing for which image is given as input, such as pictures or frames of video, the output after processing can be either image or set of attributes related to that image [3,8]. Object extraction is very useful in many image processing purposes such as object recognition [6]. Geometric objects, used in 3D representational relevance, are simple units such as points, lines, circles, polygon and rectangle etc. Some applications use only simple geometric entities such as lines and arcs; others require sculptured curves and surfaces. Geometric algorithms are utilized for creation and amendment of geometric objects and solving geometric tribulations [7]. A flow chart is characterized as a graphic illustration, unfolding a process being studied. Flow charts have a tendency to use simple and easily identifiable symbols for example oval, rectangle, line etc. [2]

The proposed analytical research approach provides a technique that is able to preserve and safeguard the graphical data. It can be used to restore them through the redrawing technique in the field of image processing.

The paper is organized as follows; Section 2 describes related work. Framework of the proposed technique is given in section 3. Section 4 presents the model algorithm and technique. Section 5 shows the experimental results. Finally, conclusions and future work is given in Section 6**.**

1.1. Contributions

The contribution of proposed analytical research is stated below.

- *To preserve and safeguard the graphical data from old registers by restoring them through the redrawing technique.*
- *To propose a model that detects the basic structure of the objects.*
- *To classify the objects on the basis of their geometric properties.*

2. Related Work

Karl Tombre [4] describes that graphics recognition is concerned with the analysis of graphics-intensive documents. Vectorization, i.e. raster–to–vector conversion, is a central part of graphics recognition problems. It deals with converting the scanned image to a vector form that is suitable for further analysis. Another major problem in vectorization process is precision, robustness and stability. The proposed system, as implied by the name, raster–to–vector conversion consists of analyzing a raster image. It converts pixel representation into a vector representation. Designing of vectorization involves many raster-to-vector conversion methods. The proposed approach describes that skeletons are computed for vectorization from distance measures.

In [1] Henri Achten describes that graphical representations constitute a major means of communication for an architect. The proposed framework implements the findings on graphic units in drawing system to interpret them. This implementation helps to understand the scope and limitations of the theory of graphic units and generic representations.

Henri Achten discussed how graphic unit recognition can take place using a multi-agent systems approach.
In [5] Liu Wenyin describes that graphics are used for describing and sharing ideas, thoughts and knowledge. Human beings and machines share information that is processed by machines. However, the process for efficiently using graphics input machines is a non-trivial problem. To overcome this problem, a digital pen is used for drawing sketches on a tablet to input graphics. This freehand graphics provide immediate and useful feedback to the user so he is able to realize errors and inappropriateness. This immediate recognition and conversion is referred to as online graphics recognition. It determines the type and parameters of its primitive shape and redisplays it in its regular form.

3. Framework Overview

The description of proposed framework is shown in Figure 1. It illustrates that the input of the system is a scanned image. After loading the image, it is essential to distinguish between the objects of interest and "the rest". The technique that is used to find the object of interest is referred to as "segmentation". Iterative threshold selection and application is used to get the binary image.
After that, thinning is applied, it is necessary for detachment of the objects. It thins the objects by one pixel. Detection of objects is done by applying an algorithm. This algorithm disconnects the objects. For the affair of recognition of objects, geometric property, rectangularity is pertained. Classification of box and oval is accomplished by algorithm.

4. Proposed Technique

The proposed technique describes that logical design of the system includes a block diagram. It shows the sequence of operations performed in the system. These operations have been described as shown below.

4.1. Point detection

Point detection algorithm is used to separate the objects from each other as shown below. Algorithm shows the process of separation of joining point. The objects of interest are needed to be disjoined in order to assign labels.

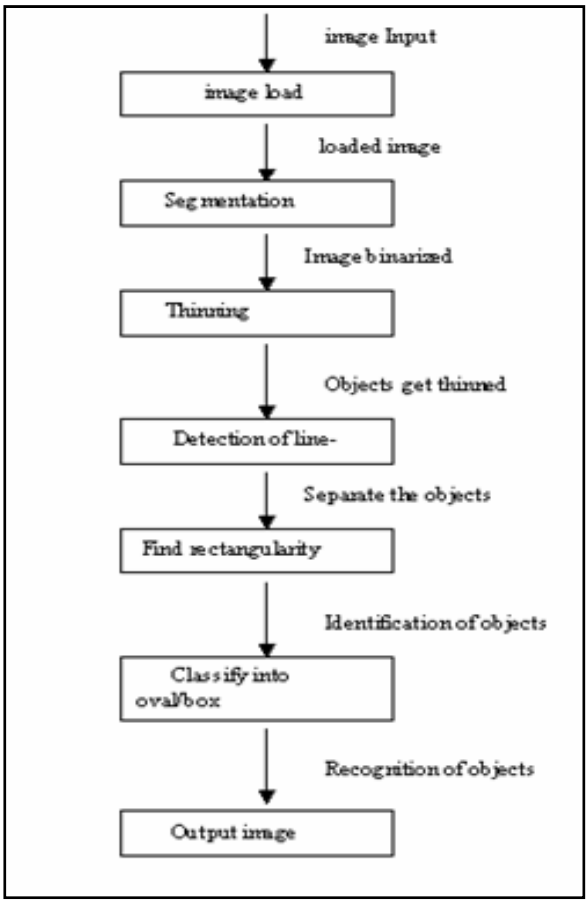


Figure 1: Block diagram of testing phase

Figure 2: Series of operations performed in the system

Algorithm: Series of operations performed in the system()
Input: scanned image
Variables: i, j, level, D, D2, D3
MatLab Functions: imread(), find(), logical(), im2uint(), imadjust(), bwmorph().
Output: a thinned image.
// Read an image.
1. i = imread('flowchart_new.jpg');
// To convert a grayscale image to BW, set a threshold point.
2. level = 170;
// Pixels less than threshold point convert to black.
3. j(find(j<level))=0;
// Pixels greater than threshold point convert to white.
3. j(find(j>=level))=1;
4. D = logical (j);
// To convert grayscale to bw.
5. D=im2uint8(D);
// To thin the lines by one pixel , take image negative.
6. D3=imadjust(D,[0;1],[1;0]);
// To thin the lines by using function "bwmorph()".
7. D2 = bwmorph(D3,'thin',1);

Algorithm: point detection ()
Input: bw (black n white) image
Variables: count, s, u, v
Output: broken image

```
for loop' 1 to  number _of_ rows
Count=0
'for loop' 1 to number _of _columns
if  pixel value j>1 then
If previous pixel is white and current pixel is black
 then
if previous pixel is black and current pixel is white
then
Count ++
endif
end
end
end
end
variable 's'=0
u (current row value) = 0
v (current column value) = 0
'for loop' 1 to number _of_ row
count=0
'for loop' 1 to number _of_ columns
      if current pixel is white
then
count=count +1
u(current row value) = i(variable  stores number _of_ rows)
v(current column value) = j(variable  stores number _of_ columns)
end
end
if  count >1 & s (current pixel) is white
then
s = 0
end
if count==1 & s (current pixel) is black
 then
u (display value of current row)
v (display value of current column)
 image(u, v) = 255 (make current pixel white)
s = 1
end
end
```

Figure 3: Point detection algorithm

4.2. Connected Component Labeling

For connected-component labeling, "bwlabel" function is used. By connected-component labeling function, different colors are assigned to the objects for distinguishing them.

4.8.

4.3. Bounding Box

To recognize the objects, bounding box is applied. Bounding box is the smallest rectangle containing the region. It bounds to specify the upper left corner and the width of bounding box along each dimension.

4.4. Find Rctangularity

Rectangularity is needed to be calculated in order to classify the geometric objects. Height, width and area of bounding boxes are calculated for finding rectangularity as shown below.

Algorithm: Rectangularity()
Secret keys: height, width, area.

```
number_of_rows i=1
for loop number_of_columns j=variable s3 (stores the rows and columns of bounding box)
then
// find the of area of the region.
area()       = stats().Area;

//To find width of bounding box.
bbox_width(i)  = stats(j).BoundingBox(3);

//To find height of bounding box.
bbox_height(i) = stats(j).BoundingBox(4);
// To find rectangularity
rectangularity(i) = area(i)/(bbox_width(i)*bbox_height(i));
i = i+1;
end
```

Figure 4: Finding Rectangularity

4.5. Classification of objects

Classification of box and oval is made by applying an algorithm given below.

Algorithm: Classification of objects ()
Input: image with bounding box around objects
Secret keys: Stats (measures properties of image regions), Rectangularity (geometric properties of image regions).
Output: values of rectangularity that the objects of image hold.

```
'for' loop from 1 to length(stats) (measure properties of image regions)
Rectangularity= stats (i). Area of the region/Area of the Bounding box
if rectangularity is > 0.8 then
disp ' rectangle'
end
if rectangularity is > 0 &  rectangularity is < =0.8 then
disp 'circle'
end
end
```

Figure 5: Objects classification algorithm

5. Experimental Results

Figure 5 shows the image with original features. No modifications have been made in the image primarily.

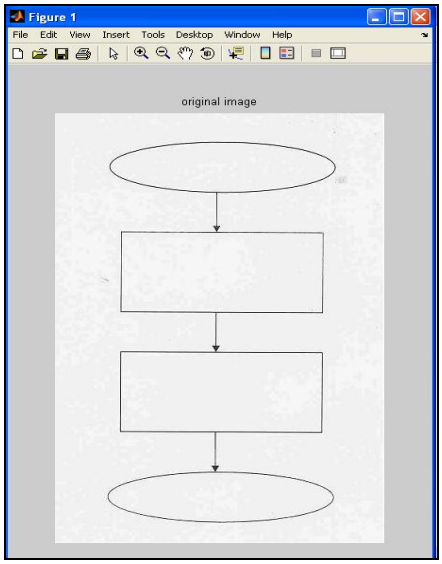


Figure 6: Image with original features

Figure 6 shows the changes occurred in image after segmentation. In Figure 7, image has been converted from gray scale to binary (BW) image.

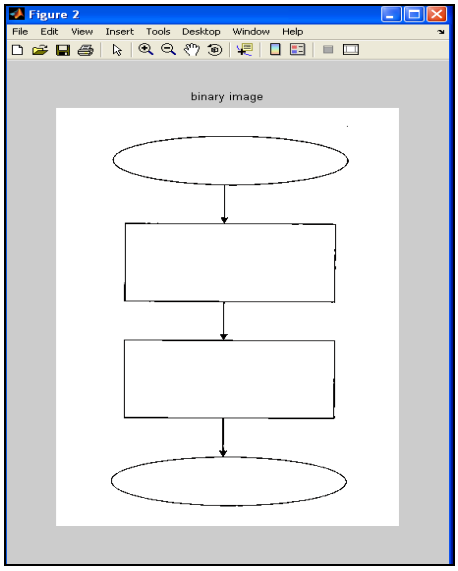


Figure 7: Binary image

Figure 8 shows a thinned image. Thinning process is essential for disjoining of connected objects. Figure depicts the changes occurred in binarized image when thinning function is applied.

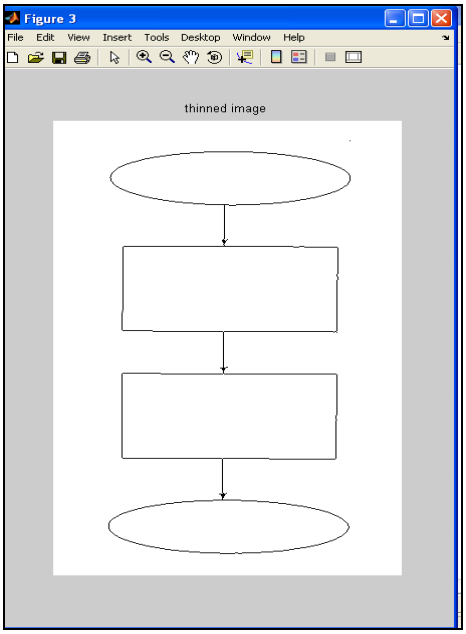


Figure 8: Thinned image

Figure 9 shows the broken points of image by applying the algorithm given in section 4, figure2.

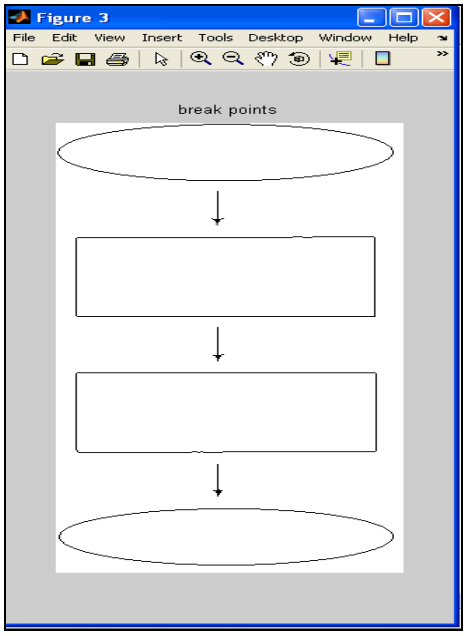


Figure 9: Break points

Figure 10 shows the image when "Connected component labeling" function assignes different colors to objects.

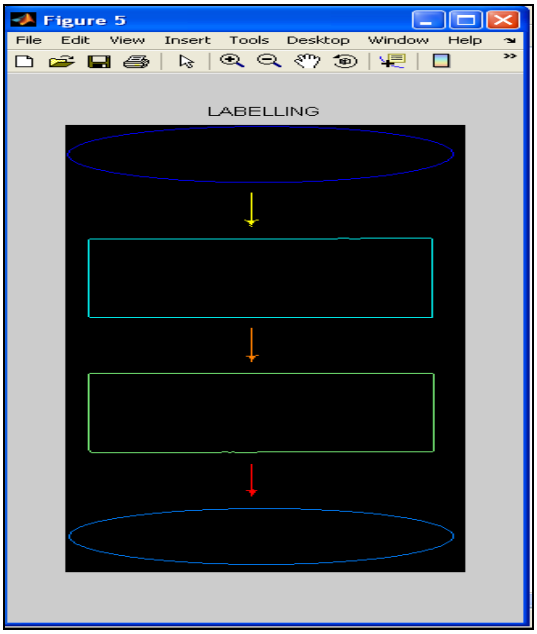


Figure 10: Connected Component Labeling

After applying connected component labeling, bounding box is applied. This makes rectangles around all the objects. The resultant image after applying bounding box is shown in the Figure 11.

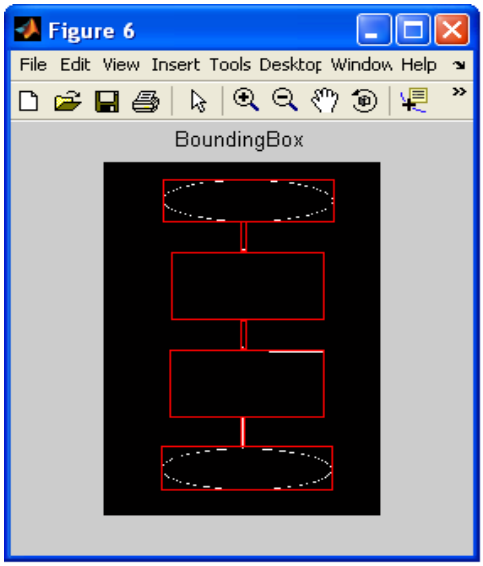


Figure 11: Bounding box

After application of bounding box, the rectangularity of all objects is found by the algorithm. Algorithm concluded the result that rectangularity of the object greater than 0.8 is a rectangle, and rectangularity which is between 0-0.8 is an oval, as shown in Figure 8.

UL-corner(y) = 31.5, Rectangularity = 0.744, CIRCLE

UL-corner(y) = 143.5, Rectangularity = 0.986, RECTANGLE

UL-corner(y) = 293.5, Rectangularity = 0.990, RECTANGLE

UL-corner(y) = 443.5, Rectangularity = 0.750, CIRCLE

Figure 12: Rectangularity of the objects

6. Conclusion and Future Work

The proposed system describes the redrawing of basic geometric objects which lies under extraction of objects technique. Extraction identifies the objects in image, recognize them and then redraw the objects. Extraction of objects is carried out by the proposed algorithm. Recognition of objects is carried out by observing different features of the geometric objects. This paper describes the algorithm for calculating rectangularity. For the matter of extraction of line, scanning of black pixels is conducted. It is concluded that the single crossing of black pixels contained the object, line. For the extraction of oval and rectangle, the geometric property of objects, that is rectangularity, is observed. It is concluded that rectangularity greater than 0.8 is a rectangle, and between 0-0.8 is an oval.
In the proposed research, 2-D is used for the enhancement of 2-D images. The work can be expanded to the 3-D images. This research work is applicable only for the basic geometric objects. The research work can also be extended to complex geometric objects like cone, polygon and cylinder etc. The objects are extracted through static method. In future this problem can be overcome by the extended object extraction algorithm that will automatically detect and recognize the objects.

References

[1] D. Forsyth, J. Malik, M. Fleck, and J. Ponce. Primitives, perceptual organization and object recognition. Technical report, Computer Science Division, University of California at Berkeley, Berkeley, CA 94720, 1997.

[2] http://www.edrawsoft.com/Flow-Chart.php

[3]http://en.wikipedia.org/w/index.php?title=Imageprocessing&oldid=315909322

[4] K. Tombre and S. Tabbone. Vectorization in GraphicsRecognition: To Thin or not to Thin. In Proceedings of the 15th International Conference on Pattern Recognition, Barcelona (Spain), September 2000.

[5] Wenyin, L. (2003). On-Line Graphics Recognition. International Workshop on Graphics Recognition, Department of Computer Science City University of Hong Kong, Hong Kong SAR, PR China

[6] Yi-Wei Jan, Jyh-Jong Tsay, Bo-Liang Wu, "WISE: A Visual Tool for Automatic Extraction of Objects from World Wide Web," wi, pp.590-593, 2005 IEEE/WIC/ACM International Conference on Web Intelligence (WI'05), 2005

[7] Paul L. Rosin, Measuring shape: ellipticity, rectangularity, and triangularity, Machine Vision and Applications, v.14 n.3, p.172-184, July 2003

[8] R. P. Futrelle and N. Nikolakis. Efficient analysis of complex diagrams using constraint-based parsing. In ICDAR-95 (International Conference on Document Analysis and Recognition), pages 782–790, Montreal, Canada, 1995.

User Authentication for Password Login Phishing Based Attack

Shumaila[1], Aihab Khan[1], Mailk Sikandar Hayat Khayal[1], Syed Afaq Hussain[2]
[1]*Dept. of Computer Science, Fatima Jinnah Women University, Rawalpindi, Pakistan.*
[2]*Faculty of Applied Sciences, Riphah International University, Islamabad, Pakistan.*
shumailakhan_08@yahoo.com,aihabkhan@yahoo.com,m.sikandarhayat@yahoo.com,
drafaqh@gmail.com

Abstract: **A password is a top secret string that is used for authentication purposes and to provide access to a resource. Therefore it is more vulnerable to attacks such as hacking, phishing, identity theft, Cyber stalking and website cloning. But the phishing is the fastest growing threat in the history of internet and the baggiest assault on online banking. In this attack the malicious user masquerades as trusted entity and attempts to steal the personal sensitive information.This research is formulated to protect the resource from unauthorized user .The user is authorized by allocating him a digital certificate and password is made secure from unauthorized user by password hashing with addition of salt. AES encryption algorithm is used to prevent the fraudulent actions on digital certificates issued by the certification authority. SHA 256, SHA 384, and SHA 512 are used frequently for the hashing purpose. These algorithms are than compared w.r.t time, memory, password hash size and throughput and found that SHA 512 is slower but more secure as compared to others. AES encryption algorithm is also compared with the other encryption algorithms w.r.t time, memory, size of file after encryption and throughput and we have concluded that AES is efficient and more secure than the other encryption algorithms.**

Keywords: Encryption, Cryptographic Hash Function, Password, Salt value

1. Introduction

A password is a top secret string that is used for authentication purposes and to provide access to a resource. It is used for the security purpose that provides control to only a restricted group of users who know the password. The security measures are always taken so that it is not easily accessible by phishers or hackers. A typical computer user needs the passwords in many respects e.g. logging into computer logins, accessing files, databases, retrieval of emails from servers and network websites. If digital criminals or other malicious users succeed in stealing the password then he can misuse the sensitive information.

As we are living in the era of digital technology and the most of people in the 'developed' world now handling their accounts, travel plans, meetings and shopping in general through the Internet, which was not possible in the past [1]. Internet fraud becomes a great threat to people's internet life. Internet fraud is an attempt to trick or deceive the internet users. Victims are mostly those people who are having online bank accounts. So the person who is being tricked suffers from financial loss as he loses to the people scamming them. Internet fraud can take place on computer programs such as e-mail, chat rooms, message boards, or web sites. Advertisements that come in form of pop up window on the websites have a major threat of being scams [2]. As the malicious users are always busy in attempting to steal the sensitive information. So recourse must be protected from the malicious users. The research has been conducted to provide security for internet users by User authentication.

1.1Contributions

Number of solutions has been presented to prevent the phishing attack. There are many solutions like introducing new protocols, new trust indicators and new user models [3].

This research is formulated to protect the resource from unauthorized user .The user is authorized by allocating him a digital certificate and password is made secure from unauthorized user by password hashing.

The division of this paper is as follows, in section 2 related work is given. In section 3 we discuss a proposed model. In Section 4, we show the experimental results. Finally, closing remarks are made in Section 6.

2. Related Work

There has been a great work done from last few years since the phishing has been materialized as an internet threat. Halderman et. al [4] refined their scheme in a tool called Password Multiplier, which caches an intermediate hashing result on the user's machine to make logins faster for valid users. They use the technique of Kelsey et al, which is "key-stretching" via repeated application of a hash function. Ashraf et. al [5] analyze a technique of password hashing, to compute secure passwords. By applying a cryptographic hash function to a string consisting of the submitted password and, usually, another value known as a salt they obtain hash value. MD5 and SHA1 are frequently used cryptographic hash functions. They implemented these algorithms and found that SHA-1 is more secure but slow in execution as SHA-1 includes more rounds than MD5 in calculating hashes. Mikhail J. Atallah [6] presents a watermarking based approach, and its implementation, for mitigating phishing attacks - a form of web based identity theft. ViWiD is an integrity check mechanism which is based on visible watermarking of logo images. ViWiD performs all of the computation on the company's web server and it does not require installation of any tool or storage of any data, such as keys or history logs, on the user's machine. To prevent the "one size fits all" attacks he watermark message is designed to be unique for every user and carries a shared secret between the company and the user.

3. Proposed Model

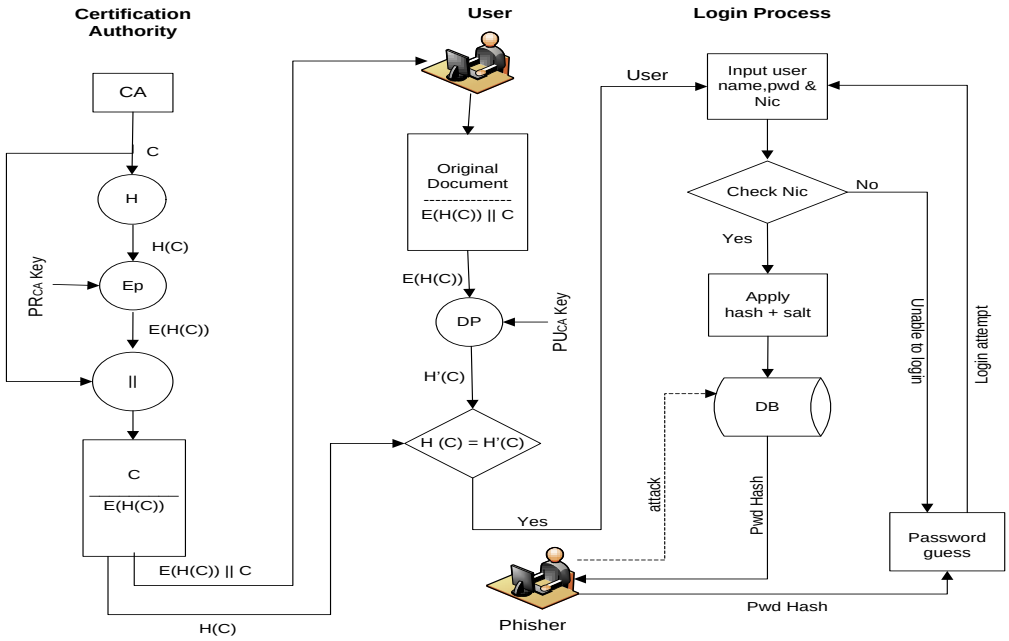


Figure 1: Cryptographic Model of User authentication for password login phishing based attack

The Certification Authority issues a Certificate and produces the message digest of the certificate and then Certification Authority will generate the message signature of the Certificate with the help of its private key PR_{CA} and send the Original Certificate along with the message signature to the user. User will decrypt the document with the public key PUCA of the Certification Authority and generate the message digest of the original certificate and then compare message digest of the certificate with the message digest of the original certificate to authenticate the website. The user will provide the username, NIC and password to login to the website. The password provided by the user is hashed by the addition of salt and then save to the database to prevent from the unauthorized user.

Algorithm

Step 1

The Certification Authority issues a Certificate (C) and produces the message digest H(C) of the certificate.

Step 2

The Certification Authority (CA) will generate the message signature E (H(C)) of the Certificate with the help of its private key PR_{CA} and then send the Original Certificate (C) along with the E(H(C)) and its public key PU_{CA} to the user.

Step 3

User will decrypt the document with the public key PUCA of the CA and generate the message digest H′(C) of the original certificate and then compare H(C) with the H′(C) to authenticate the website.

Step 4

The user will provide the username and password to login to the website. The password provided by the user is hashed by the addition of salt and then save to the database to prevent from the unauthorized user.

4. Experimental Results

Comparison of Different Hash algorithm

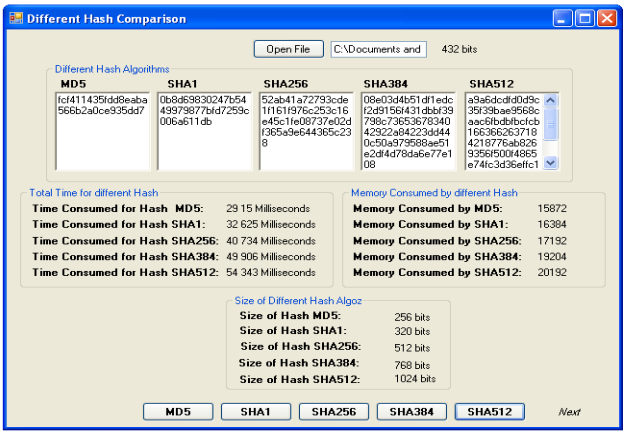


Figure 2: Different Hash algorithm Comparison

MD5, SHA1, SHA256, SHA384 and SHA512 are compared with respect to time consuming in calculating hash of file, memory consumed for each hash function, size after calculating hash of file and throughput for each hash algorithm by keeping the actual message size constant and their results are shown in the following table.

Table 1: Comparison Table for Different Hash Algorithm

Hash Algorithm	File Size	Consumed Memory	Time Consumed for Hashing	Msg Hash Size	Throughput
MD5	432 bits	15872 bytes	29.15 msec	256 bits	8.7 bits/ msec
SHA1	432 bits	16384 bytes	32.62 msec	320 bits	9.8 bits/ msec
SHA256	432 bits	17192 bytes	40.73 msec	512 bits	12.5 bits/ msec
SHA384	432 bits	19204 bytes	40.91 msec	768 bits	15.3 bits/ msec
SHA512	432 bits	20192 bytes	54.34 msec	1024 bits	18.8 bits/ msec

Different graphs obtained from the table values are

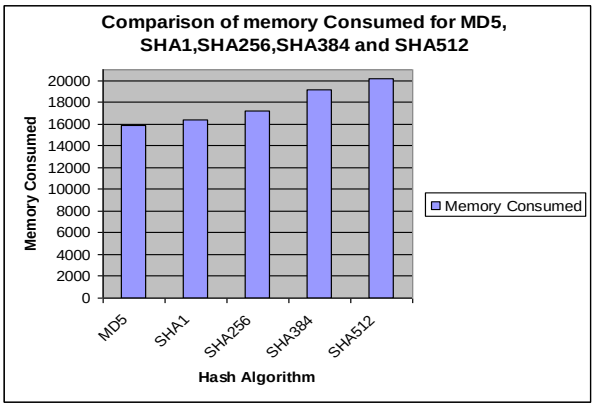


Figure 3: Memory consumed for different hash algorithm

The figure depicts the total memory consumed for different hash algorithms (MD5, SHA1, SHA256, SHA384 and SHA512). The memory is represented in bytes. We analyze that SHA512 consumes more memory than the SHA1, SHA256, SHA384 and MD5.

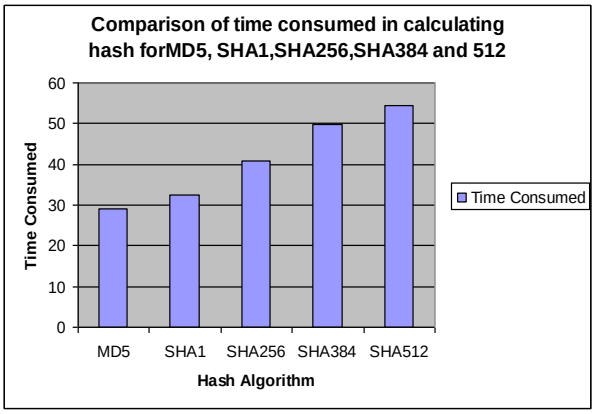


Figure 4: Time consumed in hash for different hash algorithm

This figure shows the time consumed in calculating hash for MD5, SHA1, SHA256, SHA384 and SHA512. Time is represented in milliseconds. It is analyzed SHA512 is slower than the other four algorithm because it takes more rounds to calculate hash than SHA1,SHA256,SHA384 and MD5 that takes four rounds making it more secure than MD5 ,SHA1,SHA256 and SHA384.

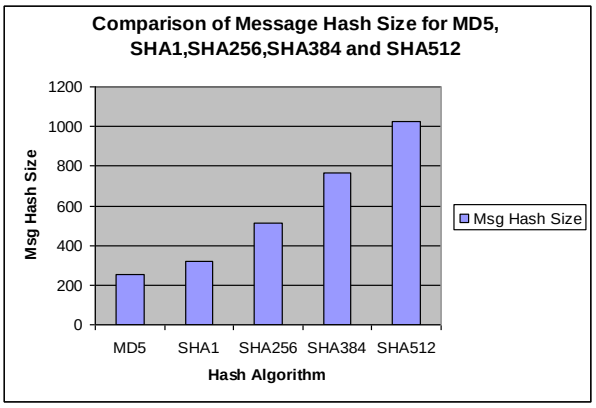


Figure 5: Message hash size for different hash algorithm

From the figure above we analyze that the Message hash size for SHA512 is also greater than the Message hash size of MD5 ,SHA1,SHA256 and SHA384 making it more complex to break than the other four.

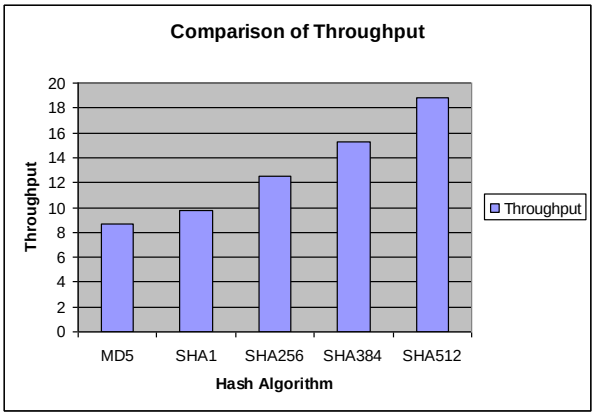


Figure 6: Throughput for different hash algorithm

In this figure throughput for MD5, SHA1, SHA256, SHA384 and SHA512 is compared. Throughput is calculated from the Message hash size and the total time consumed for calculating hash, therefore it is represented in bits per millisecond. SHA512's throughput is greater than MD5, SHA1, SHA256 and SHA384 which shows that it is more efficient than the other four with respect to the message hash size.

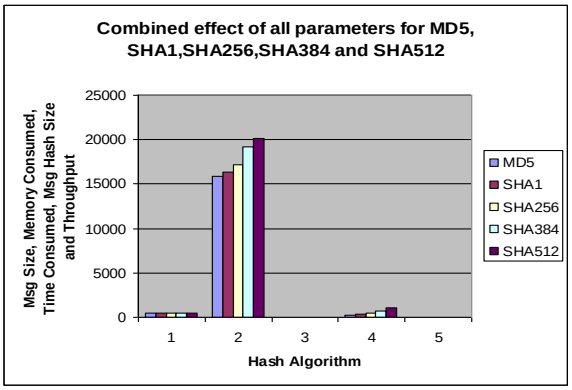


Figure 7: All parameters for different hash algorithm

Analysis

We have applied MD5, SHA1, SHA256, SHA384 and SHA512 hashing algorithms to compute hash of the message and analyses the time consumed in computing the hash, memory consumed in computing hash function, throughput and the size of the message after computing hash keeping the actual message size constant. By analyzing the table and figures we have concluded that SHA512 is more secure than MD5, SHA1, SHA256 and SHA384.

Comparison of SHA512 for different Message Size

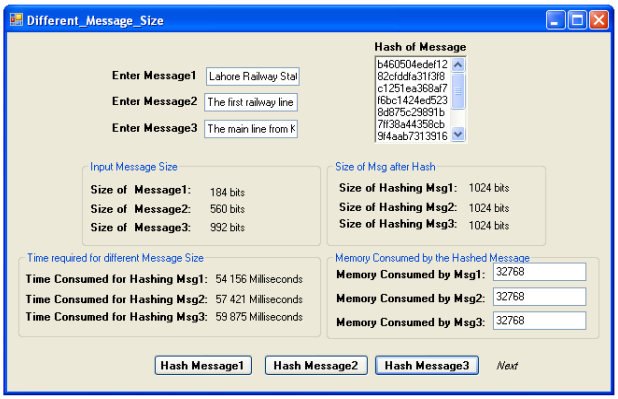


Figure 8: SHA512 Comparison for different Message Size

In this table all the above parameters are calculated for the message having different lengths by my technique SHA512.

Table 2: Comparison Table for SHA512 for different message size

Hash Algorithm	Message Size	Consumed Memory	Time Consumed for Hashing	Msg Hash Size	Throughput
SHA512	184 bits	32768 bytes	54.15 msec	1024 bits	3.3 bits/ msec
SHA512	560 bits	32768 bytes	57.42 msec	1024 bits	9.7 bits/ msec
SHA512	992 bits	32768 bytes	59.87 msec	1024 bits	16.5 bits/ msec

Following graphs are plotted from the table values

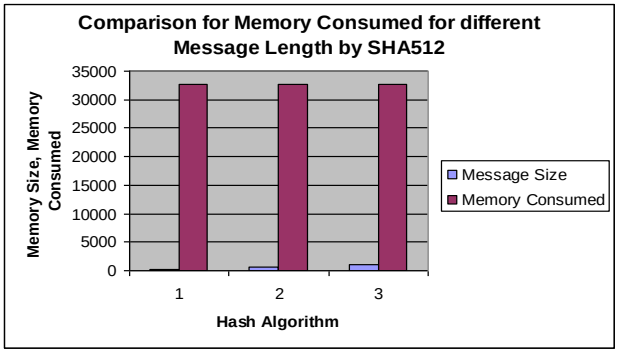


Figure 9: Memory consumed for different message length

We analyze that SHA512 function will consume same memory for the calculating hash of different message length because it produces the same hash size for any message size.

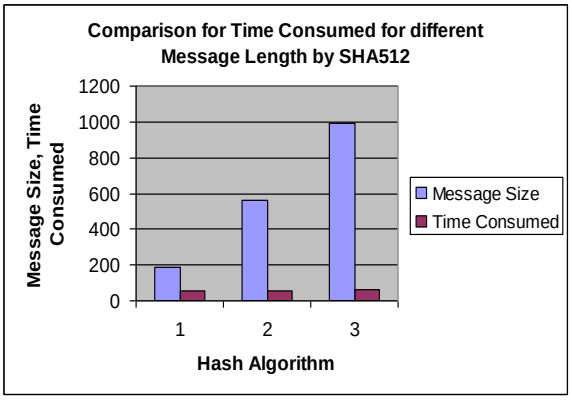


Figure 10: Time consumed for different message length

This graph depicts that SHA512 require more time to calculate hash of message having the greater length.

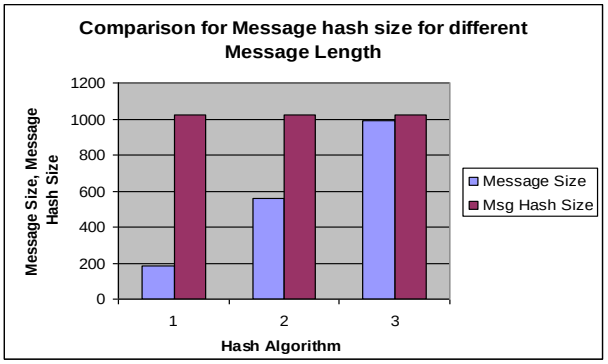


Figure 11: Message hash size for different message length

We observe from the figure that message size does not affect the message hash size because it produces the same hash size for any message size.

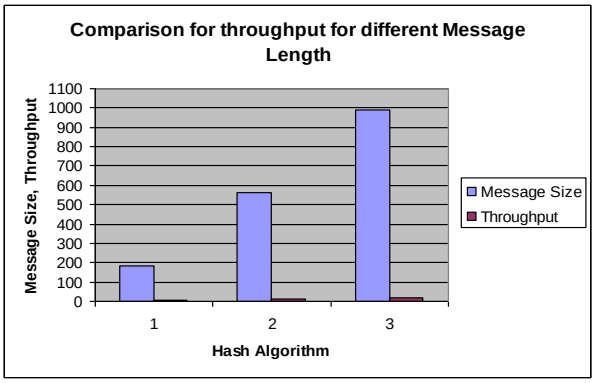


Figure 12: Throughput for different message length

We analyze that throughput differs a little bit by changing the message size. Here throughput is calculated by the actual message size and the time required for calculating hash.

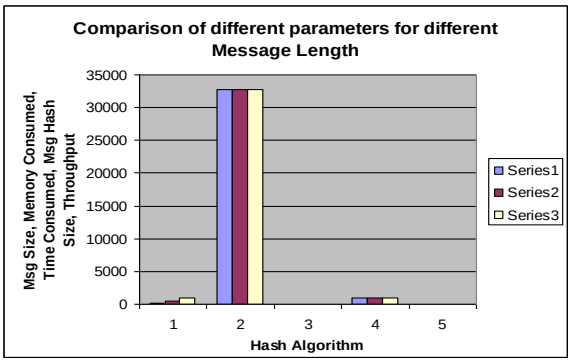


Figure 13: different parameters for different message length

Analysis

The figure depicts the different length message and calculates time consumed in computing the hash, memory consumed, throughput and the size of message after computing hash. From the figure we analyze that the message having more characters take more time for hashing but the size and memory of message after hashing is same for any length ensuring the message hash of any length equally secure.

Comparison of Different Encryption\Decryption Algorithm

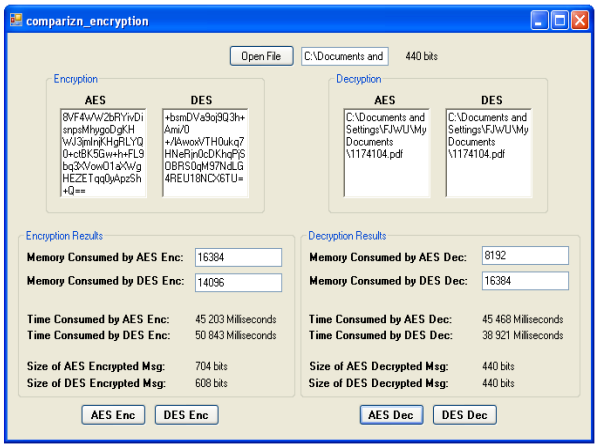


Figure 14: Different encryption and decryption algorithm Comparison

AES and DES Encryption and Decryption algorithm are compared with respect to consumed memory, time consumed, message size after encryption and throughput. And the values are shown in the following table.

Table 3: Comparison Table Encryption Algorithm

Encryption Algorithm	Message Size	Consumed Memory	Time Consumed for Encryption	Encrypted Msg SIze	Throughput
AES	440 bits	16384 bytes	45.21 msec	704 bits	15.5 bits/msec
DES	440 bits	14096 bytes	50.84 msec	608 bits	11.9 bits/msec

The following graphs are plotted from the calculated results

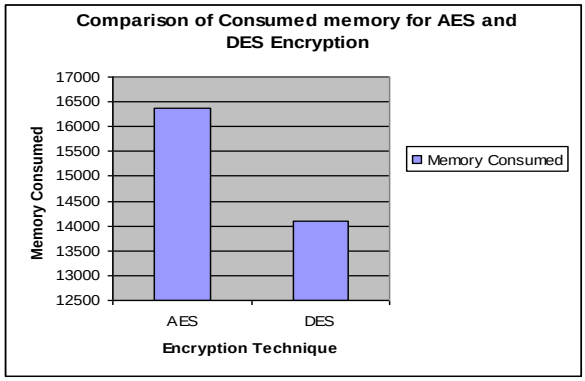


Figure 15: Memory consumed for AES and DES Encryption

It is observed that AES Encryption function consume more memory than the DES Encryption showing AES encryption more complex than DES, resulting in requiring greater memory consumption for the decryption algorithm.

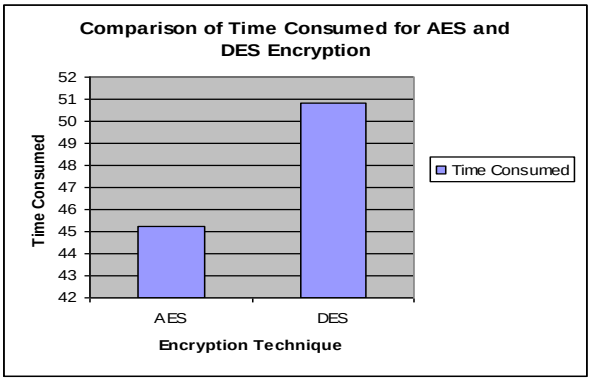


Figure 16: Time consumed for AES and DES Encryption

AES consume less time than DES Encryption for performing encryption on message which depicts that AES is efficient than DES encryption.

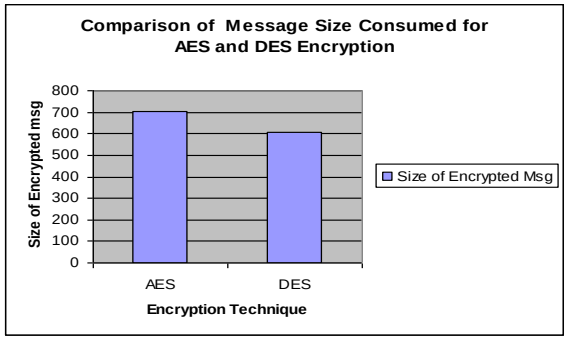


Figure 17: Consumed message size for AES and DES Encryption

AES produces greater encrypted message size than produced by the DES encryption algorithm, so AES decryption will require more time to decrypt the message.

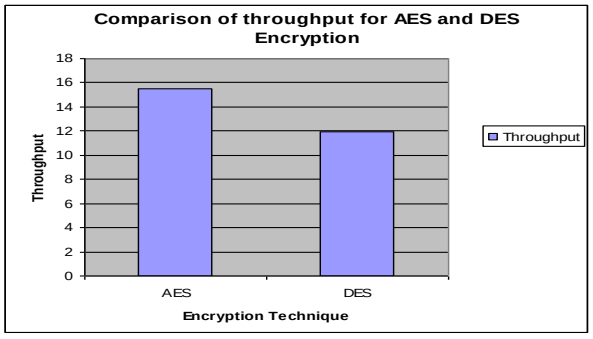


Figure 18: Throughput for AES and DES Encryption

As AES encrypted message size and consumed memory is greater than DES encrypted message and the time consumed in encryption function is less so its throughput is also greater than the DES encryption function. Therefore AES is more secure and efficient technique than DES for encrypting message.

Similarly AES and DES decryption algorithm are also compared for the above mentioned parameters and the results are shown in the following table.

Table 4: Comparison Table Decryption Algorithm

Decryption Algorithm	Consumed Memory	Time Consumed for Decryption	Encrypted Msg Size	Throughput
AES	8192 bytes	45.46 msec	440 bits	9.6 bits/msec
DES	6384 bytes	38.92 msec	440 bits	11.3 bits/msec

Form these calculations I have plotted the following graph for the AES and DES decryption algorithm.

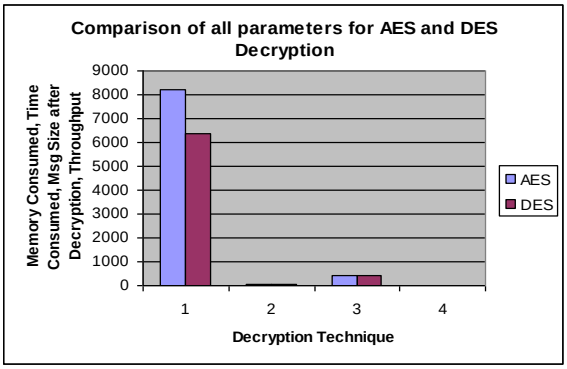


Figure 19: All parameters for AES and DES decryption

From the decryption table and figure we analyze that AES decryption is more complex than the DES decryption as it requires more time and memory to decrypt the message. So this proves that AES is more secure and complex than DES algorithm.

5. Conclusion and Future Work

In this technique, we have presented a mechanism for user authentication for password login phishing based attack. For this technique, the legitimate website will issue a digital certificate along with its signature and public key to the user to authenticate the website. For the user authentication we store the encrypted password provided by the user in database and improve its security. As highly secure data is kept in a form not useable by the unauthentic users.

We have used the concept of salt and add this salt to the user typed password and then calculate hash to make it more secure. We have compared the password strength of different hashing algorithms by using the password hash size, memory consumed after hashing, time taken in hashing password, and its throughput which is calculated as password size after hash divided by total time taken in calculating hash of password. To prevent the fraudulent actions on digital certificates issued by the certification authority we used AES encryption algorithm and compared this algorithm with the other encryption

algorithms by using size of file after encryption, memory consumed after encryption, total time taken in applying encryption and throughput which is calculated as encrypted file size divided by the time taken in encryption. We have concluded that SHA 512 is slower but more secure as its password hash size is bigger than the other hashing algorithms. Also we have concluded that AES is efficient and more secure as it consumes less time in applying encryption and its file size after encryption is bigger than the other encryption algorithms.

6. References

[1] Internet Fraud Attorney, The Blanch Law Firm P.C., New York http://criminaldefensefirm.com/index.php/topics/internetfraud/, retrieved on 29 Dec. 2010

[2] "USDOJ: CRM: Fraud: Mass-Marketing Fraud".justice.gov. http://www.justice.gov/criminal/fraud/internet/. Retrieved 19 November 2010

[3] Nelson, J., Jeske,D., Google, Inc." what-is-phishing"

[4] J. A. Halderman, B. Waters, and E. Felten, "A convenient method for securely managing passwords", Proceedings of the 14th International World Wide Web Conference (WWW 2005).

[5] Khayal, S.H.; Khan, A.; Bibi, N.; Ashraf, T "Analysis of Password Login Phishing Based Protocols for Security Improvements", IEEE International Conference on Emerging Technologies 2009 (ICET 2009), October 19-20, 2009, Islamabad, Pakistan. pp 368-371

[6] Topkara,M., Kamra,A., Atallah, M.J., and Rotaru, C.N. (2005), ViWiD : Visible Watermarking Based Defense Against Phishing, Spingerlink-Vertag Berlin Heidetberg, pp471-483

Improvement of Dynamic and Transient Stability of Micro Grid with Wind Generation

S.Venkatraj[1], Sasi.C[2] and Dr.G.Mohan[3]
[1,2]*Annamalai University, Department of Electrical Engineering,*
[3] *Department of Electrical Engineering, Annamalai University*
[1,2]*Assistant Professor*, [2]*Associate Professor*
subbian_venkat@yahoo.co.in , saasi_ceee@yahoo.co.in, mg_cdm@yahoo.com

Abstract: **A control scheme for fuel cell generation system is proposed in this paper to increase the transient stability and dynamic stability of micro-grids. With aids of ultracapacitors and the fast adjustment of power electronic conditioning systems, FC generation system can bring many benefits to distribution systems High penetration of wind power in micro grids causes fluctuations of power flow and significantly affects the power system operation. This can lead to severe problems, such as system frequency oscillations, and/or violations of power lines capability. With proper control, a distribution static synchronous compensator (DSTATCOM) integrated with ultra capacitor energy storage (UCES) is capable to significantly enhance the dynamic security of the power system. This paper proposes the use of a UCES system in combination with a DSTATCOM as effective distributed energy storage for stabilization and control of the tie line power flow of micro grids incorporating wind generation. A full detailed model of the DSTATCOM-UCES device is presented and a novel three-level control scheme is designed, comprising a full decoupled current control strategy in the *d-q* reference frame and an enhanced power system frequency controller. The dynamic performance of the proposed control schemes is completely validated through digital simulation in MATLAB/Simulink.**

Keywords: Power quality, Dynamic stability, Micro grid, Synchronous compensator, Wind turbine, Ultra capacitor energy storage.

1. Introduction

Distributed energy resources (DERs), including distributed generation (DG) and distributed energy storage (DES), are small sources of energy located near the demand and can provide a variety of benefits including improvement of reliability, if they are appropriately operated. This technological solution promotes the idea of using clean technologies of generation based on renewable energy sources (RESs) [1–2]. Presently, the most promising novel network structure that would allow obtaining a better use of DERs is the electrical microgrid (MG). This new concept tackles all DERs as a unique subsystem and offers significant control capacities on its operation. This electrical grid can be managed as if were a group with predictable generation and demand, and can be operated as much interconnected to the main power system as autonomously isolated [3]. For microgrids to work properly, an upstream interconnection switch must open typically during an unacceptable power quality condition, and the DER must be able to provide the active and reactive power requirements to the islanded loads. This includes maintaining appropriate voltage and frequency levels for the islanded subsystem, so that fast-acting generation reserve is required. As a result, for stable operation to balance any instantaneous mismatch in active power, efficient DES must be used [4].

Nowadays, grid integration of wind power generation is becoming the most important and fastest growing form of electricity generation among RESs. However, wind power frequently changes and is hardly predictable. The high penetration of wind power with abrupt changes adversely affects power system operation and can lead to severe problems. In order to overcome these problems, energy storage advanced solutions in combination with a type of power electronic equipment, such as distribution static synchronous compensator (DSTATCOM), can be utilized as an effective DES device with the ability to quickly exchange power with the electric grid. Various types of advanced energy storage technologies can be incorporated into the DC bus of the DSTATCOM, namely ultracapacitor energy storage (UCES), superconducting magnetic energy storage (SMES), flywheels and batteries, among others. However, ultracapacitors have distinct advantages for energy storage that make them almost unbeatable in many applications. They are very efficient and robust, require practically no maintenance and the lifetime is measured in decades [5].

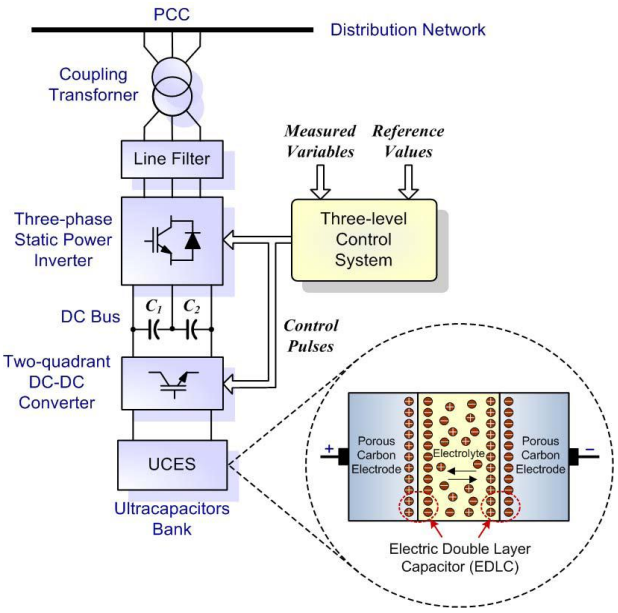


Figure 1. General structure of the DSTATCOM-UCES.

This paper proposes the use of a DSTATCOM-UCES as DES for stabilization and control of the tie-line power flow of MGs incorporating wind generation. A full detailed model of the DSTATCOM-UCES device is presented, including the ultracapacitor (UC) and the power conditioning system (PCS) used to connect to the power grid, as depicted in Figure 1. The PCS consists of the DSTATCOM and incorporates a twoquadrant DC/DC converter as interface with the ultracapacitor unit. Moreover, based on the state-space averaging method, a three-level control scheme is designed, comprising an enhanced power system frequency controller and a full decoupled current control strategy in the *d-q* reference frame. The dynamic performance of the proposed systems is validated through digital simulation carried out in MATLAB/Simulink.

2. MODELING OF THE DSTATCOM-UCES

Figure 2 summarizes the proposed detailed model of the DSTATCOM-UCES for dynamic performance studies. This model consists mainly of the DSTATCOM, the ultracapitor unit and the DC/DC converter to interface both devices. The DSTATCOM basically consists of a three-phase voltage source inverter (VSI) shunt-connected to the distribution network by means of a step-up Δ–Y coupling transformer and the corresponding line sinusoidal filter. The VSI corresponds to a DC/AC converter controlled through sinusoidal pulse width modulation (SPWM) techniques. The inverter structure is based on a diode-clamped three-level topology, also called neutral point clamped, instead of a standard two-level structure. This three-level twelve-pulse VSI topology generates a more smoothly sinusoidal output voltage waveform than conventional structures without increasing the switching frequency and effectively doubles the power rating of the VSI for a given semiconductor device.

The integration of the UCES system into the DC bus of the DSTATCOM device requires a rapid and robust bidirectional interface to adapt the wide range of variation in voltage and current levels between both devices, especially because of the ultracapacitor fast dynamic behaviour. Controlling the UCES system rate of charge/discharge requires varying the voltage magnitude according to the UC state-of-operation, while keeping essentially constant the DC bus voltage of the DSTATCOM VSI. To this aim, a combined two-quadrant two level buck/boost DC/DC converter topology by using high power fast-switched IGBTs is proposed in order to obtain a suitable control performance of the overall system. This step down and step-up converter allows decreasing the ratings of the overall power devices by regulating the current flowing from the UCES to the inverter of the DSTATCOM and vice versa.

The ultracapacitor energy storage is a relative recent technology in the field of short-term energy storage systems which is based on the electric double layer capacitor (EDLC). The construction and theory of operation of a UCES can be understood by examining the schematic view depicted in Figure 1 [5]. The elementary structure consists of two activated porous carbon electrodes immersed into an electrolytic solution, and a separator that prevents physical contact of the electrodes but allowing ion transfer between them. Energy is stored in the EDLC as a charge separation in the double layer formed at the interface between the solid electrode material surface and the liquid electrolyte in the micropores of the electrodes. This effectively creates two equivalent capacitors connected in series that gives the name to the structure. The ultracapacitor performance is based mainly on an electrostatic effect, which is purely physical reversible, although includes an additional pseudocapacitive layer contributing to the overall capacitance. Because of the complex physical phenomena in the double layer interface, traditional simple models such as the classical RC electrical model are inadequate for modelling EDLCs. Therefore, this work proposes the use of an enhanced electric model of an ultracapacitor based on the ones previously proposed in [6–7] that reflects with high precision the effects of frequency, voltage and temperature in the dynamic behaviour. The model describes the terminal behaviour of the EDLC unit over the frequency range from DC to several thousand Hertz with sufficient accuracy.

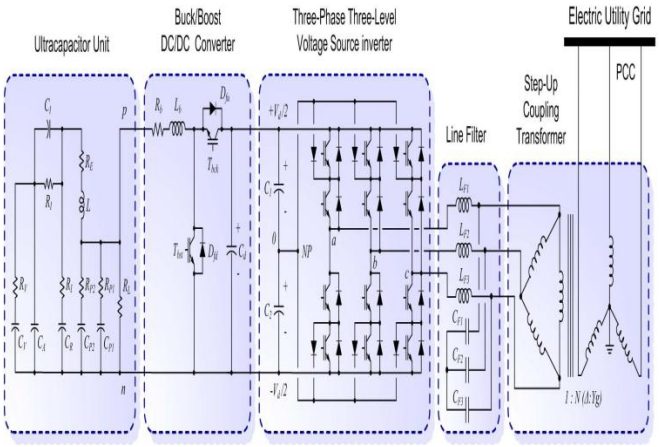


Figure 2. Detailed model of the proposed DSTATCOM-UCES

3. CONTROL STRATEGY OF THE DSTATCOM-UCES

The proposed hierarchical control of the integrated DSTATCOM-UCES consists of an external, middle and internal level, as depicted in Figure 3.

A. External Level Control

The external level control, which is outlined in Fiure 3 (left side), is responsible for determining the active power exchange between the DSTATCOM-UCES and the microgrid. This control mode aims at controlling the microgrid frequency through the modulation of the active component *id*. To this aim, the reference *idr1* is forced to vary with a stabilizer signal proportional to the frequency deviation Δf (defined as $fr-f$) which directly represents the power oscillation of the grid; the purpose

of this variation being to effectively improve the damping of power system oscillations. Since a robust and efficient frequency control scheme requires the effective damping of a wide range of generators power oscillations, ranging from less than 0.2 Hz for global oscillations to 4 Hz for local oscillations of units, a flexible multi-band structure (MBS) controller is proposed in this work. In this way, the novel proposed compensator architecture depicted in Figure 3 presents several degrees of freedom for achieving a robust tuning over a wide range of frequencies while keeping the same structure. The basic idea is to separate the frequency spectra into two decoupled bands for covering both small and large signal frequency disturbances. The first case is handled by the intermediate band and aims at damping inter-area modes usually found in the range of 0.2 to 3.0 Hz. The second case is treated by the low band and takes care of very slow oscillating phenomena such as common modes found on isolated systems and fluctuations caused by wind power generation. Appropriate damping of power swings in the intermediate spectral band require from the controller a frequency response with an increasing gain from low to high bands and phase leading in the whole range of action. This condition is achieved by employing differential filters synthesized through lead-lag compensators, providing intrinsic DC wash-out, zero gain at high frequency and phase leading up to the resonant frequency. Thus, the two resulting compensators are superposed in order to obtain a combined frequency stabilizer with an adequate phase characteristic for all frequency deviation modes.

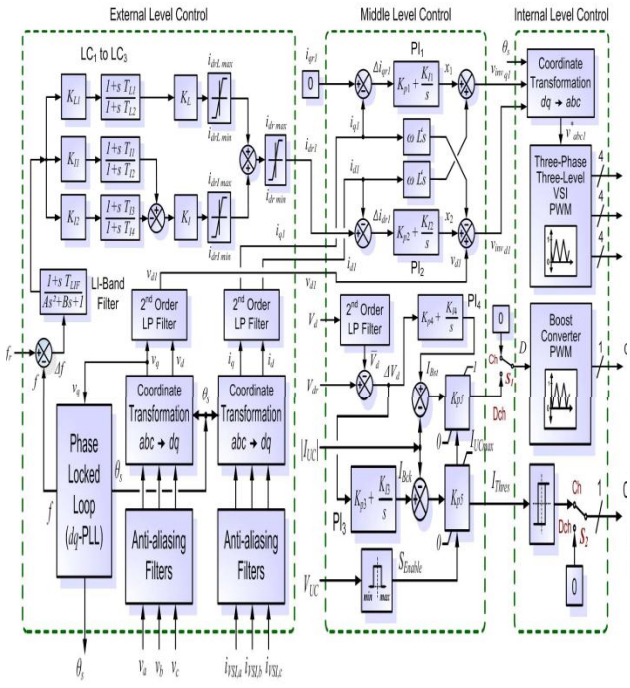


Figure 3. Multi-level control scheme for the DSTATCOM-UCES system

In the case of large signal frequency disturbances, since the DSTATCOM-UCES participates of the primary frequency control, the gain needed for the low frequency band is lower than the previous case and roughly constant for all the spectral band of interest which extends from near DC to 0.1 Hz. This frequency compensator structure controls the rapid active power exchange between the DSTATCOM-CES and the power system, forcing the UC to absorb active power when generators accelerate (charge mode), or to inject active power when they decelerate (discharge mode). This global architecture ensures almost the same good performance in damping power oscillations at all modes of interest. An input frequency filter is used for processing the frequency deviation signal, Δf obtained from the phase locked loop (PLL). The filter is associated with the low and intermediate bands, and guarantees a plane response in the 0 to 3 Hz range. In all cases, the frequency signal is derived from the positive sequence components of the AC voltage vector measured at the PCC of the DSTATCOM-UCES, through a PLL.

B. Middle Level Control

The middle level control makes the actual active power exchange between the DSTATCOM-UCES and the AC system to dynamically track the reference value set by the external level. The middle level control design, which is depicted in Figure 3 (middle side), is based on a linearization of the state space averaged mathematical model of the DSTATCOM in *d-q* coordinates described in [8]. The dynamics equations governing the instantaneous values of the three-phase output voltages in the AC side of the VSI and the current exchanged with the utility grid can be derived in the *dq* reference frame as follows:

$$s\begin{bmatrix} i_d \\ i_q \\ V_d \end{bmatrix} = \begin{bmatrix} \frac{-R_s}{L_s - M} & w & \frac{maS_d}{2(L_s - M)} \\ -w & \frac{-R_s}{L_s - M} & \frac{maS_q}{2(L_s - M)} \\ \frac{-3}{2C_d} mas_d & \frac{-3}{2C_d} mas_q & \frac{-2}{R_p C_d} \end{bmatrix} \begin{bmatrix} i_d \\ i_q \\ V_d \end{bmatrix} - \begin{bmatrix} \frac{|v|}{L_s - M} \\ 0 \\ 0 \end{bmatrix} \quad (1)$$

where,

$s=d/dt$: Laplace variable, defined for t > 0.

ω - synchronous angular speed of the grid voltage at the fundamental frequency.

M - modulation index of the VSI, $mi \sum [0, 1]$.

$a = \frac{\sqrt{3}}{\sqrt{2}}\frac{n_2}{n_1}$ turns ratio of the Δ–Y coupling transformer.

Sd = cos *α*, *Sq* = sin *α*: average switching factors of the VSI in the *dq* frame, and *α* the phase-shift of the VSI output voltage from the reference position.

Inspection of (1) shows a cross-coupling of both components of the DSTATCOM-UCES output current through *ω*. Therefore, in order to achieve a fully decoupled active and reactive power control, it is simply required to decouple the control of *id* and *iq* through two conventional proportional integral (PI) controllers, as depicted in Figure 3. In addition, it can be seen the additional coupling resulting from the DC capacitors voltage *Vd*, in the DC side as well in the AC side This feature demands to maintain the DC bus voltage as constant as possible in order to minimize its effect on *id* and *iq*. In the charge operation mode of the UCES, switches *S1* and *S2* are set at position Ch (charge) so that the DC/DC converter acts as a buck or step-down chopper. In this way, only the upper IGBT T_{bck} is switched while the lower one is kept off all the time. Since the UC current is highly responsive to the voltage applied, being this relation especially increased by the UC properties such as the exceptionally low ESR and large capacitance, an adaptive hysteresis (nearly constant-frequency) current control technique (AHCC) for the DC/DC converter operating in continuous conduction mode of I_{UC} is proposed [9].
This technique gives good performance, ensuring fast response and simplicity of implementation. In this way, the charging of the U_{CES} is rapidly accomplished at a current I_{Thres} computed by the external level control, provided that the voltage V_{UC} is below the limit V_{UCmax}. During this process, the VSI DC bus voltage is controlled at a nearly constant level via a PI control of the error signal between the reference and the measured voltage at the DC bus, in such a way that a balance of powers are obtained between the DSTATCOM inverter and the UC. In the discharge operation mode of the UCES, switches *S1* and *S2* are set at position D_{ch} (discharge), so that the DC/DC converter acts as a boost or step-up chopper. In this way, only the lower IGBT T_{bst} is switched while the upper one is kept off at all times. Since the ultracapacitor discharge current is to be controlled by the DC/DC converter input impedance, a pulsewidth modulation (PWM) control technique with double-loop control strategy is proposed to be employed. This control mode has low harmonic content at a constant-frequency and reduced switching losses. In this way, the discharging of the U_{CES} is rapidly accomplished at a level determined by the external level control, provided that the voltage V_{UC} is above the limit V_{UCmin}. During this process, the VSI DC bus voltage is regulated at a constant level via a PI control of the error signal between the reference and the measured voltage at the DC bus. Thus, by adjusting the duty cycle *D* of the boost chopper, the energy released from the ultracapacitor unit towards the VSI is regulated. An inner current loop is introduced into the voltage loop to achieve an enhanced dynamic response of the ultracapacitor current I_{UC}, so that rapid response can be derived from the DC/DC boost converter.

C. Internal Level Control

The internal level (right side of Figure 3) is responsible for generating the switching signals for the twelve IGBTs of the three-level VSI, and for the two ones of the bidirectional DC/DC converter. This level is mainly composed of a line synchronization module, a three-phase three-level SPWM firing pulses generator, and a PWM/hysteresis control firing pulses generator for the bidirectional DC/DC chopper.

4. DIGITAL SIMULATION RESULTS

The dynamic performance of the proposed DSTATCOMUCES device is assessed through digital simulation carried out in the MATLAB/Simulink environment [10], by using SimPowerSystems. The test microgrid employed to study the dynamic performance of the proposed full detailed modeling and control approach of the DSTATCOM-UCES device is presented in Figure 4 as a single-line diagram. This 12-bus power distribution system operates at 25 kV/50 Hz and includes a multiplicity of DER units (DG based on fossil and renewable fuels and advanced DES) and different types of loads (DR). The small microgrid implements a dynamically-modeled double generator-type DG linked to a utility system represented by a classical single machine-infinite bus type (SMIB) system. The first generator is composed of a dispatchable unit powered by a gas microturbine and includes a voltage regulator and a speed governor. The second generator is made up of a variable speed wind turbine generator grid-connected through a back-to-back converter [11]. Two sets of sheddable linear loads, grouped respectively at buses 9 and 11, are modeled as constant impedances. The proposed DSTATCOM-UCES device represents the microgrid DES and is placed at bus 4. A microgrid central breaker (MGCB) with automatic reclosing capabilities is employed for the interconnection of the point of common coupling (PCC) of the MG (bus 4) to the substation of the utility distribution system through a 15 km tie-line.
Three different case studies relative to basic protection and operation rules are considered, permitting to carry out both a large and a small-signal performance study of the DSTATCOM-UCES, besides the tie-line power flow stabilization and control.

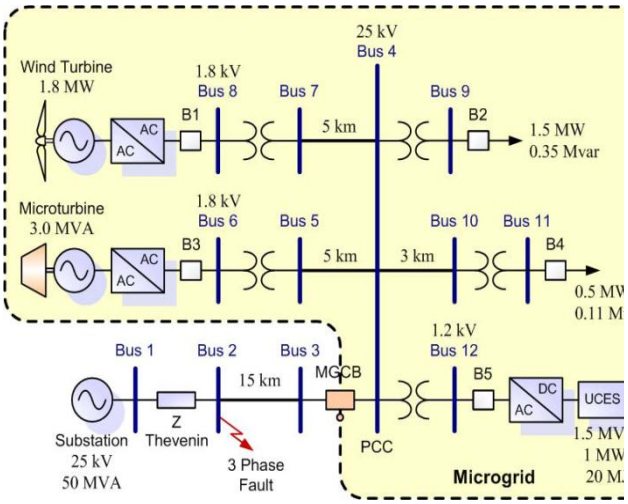


Figure 4. Single-line diagram of the test power system with the proposed MG

The first case study (Scenario 1), which corresponds to a severe disturbance such as the MG island operation mode, considers a permanent fault which needs to be isolated by the instantaneous trip operation of the MGCB. A three-phase-toground fault is applied at bus 2 in the utility system at t=0.1 s, and cleared 10 cycles later (200 ms) by tripping the tie line through the opening of the main microgrid circuit breaker. A load shedding scheme (LS) is included at all loads in order to prevent the system frequency collapse during the severe disturbance. The second case study (Scenario 2), which represents a quite less severe disturbance than the prior case, such as power oscillations damping, assumes that the fault is temporary and implements an instantaneous trip action with automatic breaker reclosing at a preset delay-time of 250 ms. The third case study (Scenario 3), considers the stabilization of the tie-line power flow when there is high penetration of wind generation. This inherently unpredictable and highly variable generation causes fluctuations of tie-line power flow which significantly affects power system operations.

A. Scenario 1: Assessment of MG operation in island mode

One of the main goals in forming a microgrid is to maintain uninterrupted power to critical loads. Thus, the ability of a MG to form intentional islands is assured by appropriately operating the DG located downstream of the distribution utility jointly with DES and loads. To this aim, the proposed test MG is intentionally forced to operate in island mode at t=0.12 s and the microgrid performance during the starting of the island is analyzed through the simulation results of Figure 5. For the configuration presented in the test case prior to the fault in steady-state, the gas microturbine is dispatched at 1.2 MW, while the wind generator is disconnected. In these circumstances the active power demanded by loads is 2 MW so that the microgrid needs to import about 0.8 MW from the main distribution system. After the fault is cleared and the tie-line tripped, the generator is operated in island conditions. Under these circumstances, the microturbine itself has to supply all the power required by loads. As can be seen from the simulation results shown in black dashed lines for this base case with no
DES, the gas microturbine responds slowly and is not capable of supporting the system frequency and thus avoiding the microgrid collapse. The activation of the automatic LS scheme with a total load rejected of 0.8 MW is required in order to recover the system frequency to its scheduled value.

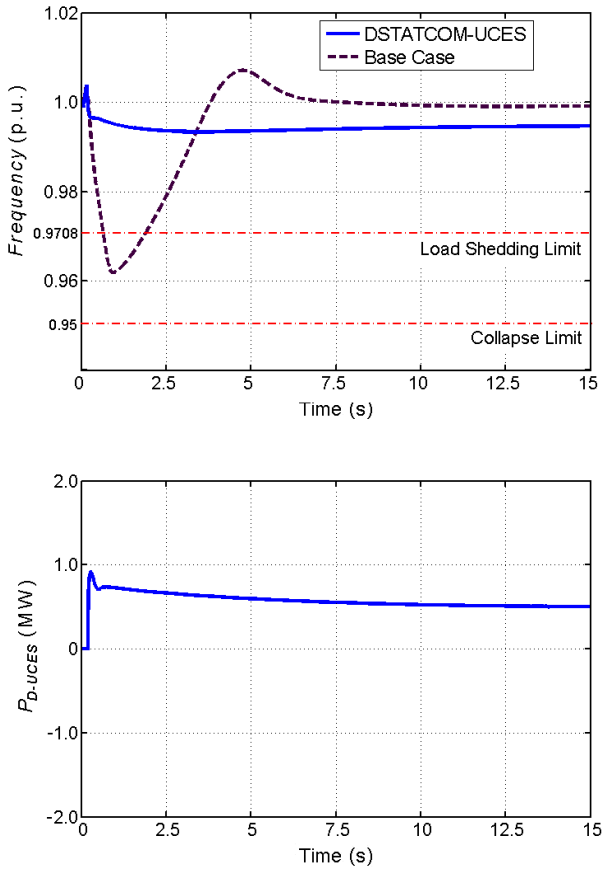


Figure 5. Microgrid responses to scenario 1: (MG operation in island mode)

The effect of incorporating a 1 MW/20 MJ UCES coil into the DC bus of the conventional ±1.5 MVA DSTATCOM device can be studied through the simulation results of Figure 5, shown in blue solid lines. These results clearly show the outstanding dynamic performance of the DSTATCOM-UCES.
The rapid active power supply quickly absorbs the sudden power loss occurred after the tie-line tripping and thus enhances the damping of low-frequency oscillations. This condition permits to greatly decrease the power strain of the microturbine, which results in an improvement of the MG reliability. In this case, the effects of the disturbance are totally mitigated in a shorter time than in the base case without being necessary to activate the load shedding scheme. The improvement of the frequency control is obtained by the immediate action of the UCES coil for supplying/absorbing active power, which provides power for about 15 s (approximately 9 MJ of energy).

B. Scenario 2: Assessment of MG operation in interconnected mode to a faulted feeder

The performance of the microgrid aiming at damping power flow oscillations in interconnected operation is now analyzed through the simulation results of Fig. 6, for the base case (i.e. with no DES) shown in black dashed lines. The disturbance occurring in the main distribution power system after the fault clearance and subsequent automatic reclosing of the breaker MGCB causes electromechanical oscillations of the gas microturbine generator. These local oscillations, between the electrical machine and the rest of the utility system must be effectively damped to maintain the microgrid stability. As can be noted from digital simulations, a local mode of approximately 2.5 Hz that settles down to its steady state value only after 6 s is induced in the microgrid.

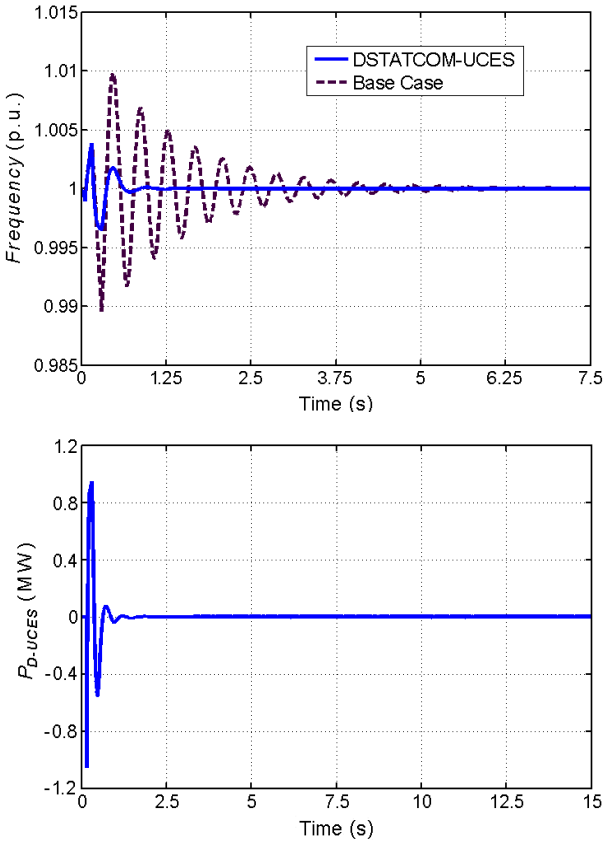


Figure 6. MG responses to scenario 2 (power flow oscillations damping mode)

The effect of incorporating the DSTATCOM-UCES can be verified through the simulation results of Figure 6, shown in blue solid lines. The transient response clearly proves the outstanding small-signal dynamic performance of the proposed multi-band structure (MBS) of the DSTATCOM-UCES. The UCES unit acts as an efficient damper, absorbing surplus energy from the system and releasing energy at the appropriate time when required. The UCES unit with the proposed controller is capable of damping the oscillations in a short time and reducing the amplitude of the pulsations on the frequency considerably. In the present analysis, the settling time for the system frequency is about 1 s when the UCES unit is used for active power compensation employing the MBS. A noteworthy point is that the capacity rating of the UCES unit used in this case study for damping low frequency power swings is only 0.15 MJ with a maximum power rating of almost 0.9 MW.

C. Scenario 3: Assessment of MG operation with high penetration of wind generation

The performance of the MG in interconnected operation and with high penetration of wind generation is now analyzed through the simulation results of Figure 7, for the base case (i.e. with no DES) shown in black dashed lines. Real data of wind profile during 300 s has been employed as input of the 1.8 MW wind power generator. Under these circumstances, the MG tieline to the main distribution power system is subjected to considerably changed power that significantly affects the operation of both the microgrid and

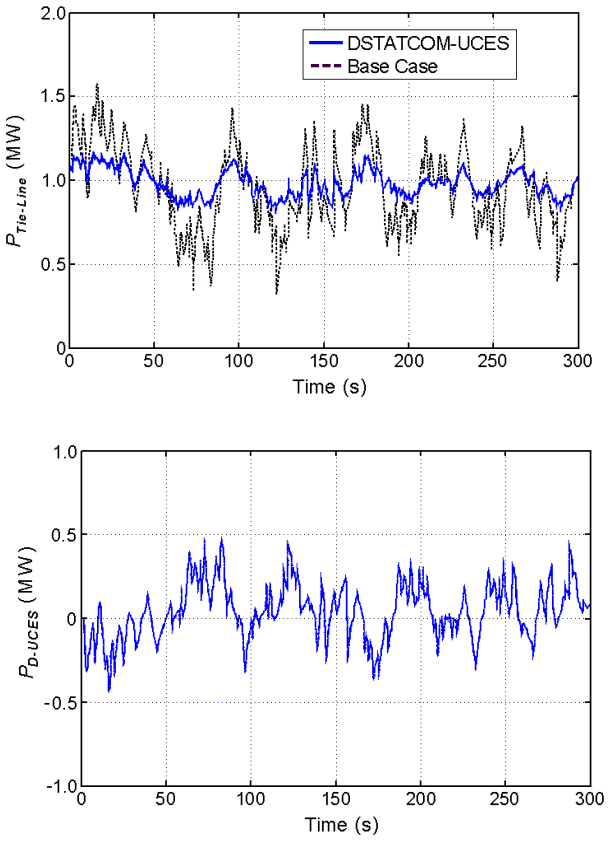


Figure 7. MG responses to scenario 3 (grid tie-line power flow stabilization mode)

the bulk power distribution system. Since the gas microturbine is disconnected in this case study, all loads are provided by the wind generator alone so that the power imported from the main utility is highly fluctuating between 0.5 a 1.5 MW.

The consequence of including the DSTATCOM-UCES can be verified through the simulation results of Figure 7, shown in blue solid lines. The transient response clearly proves the outstanding dynamic performance of the proposed MBS of the DSTATCOM-UCES. The UCES effectively stabilize the tieline power flow, absorbing surplus energy from the system and releasing energy at the appropriate time when required. Thus, the tie-line power flow with the DSTATCOM-UCES

compensation slightly fluctuates around a 1 MW and the wind generation with DES acts as an overall near dispatchable DGRES unit. In this way, the maximum and minimum tie-line power flow is restricted and therefore the capacity is maximized. The capacity rating of the UCES unit employed in this scenario is only around 0.3 MJ with a power rating of nearly 0.5 MW.

5. CONCLUSION

This paper presented an effective DSTATCOM-UCES controller used as DES of a microgrid with high penetration of wind generation. A real detailed full model and a novel multilevel control algorithm based on a decoupled current control strategy in the synchronous-rotating *d-q* reference frame were proposed. The control system employs a flexible multi-band structure controller for power damping in the frequency range of up to 3 Hz. The multi-level control scheme ensures fast controllability of the DSTATCOM-UCES, which enables to increase the transient and dynamic stability of the microgrid.

REFERENCES

[1] W. El-Khattam, and M.M.A. Salama, "Distributed generation technologies, definitions and benefits," *Elect. Pow. Syst. Res.*, vol. 71, no. 2, pp. 119-128, Oct. 2004.

[2] S. Rahman, "Going green: the growth of renewable energy," *IEEE Pow. & Ener. Mag.*, vol. 1, no. 6, pp. 16-18, Nov./Dec. 2003.

[3] B. Kroposki, R. Lasseter, T. Ise, S. Morozumi, S. Papatlianassiou, and N. Hatziargyriou, "Making microgrids work," *IEEE Pow. & Ener. Mag.*, vol. 6, no. 3, pp. 40-53, May/June 2008.

[4] F. Katiraei, R. Iravani, N. Hatziargyriou, and A. Dimeas, "Microgrids management: Controls and operation aspects of microgrids," *IEEE Pow. & Ener. Mag.*, vol. 6, no. 3, pp. 54-65, May/June 2008.

[5] B. E. Conway, *Electrochemical supercapacitors: scientific fundamentals and technological applications*, 1st ed., New York: Kluwer Academic Press/Plenum Publishers, 1999.

[6] F. Rafika, H. Gualous, R. Gallay, A. Crausaz, and A. Berthon, "Frequency, thermal and voltage supercapacitor characterization and modeling," *Jrnl. of Pow. Sources*, vol. 165, no. 2, pp. 928-934, 2007.

[7] L. Zubieta, and R. Bonert, "Characterization of double-layer capacitors for power electronics applications," *IEEE Trans. on Ind. App.*, vol. 36, no. 1, pp. 199-205, 2000.

[8] M.G. Molina, and P.E. Mercado, "Control design and simulation of DSTATCOM with energy storage for power quality improvements," *in IEEE/PES Transm. and Distrib. Conf.: Lat. Am.*; August 2006. p. 1-8.

[9] P.S. Ninkovic, "A novel constant-frequency hysteresis current control of PFC converters," *in Proc. IEEE Int. Symp. on Ind Elect. (ISIE)*, L´Aquila, Italy, 2002.

[10] The MathWorks Inc., "SimPowerSystems for use with Simulink: User's Guide", R2009a, Sept. 2009. Available at: <www.mathworks.com>.

[11] S. Song, S. Kang, and N. Hahm, "Implementation and control of grid connected ac-dc-ac power converter for variable speed wind energy conversion system," *in IEEE App. Pow. Elect. Conf. (APEC)*, Jan. 2003. p. 154-158.

Author's Biographies:

S.VENKATRAJ (1978) received Bachelor of Engineering in Electrical and Electronics Engineering (1999), Master of Engineering in Power System Engineering (2001) and he is working as Assistant Professor in the Department of Electrical Engineering, Annamalai University, Annamalainagar. He is currently pursuing Ph.D degree in Electrical Engineering from Annamalai University. His research interests are in Power Systems, Renewable source of energy, and Filter design. , Department of Electrical Engineering, Annamalai University, Annamalainagar-

608002, Tamilnadu, India,.Mobile:+91- 9824540468. subbian_venkat@yahoo.co.in

SASI.C (1981) received Bachelor of Engineering in Electrical and Electronics Engineering (2002), Master of Engineering in Power System Engineering (2008) and he is working as Assistant Professor in the Department of Electrical Engineering, Annamalai University, Annamalainagar. He is currently pursuing Ph.D degree in Electrical Engineering from Annamalai University. His research interests are in Power Systems, Renewable source of energy, and Filter design. , Department of Electrical Engineering, Annamalai University, Annamalainagar-608002, Tamilnadu, India, Tel: 91-04144-228428.Mobile:+91- 9865230002. saasi_ceee@yahoo.co.in

Dr.G.MOHAN (1963) received B.Tech in Instrument Technology (1986), Master of Engineering in Power System Engineering (1999) and Ph.D in Electrical Engineering (2010) from Annamalai University, Annamalainagar. From 1988 he is working as Associate Professor in the Department of Electrical Engineering, Annamalai University, Annamalainagar. His research interests are in Power Systems, and Renewable source of Energy, Department of Electrical Engineering, Annamalai University, Annamalainagar – 608002, Tamilnadu, India, mg_cdm@yahoo.com

Heuristic approach of Tolerance-Based Algorithm for TSP

Fozia Hanif Khan[1] , Shaikh Tajuddin Nizami[2], Jawaid Ahmed Khan[3] ,
Syed Inayatullah[4] and Nasiruddin Khan[5]

[1] *Department of Mathematics, Sir Syed University of Engineering &Technology, Karachi, Pakistan*
[2&3] *Department of computer Science & Information Technology , NED University of Engineering & Technology, Karachi, Pakistan ,*
[4&5] *Department of Mathematics, University of Karachi, Pakistan*
{ [1]mf_khans@hotmail.com [2]nizamitaj@yahoo.com, [3] jawaid_bilal@yahoo.com,
[4] inayat@uok.edu.pk,,[5]drkhan.prof@yahoo.com }

***Abstract*: Finding the optimal TSP solution is an important task, but process is usually done on the basis of cost of the edges. This paper presenting an algorithm which helps in searching the optimal solutions on the basis of selection of cost arcs or edges. Obviously the idea of the algorithm is taken from the branch and bound algorithm as the branching process is widely effective as far as the computation time of the process is concern. Moreover this paper also reveals that the proposed algorithm is better in solving than the other previously explained algorithm.**

***Keywords*:** Upper tolerance, lower tolerance, travelling salesman problem, survival sets.

1. Introduction

The Travelling Salesman problem TSP is the problem of finding a shortest tour through all the given location exactly once. It is a very well-known problem and finding its solution is clearly very attractive. Different aspects of this problem have been studied, regarding the lower bound, upper bound, non-optimal edges and optimal edges. Thousands of techniques have been developed and different researchers had explored the different criteria and techniques to make the TSP problem as simple as possible. But it is a well-known fact that this problem is easy to state but difficult to solve. The best known exact algorithm that solves TSP is branch and bound algorithm. Most of the algorithms for TSP are based on the selection of arcs or edges that should be in the optimal solution. But this strategy is not supposed to be accurate in all cases because smallest arcs or edges are not the definite criteria that can predict the optimal solution. In this paper we are presenting an algorithm which deals with branching criteria for arcs or edges that should be saved for the optimal solution and collectively calculates the overall percentage of the solution. Overall percentage of the solution will measure the optimality of the solution. This problem is highlighted before, [1] has given the Branch and Cut method for asymmetric TSP, [2], [3] have applied the concept of tolerance, also [4] has given the another version of tolerance for STSP.

The presented algorithm is basically the inspiration of branch and bound algorithm, searches of optimal vertices by finding its tolerance value (which arcs are more suitable for the tour and which should be disposed off). Like most of the Branch and Bound algorithms, in the following algorithm we are taking assignment problem (AP) as a relaxation, as the value of AP solution of the TSP is the lower bound to the optimality. The solution of AP can be represented as a set of cycles, and AP solution is also called a minimum cycle cover. The sub-cycles of AP is also called survival set that also appears in the optimal tour breaking the survival sets and fixing with the each other is basically the patching problem. There are many other algorithms which have followed this criteria, Carpaneto(1980) [5], also Depth First Search (DFS) and Best First Search (BFS) which solves sub-problem with the lowest value of AP. Another approach that constructs feasible ATSP tour from AP solution is the patching procedure by Karp and Steele (1990)[6]. The idea for this paper is taken from the [7] but here we are trying to present the new and simple way for finding the tolerance criteria.

1.1 Importance of Tolerance:

The starting point for solving TSP is very important, that decides which edges are in a good tour with high probability and which are not. For this purpose the term tolerance is a good measuring tool. For TSP the tolerance is defined as follows:
Let an optimal (not necessarily unique) tour be given,

1.2 Upper Tolerance:

The upper tolerance of an edge from this optimal tour is defined as the minimum weight this edge must be increased so that this edge is not contained in at least one optimal tour.

1.3 Lower tolerance:

The lower tolerance of an edge outside this optimal tour is defined as the minimum weight this edge must be decreased so that this edge is contained in at least one optimal tour [8].

The aim of this paper is to implement a new algorithm for faster solving TSP. Basically this algorithm is a tolerance based criteria that is for the choice of the edges will be analyzed and applied in heuristics. In detail we want to show that the tolerance based choice of the edges is superior to a usual weight based choice [8]. Here we are applying the criteria for the degree of upper tolerance as well as the lower tolerance. On the basis of that, arcs are included or excluded in the tour.

2. Steps of Algorithm

i. Starting with an AP solution construct a minimum cycle cover on it. If the minimum cycle cover at hand is a complete tour then the TSP instance is solved [7]. Otherwise the problem is partitioned in to new sub-problems after breaking sub-cycles by removing arcs.

ii. Now there is an intriguing question which arcs should be removed. Identification of such arcs is of course a time consuming process. By using the selection of edges criteria, arcs that have lower tolerance should be retained. Let S be set of sub-cycles which are obtained from the AP solution and let the value of AP solution is equal to A. Let e is the value of the arc which is considered for the selection or rejection and LAP is the least value of arcs among all the sub-cycles which present in S. The criteria for the tolerance is,

$$\text{Criteria for tolerance} = \frac{e}{A-LAP}\,100\%$$

iii. If the above value is less than equal to 75% then that arc could be tolerated. Otherwise remove it.

iv. Like this solve the patching problem with the selection and rejection of different arcs.

v. Calculate the total percentage of each path that can exist, and in this way the least one will be chosen as an optimal value.

3. Example

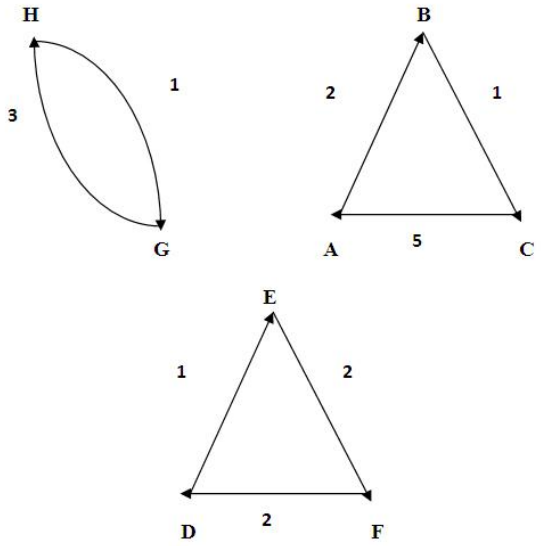
Consider the example,

	A	B	C	D	E	F	G	H
A	∞	2	11	10	8	7	6	5
B	6	∞	1	8	8	4	6	7
C	5	12	∞	11	8	12	3	11
D	11	9	10	∞	1	9	8	10
E	11	11	9	4	∞	2	10	9
F	12	8	5	2	11	∞	11	9
G	10	11	12	10	9	12	∞	3
H	10	9	10	10	6	3	1	∞

The matrix that will obtained after row and column reduction is,

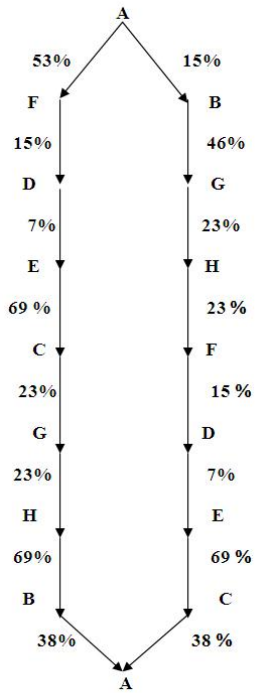
	A	B	C	D	E	F	G	H
A	∞	0	9	8	6	5	4	3
B	3	∞	0	7	7	3	5	6
C	0	9	∞	8	5	9	0	8
D	8	8	9	∞	0	8	7	9
E	7	9	7	2	∞	0	8	7
F	8	6	3	0	9	∞	9	7
G	5	8	9	7	6	9	∞	0
H	7	8	9	9	5	2	0	∞

The sub-cycle which are obtained after solving the above problem by assignment method are,



In the above problem the least value among all the sub-cycles is 4 and the value of the assignment problem will be 17, Calculate the tolerance among the edges of the sub-cycles according to the described in algorithm for solving the patching problem.

The following figure shows two possible tours, that showing the tolerance % of every edge.

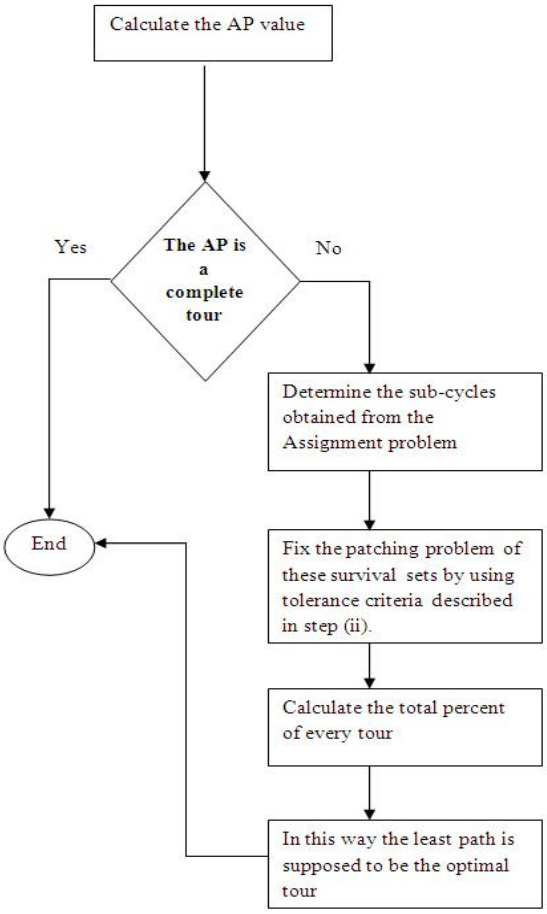


On the basis of cumulative tolerance the optimal tour is supposed to be,

$$A \rightarrow B \rightarrow G \rightarrow H \rightarrow F \rightarrow D \rightarrow E \rightarrow C \rightarrow A$$

with a total length of 33.

4. Flow Chart of the Algorithm



5. Conclusion

In the presented paper we have described the tolerance criteria of the edges for finding the optimal TSP path. The basic inspiration is taken from the branch and bound algorithm, but it can be easily seen that the provided algorithm could produce good result as compared to the algorithm given by [8]. The patching problem of the sub-cycles basically the main purpose of the algorithm.

6. Summary and Conclusion

From the general description in section 4 of the use of Genetic Algorithm in the Assignment Problem and from the test problem solved in section 5, a little efforts shows that these two problems yield the same results with the use of Hungarian Method . It is evident that this method is shorter and more efficient than Hungarian method. The Hungarian Method requires in general, a succession of steps to take care of zeros, where as Genetic Algorithm uses the Genetic Operators only thrice in 4 order cost matrix. Compare to Genetic Algorithm method, the Hungarian method, when applied to the Assignment Problem is something of a long haul.

References

[1] Fischetti, m., Lodi, A., Toth, P., 2002. Exact Methods for the Asymmetric travelling Salesman problem In: Gutin, G., Punnen, A. P. (Eds), The travelling salesman problem and its variations. Kluwer, Dordrecht, pp. 169-194. (Chapter 9).

[2] Libura, M., Van der poort, E. S., Sierksma, G., Van der Veen, J.A.A., 1998. Stability aspects of the travelling salesman problem based on k-best solutions. Discrete Applied Mathematics 87, 159-158.

[3] Lin, C. J., Wen, U. P., 2003. Sensitivity analysis of the optimal assignment . Discrete Optimization.

[4] Helsghan, K., 2000. An effective implementation of Lin-Kernghan travelling salesman heuristic. European journal of Operational Research 12, 106-130.

[5] Carpaneto G., Toth, P., 1980. Some new branching and bounding criteria for the asymmetric travelling salesman problem. Management Science 21, 736-743.

[6] Karp, R. M., Steel, J. M. 1990. Probabilistic Analysis of Heuristics In: The Travelling Salesman Problem. Wiley, New York, pp. 181-205.

[7] http://www.informatik.uni- halle.de/ti/forschung /toleranzen/index.en.php

[8] Turkensteen, M., Ghosh. D., Goldengorin, B., and Sierksma, G., 2008. Tolerance-based Branchand Bound algorithm for ATSP European Journal of Operational Research 198, 775-788.

Power Quality Improvement of Weak Distribution System by Variable-Speed Wind Turbines

Sasi.C[1] and Dr.G.Mohan[2]

[1]Annamalai University, Department of Electrical Engineering,
[2] Department of Electrical Engineering, Annamalai University
[1]Assistant Professor, [2]Associate Professor
saasi_ceee@yahoo.com , gmohan@yahoo.com

Abstract: This paper analyzes the power quality improvement of weak electric distribution systems by variable speed wind turbines, based on simulation results. The effects on the voltage profile caused by variable-speed wind turbines are compared to the effects caused by fixed-speed wind turbines. Both types of wind turbines are assumed to be equipped with asynchronous machines. In the Variable speed mode of operation, a voltage-source converter cascade is used, employing field-oriented control for the generator-side converter and three independent hysteresis controllers for the grid-side converter. For the simulation of the wind park and the grid a library of wind turbines, electrical grid components were developed. By using the developed simulation tool, two cases concerning high and low wind speed are studied. The advantages of the studied variable speed operation scheme are confirmed and the possible increase in the installed capacity of the wind power over the fixed speed mode, maintaining the same power quality standards, is estimated.

Keywords: Power quality, Variable-speed wind turbines, Vector control, Wind power, Wind turbine, Power quality improvement.

1. Introduction

In this paper, simulation results from a study dealing with the repercussions from the installation of a wind park in a weak electrical grid are presented. The grid examined is located in a rural area named Tirunelveli at the South part of Tamilnadu in India. This area presents excellent wind potential and, as a result, a lot of interest has been expressed by independent power producers for the installation of wind parks. Penetration of wind power in this network is, however, limited by the power-quality standards applied by the electric utility. These regulations limit median voltage within $\pm 5\%$ of the nominal and deviation around median within $\pm 3\%$. Flicker severity index (short term), Pst, must be less than 0.9 for medium voltage while voltage total harmonic distortion must be lower than 6.5% and 8% at medium and low voltage, respectively. It is well known that the power delivered by wind turbines (WTs) directly coupled to the grid is not constant as a result of the wind variability. In the absence of storage systems, a fluctuating power supply produced, for example, by gusts, can lead to voltage variations in the grid and flicker. Another disadvantage of most induction machine WTs is that the required reactive power varies with wind speed and time. In

case of variable-speed (VS) WTs, the previous problems are ameliorated, but the problem of grid "pollution" due to production of the power-converter harmonics arises. The study of the aforementioned effects imposes the development of suitable simulation tools [2]–[3].

In this paper, a simulation tool developed using Matlab code and Simulink is used. Analytical models for various components of the system were developed. In addition, this tool benefits from Matlab's environment that enables detailed analysis and convenient design of such a system. For example, the design of the control system, its analysis, and the implementation of modern control schemes is relatively easy, something that is not often offered by most of the customized models [5]–[6]. The variable speed wind turbine that is studied employs a voltage-source converter cascade using an indirect field-oriented voltage controller and a hysteresis current controller for the generator and the grid-side converter, respectively [7], [8].

The hysteresis current controller is composed of three independent per phase current controllers. The proposed scheme has not been adequately studied for WT applications so far, while it presents very good operational characteristics, as indicated by the reported simulations. It is shown that using the proposed technology, a 30 to 50% increase of the installed capacity over fixed speed WTs is possible at the same connection point, without violating the power-quality regulations imposed by the local utility.

2. Simulation Models

In this section, the simulation models of the main electrical components are briefly reviewed, especially the models of induction machines and power

loads. Emphasis is placed on the control method applied to the power converters.

Induction machines are represented by the fourth-order model expressed in the arbitrary reference frame [9]. Stator and rotor currents are used as state variables. The equivalent of three or six elastically connected masses can be optionally used for simulating the mechanical system of the WT, while the performance coefficient Cp curves are used for the study of the blades dynamics [2].

Electrical loads are assumed as constant active- and reactive- power loads. This assumption is modeled by the following dq-axis current components obtained from the absorbed active and reactive powers:

$$I_d = \frac{V_d}{V_d^2 + V_q^2} P + \frac{V_q}{V_d^2 + V_q^2} Q$$

(1)

$$I_q = \frac{V_q}{V_d^2 + V_q^2} P - \frac{V_d}{V_d^2 + V_q^2} Q$$

There are also two more options for the loads (i.e., they can be considered as constant admittance or constant current loads). In addition, the developed library contains models for transformers (linear), circuit breakers, power converters, measurement devices of voltage, current, flicker, total harmonic distortion (THD), etc.

The connection of the variable speed WTs to the grid is achieved with a voltage-source converter cascade in order to control the reactive power exchanged between the network and the WP and to provide variable-speed mode of operation. The generator-side converter employs the SPWM technique, while the grid-side converter uses a hysteresis current controller [7], [8], [10]–[15].

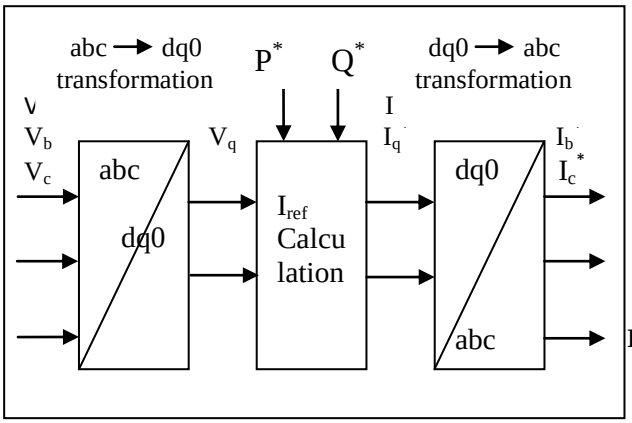


Figure 1. General concept of grid-side converter controller.

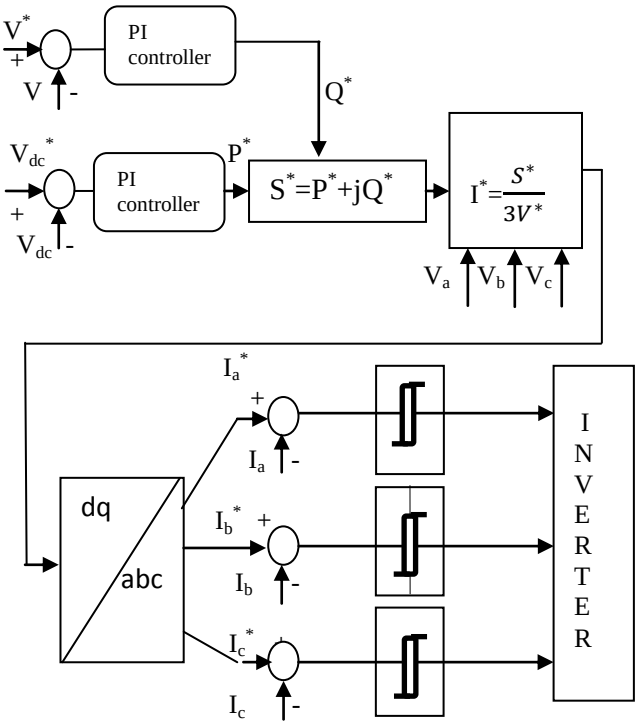


Figure 2. Block diagram of the hysteresis current controller.

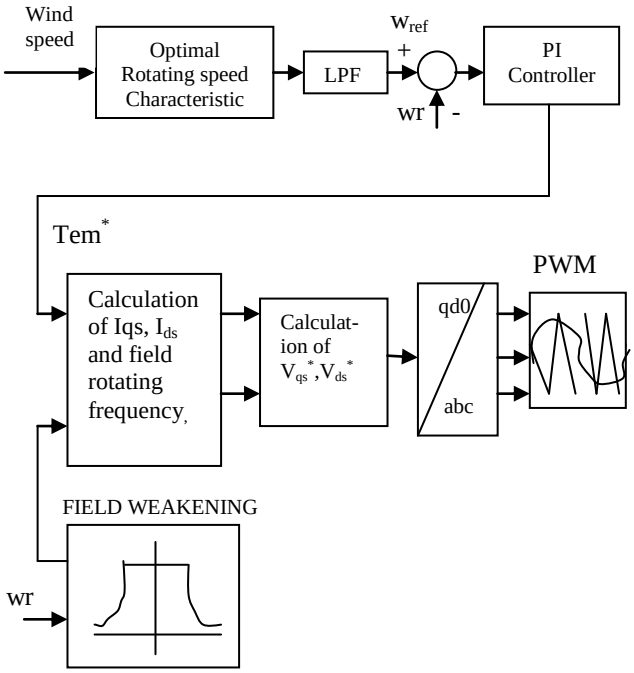


Figure 3. Indirect field-oriented voltage controller.

The general concept for the grid-side converter control is shown in Figure. 1 [10]. The reference values for the instantaneous output currents are calculated from the measured phase voltages and the reference values of the converter active and reactive powers. The hysteresis band used is 0.001 p.u. of the current base value. The control system of the grid-side converter is shown in more detail in Figure. 2, where the two major control loops of the dc and the converter output voltage are

distinguished. The second control loop is optional and is not examined in this paper (i.e., a unity power factor is assumed). The first loop controls the active power injected to the grid in order to maintain the dc voltage at its set value, $V_{dc,ref}$.

The generator control system consists of two major loops as shown in Figure. 3, one for the blades rotating speed and the other for the rotor flux linkage. Indirect field-oriented voltage control is applied to the generators of the WTs. The wind speed input signal is led to the wind speed blades optimal rotating speed characteristic, which produces the input signal to a low-pass filter. The output of the low-pass filter is fed next as input to the torque controller. For low wind speed, maximum energy efficiency is achieved by tracking the optimal rotating speed. At high wind speeds, the control scheme imposes a constant rotating speed, taking advantage of the blades stall property for the limitation of the torque and the produced power below the design values. As mentioned before, the desired electromagnetic (EM) torque is achieved by the application of an indirect field-oriented voltage-control scheme. Knowing the value of the desired EM torque, the q-axis current component in the field-oriented frame is given by [11]

$$I_{qs}^{e*} = \frac{4L_r' T_{em}^*}{3PL_m \lambda_{dr}^{e*}} \qquad (2)$$

It is also known that, when properly oriented, the slip speed and the dq-axis current components in the field-oriented frame are related as [11]

$$w^* = w_e - w_r = \frac{r_r'}{L_r'} \frac{I_{qs}^{e*}}{I_{ds}^{e*}} \qquad (3)$$

Rotor flux can be controlled by regulating I_{ds}^{e}. Given some desired level of the rotor flux, the desired value of the -axis current component can be obtained from [11]

$$I_{ds}^{e*} = \frac{r_r' + L_r' p}{r_r' L_m} \lambda_{dr}^{'e} \qquad (4)$$

The conditions shown before ensure decoupling of the rotor voltage equations. The desired voltage components in the field oriented frame are obtained from the fourth-order model of the induction machine. The only drawback of this control scheme is that it requires accurate knowledge of the machine parameters. It is commonly used with online parameter adaptive techniques for tuning the value of the parameters used in the indirect field controller, ensuring in this way successful operation.

3. Study Case System

The examined network is radial and consists of a medium voltage overhead 20-kV feeder, supplying various types of loads, mostly residential and commercial. The total maximum demand amounts to 7 MVA. The main line of the feeder comprises ACSR95 conductors with a total length of 45 km.

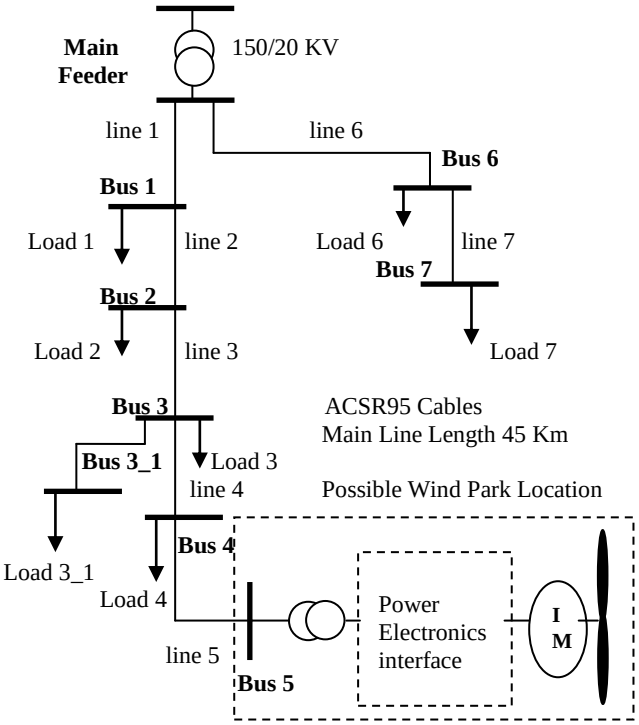


Figure 4. Simplified network that is used in the simulation.

This network is extremely weak and this results in high-voltage variations and, consequently, in the possibility of unstable operation. Assuming a typical short circuit level of 250 MVA at the origin of the feeder, the short-circuit level at the WP's location is calculated at approximately 40 MVA. Following connection practices applied in several European Countries a WP of only approximately 2 MVA can be installed without the need to investigate the produced flicker. Consequently, significant voltage variations can be expected if a WP of higher installed capacity is connected. The problem is more profound for the consumers connected near to the coupling point of the WP.

In the following analysis, the network is simplified and represented by its eight most important nodes corresponding to main junctions or major consumer points. All of the other loads are aggregated into these nodes. The simplified equivalent electrical network and the connection point of the WP are shown in Figure. 4. All WTs are assumed to be equipped with equivalent induction machines.

4. Simulation Results

A series of simulations was initially performed considering different installed capacities of the WP

(consisting of FS WTs). It was found that for an installed capacity of higher than 7.5/6 MVA in cases of low and high mean wind speed, respectively, the WP was led to unstable operation. Then it was shown that using the proposed VS scheme, penetration can be increased to FS operation by 30% and 50%, in cases of high and low mean wind speed, respectively. For both cases, the same voltage standards and power-quality regulations mentioned in the introduction are satisfied.

The following four cases are examined:
1) low mean wind speed (7.5 m/s) using FS WTs (7.5-MVA installed capacity);
2) low mean wind speed using VS WTs (11-MVA installed capacity);
3) high mean wind speed (15 m/s) using FS WTs (6-MVA installed capacity);
4) high mean wind speed using VS WTs (8-MVA installed capacity).

The active and reactive powers of the WP with FS WTs (case 1) are shown in Figure 5. Figures 6–10 are the VS mode of operation described in Section II. The WP operates at unity power factor. The desired and the measured blade rotating speed for case 2 are shown in Figure 6. It is obvious that the vector-controller response to wind-speed variations is fast and stable as the two curves almost coincide. In this way, optimum operation is ensured. In Figure 7, the aerodynamic and the EM torque are compared. The resulting variations of the generator EM torque [2], [15] indicate a significant attenuation of the fluctuations of the primary source. It is obvious that the EM torque tracks only the slow variations of the wind, contrary to the aerodynamic torque. This is achieved due to the use of the low-pass filter—after the optimal rotating speed characteristic—leading to the enhancement of the low-pass characteristics of the whole system [2], [10]. The attenuation of the EM torque variability

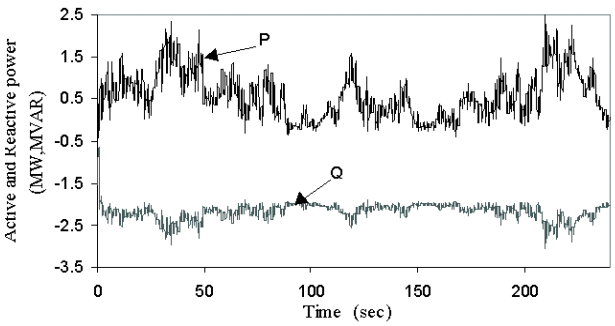


Figure 5. Active and reactive powers produced by the fixed-speed WP for low wind speed, case 1a.

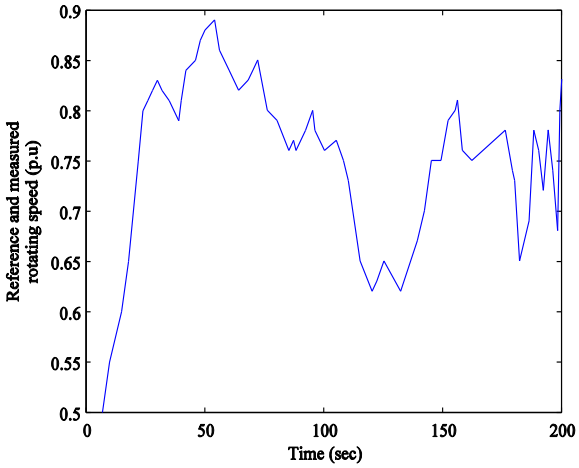


Figure 6. Desired and actual blade rotating speed, case 1b.

is propagated to the generator active power contributing to the improvement of the produced power quality, as shown in Figure 8. This does not happen in the case of the constant speed mode of operation, where the produced active power retains higher frequency components. The enhancement of the low-pass characteristics of the system in case of variable-speed mode of operation is very desirable, especially when the WTs are connected to be weak or autonomous electrical systems as described in [15]. Also, the mechanical stresses of the WTs have significantly decreased compared to the constant-speed operation [16], which was another of the design objectives of the generator control system. The active-power production has significantly increased in the case of VS WTs as shown in Figure 8.

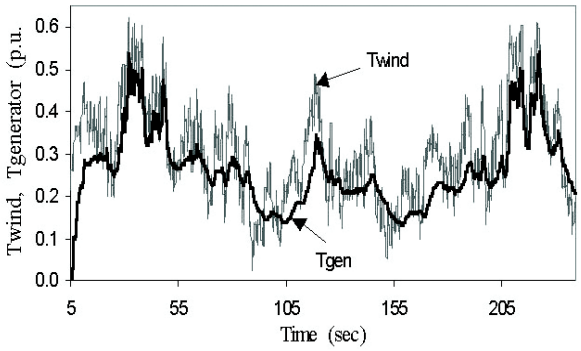


Figure 7. Aerodynamic and EM torque, case 1b.

The grid-side converter controller operates absolutely satisfactorily as the dc voltage and the reactive power injected to the grid, are maintained to their set values, as shown in Figures 9 and 10.

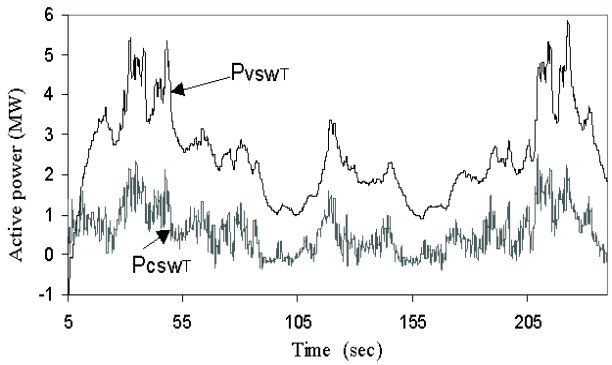


Figure 8. Active power produced by variable- and constant-speed WTs for low wind speed, cases 2 and 1a, respectively.

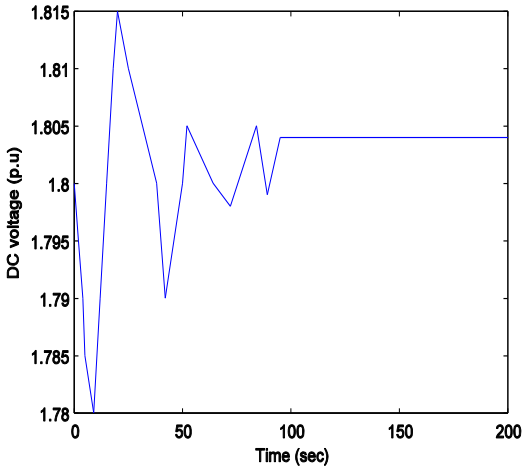


Figure 9. Voltage at dc side, case 2.

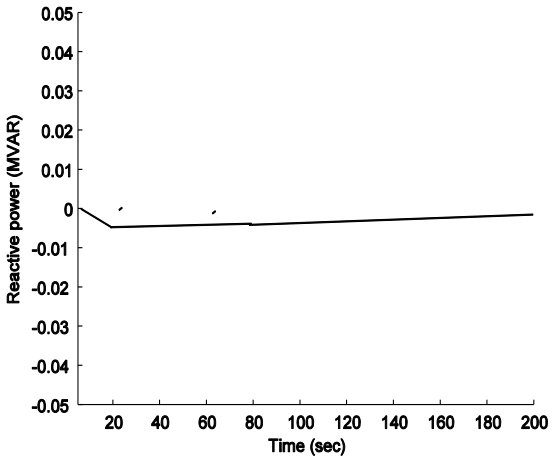


Figure 10. Injected to the grid reactive power, case 4.

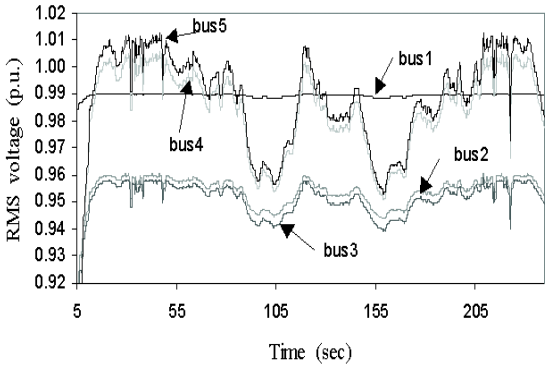


Figure 11. RMS voltage at buses 1–5 for low wind speed and VS WTs, case 2.

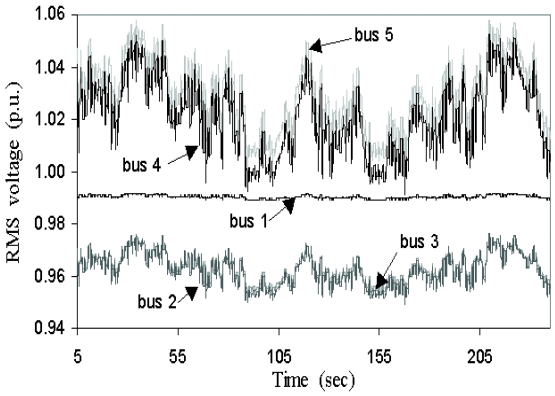


Figure 12. RMS voltage at buses 1–5 for low wind speed and fixed-speed WTs, case 1.

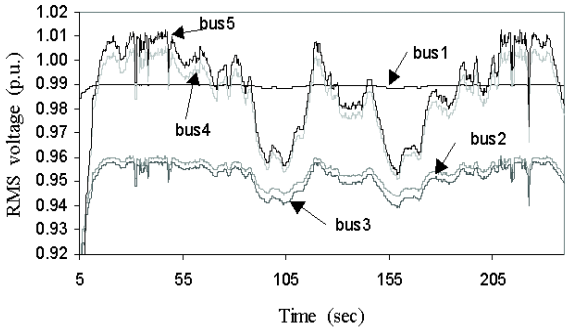


Figure 13. RMS voltage at buses 1–5 for high wind speed and VS WTs, case 4.

For each study case, the voltage profiles at the nodes of the main feeder network are shown in Figures 11–14. As expected, nodes closer to the infinite bus have lower voltage variations. Without reactive compensation at bus 5, voltage drop exceeds acceptable limits at practically all buses, especially in the case of constant speed operation. The capacitors used at bus 5 are 550, 140, 450, and 140 KVAR for cases 1, 2, 3, and 4, respectively. The capacitors were sized so that the

median voltage at all buses is limited within ±5% of the nominal. In case of VSWTs, they were sized considering first the voltage limits and, subsequently, the damping of the harmonics. The voltage fluctuations are larger in the case of low wind speed because for high wind speed, the produced power is limited by the stall effect, for most of the simulation time. In all cases, a voltage increase is observed at buses 4 and 5. This is justified as the WP acts as a negative load, which operates with a unity power factor in case of VS operation and benefits from the reactive compensation in case of FS operation.

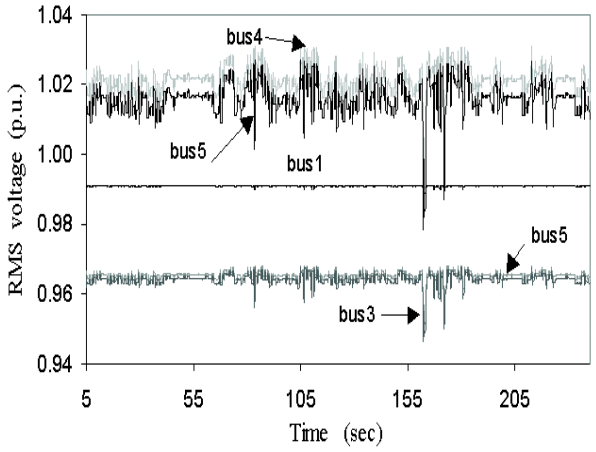


Figure 14. RMS voltage at buses 1–5 for high wind speed and fixed-speed wind turbines, case 3.

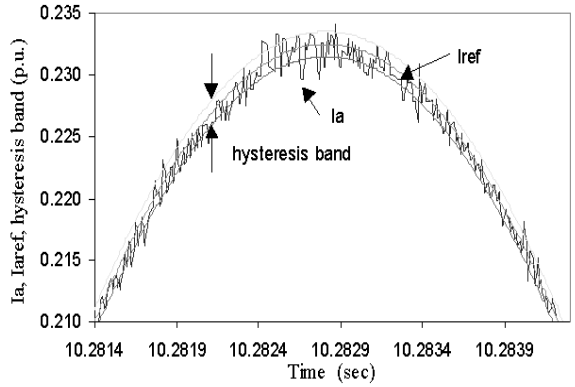


Figure 15. Hysteresis band, current reference, and actual current.

For the VS WTs, the amplitude of the voltage variations presents significant attenuation, similar to the one of the produced active power. Moreover, the amplitude of voltage deviation decreases with increase in mean wind speed, as shown in Figures 11 and 13. However, in case of high wind speed, the frequency of voltage variations seems to increase and the problem of flicker causes concern. Several tests were performed in order to compare the voltage deviation and the flicker produced by the specific WP. The values for the short-term flicker severity index Pst, were less than 0.9 for all study cases. More information about the Pst values obtained, is given in Table I.

Harmonic injection, caused by the nonlinear behavior of the grid-side converter, is studied next. The narrower the hysteresis band is, the higher switching frequencies occur, but less harmonic distortion is propagated to the grid. The actual injected current is adequately maintained in the hysteresis band, as shown in Figure 15. A filter has been used for the connection of the grid-side converter that mainly damps the higher-order harmonics. It consists of a 0.5-p.u. series reactance. In Figures 16 and 17, the harmonic content of bus 2 and WP bus voltages, in the 0-to-10-kHz frequency domain, is given. As expected, harmonics are considerably damped at bus 2 because the network is stronger at this point. Furthermore, it has been observed that peaks occur at the multiples of the basic frequency. Comparison between the voltage waveforms at bus2 and WP connection bus is shown in Figure 18, confirming the previously mentioned conclusions drawn by Fourier analysis.

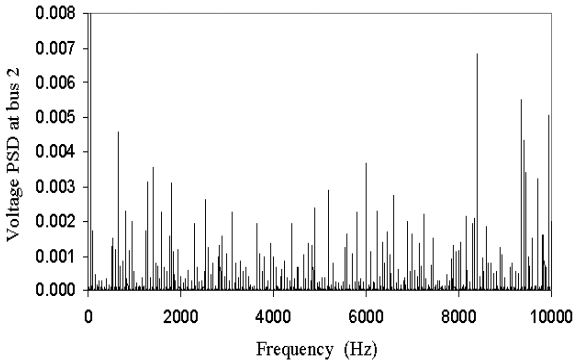


Figure 16. Voltage power spectral density at bus 2.

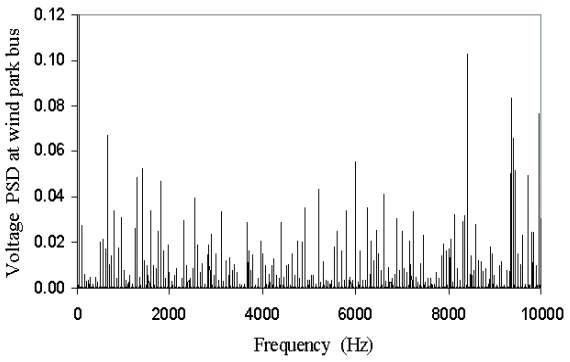


Figure 17. Voltage power spectral density at WP bus.

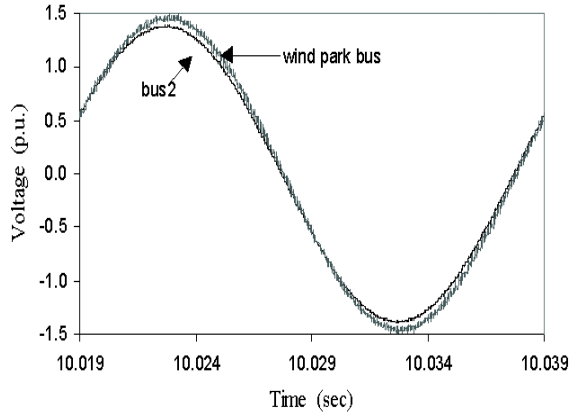


Figure 18. Voltage waveforms at bus 2 and WP bus.

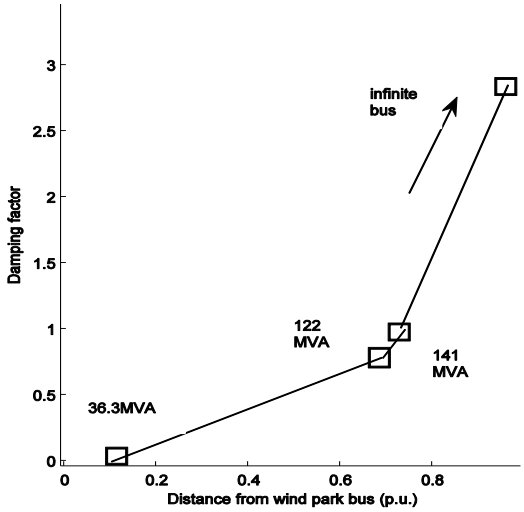


Figure 19. Damping of voltage harmonic content along the network together with the corresponding short-circuit power.

THD Factor

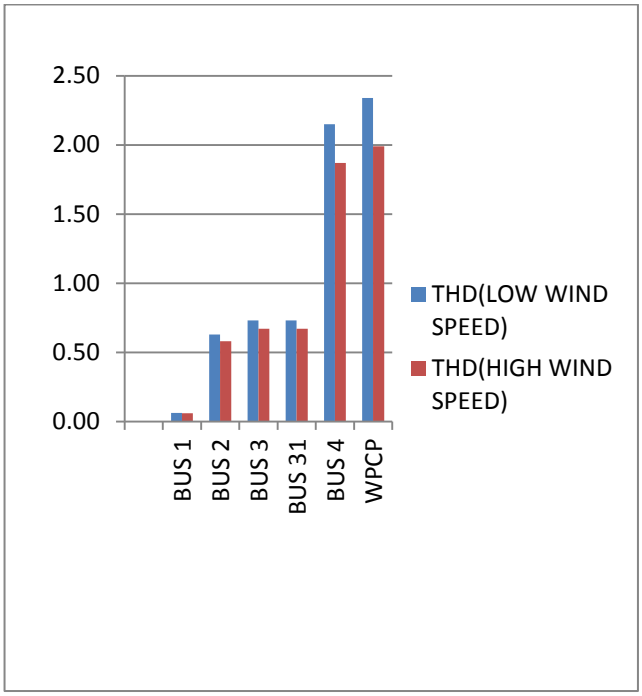


Figure 20. Voltage total harmonic distortion at buses 1–5 for low and high wind speed, cases 2 and 4.

The harmonic damping factor is defined as

$$a_{n,fi} = \log \frac{PSDWPbus[fi]}{PSD_n[fi]} \qquad (5)$$

where, PSDWPbus[fi] is the power spectral density at the frequency fi for the WP bus voltage and $PSD_n[fi]$ is the power spectral density at the frequency fi for the bus voltage.

This can be used to calculate the damping at all buses for each harmonic with respect to WP coupling point. Taking into account the mean values of the damping factor, the way that the harmonic content damps along the network together with the corresponding short-circuit power is given in Figure 19. In addition, the voltage total harmonic distortion at each bus is shown in Figure 20. It is worth mentioning that the harmonic distortion decreases as the power produced by the WP increases because the current controller seems to operate better at higher current reference as shown in the last figure. From further simulations, it is concluded that increasing the size of the capacitors results in a decrease in the harmonic content. This can be justified by the fact that capacitors act as low-pass filters.

TABLE I

COMPARISON BETWEEN VARIABLE AND FIXED SPEED MODE
OF OPERATION FOR EACH STUDY CASE

Wind Turbine type/ case	FS/1a	VS/1b	FS/2a	VS/2b
Mean wind	7.5	7.5	15	15

speed (m/sec)				
WP Capacity (MVA)	7.5	11	6	8
Used Capacitors (KVar)	550	140	450	140
Voltage THD at WP bus (<6.5%)	-	2.34	-	1.99
Max Voltage drop (<8%)	5	5.8	5.1	4.6
Flicker Pst at WP bus (<0.9)	0.569	0.236	0.376	0.3

The most significant results for each study case are summarized in Table I. This table clearly shows the significant advantages of the proposed VSWT, namely the considerable increase of the installed capacity over FS WTs and the power-quality improvement. Voltage THD is considerably smaller than 6.5%, allowing for the use of a wider hysteresis band.

5. Conclusion

In this paper, results from a study concerning the connection of a VSWP to an actual weak electrical grid are presented. The VS mode of operation studied comprises a voltage-source converter cascade employing field-oriented control for the generator- side converter and three independent hysteresis controllers for the grid-side converter. A simulation tool was developed using the Matlab Simulink environment in order to examine the effects of VS and FS WPs on the operation of weak distribution networks. Using this tool, the advantages of the examined VS mode of operation were highlighted, such as the significantly increased penetration, the attenuation of the voltage fluctuations, and the improved power quality. Furthermore, it was shown that the installation of reactive compensation is essential, even in case that a unity power factor operation is achieved. The existence of an additional voltage-control loop can eliminate this need. It was shown that the harmonic distortion is higher at buses that are nearer to the WP, being rapidly damped at buses located closer to the HV system. For all study cases of VS operation, it was shown that the voltage THD at every bus is considerably lower than the 6.5% limit. It was also shown that using the proposed technology, a 30 to 50% increase of the installed capacity over FS WTs is possible at the same connection point, without violating the power-quality regulations imposed by the local utility. Finally, capacitors next to reactive compensation, act as an additional countermeasure to the propagation of the harmonics produced by the VS WP.

References

[1] The Delhi International Renewable Energy Conference (DIREC 2010) October 2010, in New Delhi, India..

[2] Haniotis, A. E.; Soutis, K.S.; Kladas, A.G.; Tegopoulos, J.A.; "*Grid connected variable speed wind turbine modeling, Dynamic performance and control*," Power system conference in 2004 , pp 759 - 764 vol.2.

[3] Zaragoza, J.staines, C.S, Arias A., Pou. J, Robles. E, Ceballos. S, "*Comparison of speed control strategies for maximum power tracking in a wind energy conversion system*," Melecon 2010, 15th IEEE Electrotechnical conference, 2010, pp: 961-9661997.

[4] Duran, E.; Galan, J., Sidrach-de-Cardona, M., Segura, F., "*An application of interrevealed DC-DC convertors to obtain I-V characteristic curves of photovoltaic modules*," in Proc. IEEE Int. Industrial appl. , pp: 2284-2289, 2008

[5] Shoujun Song, Weiguo Liu, "*A Novel method for Non linear Modeling and dynamic simulation of a four phase switched reluctance Generator system based on Matlab/simulink*," Industrial Electronics and application, pp. 1509, Sep. 2007.

[6] Sharaf, A.M., El-Gammal, A.A.A., "*Optimum Self tuned variable structure sliding mode for co ordinate wind diesel utilized scheme*," 2010 ,fourth Conf. Power., ,pp 431-437, 2010.

[7] Neam, M.M., El-Sousy, F., Ghazy, M.A., Abo-Adma, M.A., "*Pulse width modulation for electronic power converters for renewable energy conversion*," Proc. IEEE, vol. 82, pp. 1682 – 1691, 2009.

[8] Dixon, Juan W., Kulkarni, Ashok B., Nishimoto, Masahiro, Ooi, Boon-Teck, D. M. Brod and D. W. Novotny, "*Characteristics of a Controlled-Current PWM Rectifier-Inverter Link*," IEEE Trans. Ind. Applicat., vol. IA-23, pp. 1022-1028, April 2008.

[9] P. C. Krause, *Analysis of Electric Machinery*. New York: McGraw-Hill, 1986.

[10] N. D. Hatziargyriou P. C. Krause *et al.*, "*Modeling New Forms of Generation and Storage, CIGRE Task Force 38.01.10*,", Paris, France, 2000.

[11] C.-M. Ong, *Dynamic Simulation of Electric Machinery Using Matlab/Simulink*. Englewood Cliffs, NJ: Prentice-Hall, 1998.

[12] W. Leonard, *Control of Electrical Drives*. New York: Springer-Verlag, 1985.

[13] B. K. Bose, *Power Electronics and AC Drives*. Englewood Cliffs, NJ: Prentice-Hall, 1986.

[14] Power *Electronics and Variable Frequency Drives—Technology and Applications*. Piscataway, NJ: IEEE Press, 1997.

[15] H. Siegfried, *Grid Integration of Wind Energy Conversion Systems*. New York: Wiley, 1998.

[16] A. Feijoo and J. Cidras, "*Analysis of mechanical power fluctuations in asynchronous WEC's*," IEEE Trans. Energy Conversion, vol. 14, pp. 284–291, Sept. 1999.

Author's Biographies:

SASI.C (1981) received Bachelor of Engineering in Electrical and Electronics Engineering (2002), Master of Engineering in Power System Engineering (2008) and he is working as Assistant Professor in the Department of Electrical Engineering, Annamalai University, Annamalainagar. He is currently pursuing Ph.D degree in Electrical Engineering from Annamalai University. His research interests are in Power Systems, Renewable source of energy, and Filter design. , Department of Electrical Engineering, Annamalai University, Annamalainagar-608002, Tamilnadu, India, Tel: 91-04144-228428.Mobile:+91-09865230002. **saasi_ceee@yahoo.co.in**

Dr.G.MOHAN (1963) received B.Tech in Instrument Technology (1986), Master of Engineering in Power System Engineering (1999) and Ph.D in Electrical Engineering (2010) from Annamalai University, Annamalainagar. From 1988 he is working as Associate Professor in the Department of Electrical Engineering, Annamalai University, Annamalainagar. His research interests are in Power Systems, and Renewable source of Energy, Department of Electrical Engineering, Annamalai University, Annamalainagar – 608002, Tamilnadu, India, **mg_cdm@yahoo.com**

SLAM for a Mobile Robot using Unscented Kalman Filter and Radial Basis Function Neural Network

Amir Panah[1,2], Samere Fallahpour[2], Omid Panah[3] and Amin Panah[4]

[1]*Member of Young Researchers Club, Qazvin Islamic Azad University, Qazvin, Iran*
[2] *Department of Electrical, Computer and IT Engineering, Qazvin Islamic Azad University, Qazvin, Iran*
[3,4] *Department of Computer Engineering, Islamic Azad University Ayatollah Amoli, Amol, Iran*

Corresponding Adresses
amir.panah2020@gmail.com

***Abstract*:** This paper presents a Hybrid filter based Simultaneous Localization and Mapping (SLAM) for a mobile robot to compensate for the Unscented Kalman Filter (UKF) based SLAM errors inherently caused by its linearization process. The proposed Hybrid filter consists of a Radial Basis Function (RBF) and UKF which is a milestone for SLAM applications. A mobile robot autonomously explores the environment by interpreting the scene, building an appropriate map, and localizing itself relative to this map. The proposed approach, based on a Hybrid filter, has some advantages in handling a robot with nonlinear motions because of the learning property of the RBF neural network. The simulation results show the effectiveness of the proposed algorithm comparing with an UKF based SLAM and also it shows that in larger environments has good efficiency.

***Keywords*:** *SLAM, UKF, RBF, Hybrid filter SLAM.*

1. Introduction

Research efforts on mobile robotics have mainly focused on topics such as obstacle detection, autonomous navigation, path planning, exploration, map building, etc., and many algorithms have been proposed for these purposes [8]. Currently SLAM is one of the most widely researched major subfields of mobile robotics. In order to solve SLAM problems, statistical approaches, such as Bayesian Filters, have received widespread acceptance. Some of the most popular approaches for SLAM include using a Kalman filter (KF), an extended Kalman filter (EKF) and an unscented Kalman filter (UKF) and a particle filter [9]. As in any UKF based algorithm, the UKF SLAM makes a Gaussian noise assumption for the robot motion and its perception. In addition, the amount of uncertainty in the posterior of the UKF SLAM algorithm must be relatively small; otherwise, the linearization in the UKF tends to introduce unbearable errors. The UKF uses the unscented transform to linearize the motion and measurement models. Especially, the UKF is usually used in order to compensate for the EKF's drawbacks which inherently results from linear approximation of nonlinear functions and the calculation of Jacobian matrices [13]. RBF neural network, adaptive to the changes of environmental information flowing through the network during the process, can be combined with an UKF to compensate for some of the disadvantages of an UKF SLAM approach, which represents the state uncertainty by its approximate mean and variance [4,12].

Houshangi and Azizi [5] integrated the information from odometry and gyroscope using UKF. To improve the performance of odometry, a fiber optic gyroscope is used to give the orientation information that is more reliable. This method is simple to implement, needless to frequent calibration and applicable to different situations likely EKF. The results show that the UKF estimates the robot's position and orientation more accurately than the EKF.

Ronghui Zhan and Jianwei Wan [10] presents a robust learning algorithm for an multilayered neural network based on UKF is derived. Since it gives a more accurate estimate of the link weights, the convergence performance is improved. The algorithm is then extended further to develop a neural network aided UKF for nonlinear state estimation. The neural network in this algorithm is used to approximate the uncertainty of the system model due to mismodeling, extreme nonlinearities, etc.

Lee and Choi [9] present a Hybrid filter SLAM scheme for a mobile robot to compensate for the EKF based SLAM errors inherently caused by its linearization process. The proposed Hybrid filter consists of a neural networks and EKF.

Choi et al [2] approached the SLAM problem with a neural network based on an extended Kalman filter (NNEKF). When the robot is trained online by a neural network, the NNEKF can capture the unmodeled dynamics, and adapt to the changed conditions intelligently. According to the research results, the NNEKF SLAM, shows better performance than the EKF SLAM.

In this paper, we present a Hybrid approach using RBF neural network and UKF based SLAM problem for decreasing uncertainty in compare to SLAM using UKF.

We also discuss the effectiveness of RBF algorithm to handle nonlinear properties of a mobile robot.

Some related algorithms on SLAM are described in section 2, and the Hybrid SLAM algorithm is presented in section

3. Section 4 shows the simulation results of the SLAM based on UKF, and Hybrid filter. Concluding remarks, discussion and further research are discussed in section 5.

2. Related Algorithms for SLAM

2.1 Radial Basis Function Neural Network

Design of artificial neural networks is motivated by imitating human brain and thinking activities as a mechanical tool for various purposes.

Frequently, neural networks are used especially in modeling and simulation of nonlinear systems. Neural networks have two fundamental characteristics of learning based on experimental data and structural parallel. RBF neural network is proposed as a neural network model by Moody and Darken. In RBF neural network, originally, RBF, approximation density function and level fitting technique, are considered as probability functions. RBF neural network typically have three layers, namely, an input layer, a hidden layer with a nonlinear RBF activation function, and a linear output layer. Input layer transfers all data information to hidden layer. This transfer is done through a series of communications with unknown weights. This hidden layer consists of local basis functions. Often, a function is used which is called Gaussian function and does a nonlinear transition process and it is completely local [6].

Network training is divided into two stages: first, the weights from the input to the hidden layer are determined; then, the weights from the hidden layer to the output layer are determined. The results can be used to simulate the nonlinear relationship between the sensors measurements with the errors, and the ideal output values by using the least squares method [14].

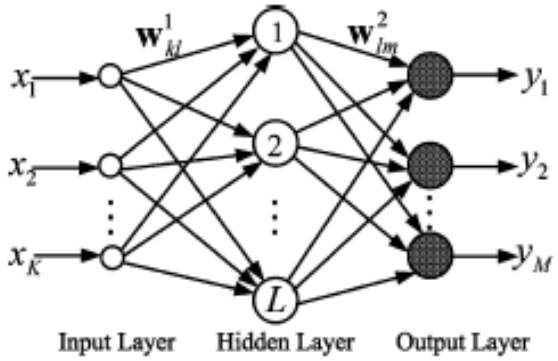


Figure 1. A Radial Basis Function Neural Network Structure

2.2 Unscented Kalman Filter

UKF was introduced for the first time by Uhlmann and Julier in 1997. This filter is built based on transformation as unscented transformation.

The base of this transformation is based on this principal which states the estimation a probability is easier than a nonlinear function or a nonlinear transformation. UKF method is more accurate than the EKF for estimation of nonlinear systems [7]. EKF for linearization of nonlinear system only uses the first term of Taylor series. Therefore, in cases where the system is fully nonlinear and higher terms in the Taylor series are important, Linearization model by this method is not a good approximation of the real system and this leads to lack of accuracy in the estimation of states or parameters of these types of systems. In The UKF, there is no need to calculate Jacobian matrix. Since, the process noise in this system is accumulative; therefore the augment state vector is used to implementation this method. In this method, the mean and covariance estimation are calculated with considering the second order of the Taylor series [7].

Suppose that a random variable x with mean μ and covariance P_x is given and also a random variable z as with x is associated: $z=f(x)$. Problem calculating the mean and covariance z is, as predicted and corrected the problem in stages UKF a nonlinear system. In the method of unscented transformation, to obtain the mean and covariance random variable z, a set of weighted points called sigma points are used. This sigma points should be selected so that have a mean μ and covariance P_x.

An n-dimensional random variable can be approximated by a set of 2n+1 weighted sigma points given by the following deterministic algorithm:(0<i<n)

$$X_0 = \mu, W_0 = \frac{\lambda}{n+\lambda} \quad (1)$$

$$X_i = \mu + (\sqrt{(n+\lambda)P_x})_i, W_i = \frac{\lambda}{2(n+\lambda)} \quad (2)$$

$$X_{i+n} = \mu - (\sqrt{(n+\lambda)P_x})_i, W_{i+n} = \frac{\lambda}{2(n+\lambda)} \quad (3)$$

$$\lambda = \alpha^2 (n+\beta) - n \quad (4)$$

n number of state variables are augmented. Also, α and β are the coefficients that with their adjustment, the estimation error can be minimized and their values influence on the error rate resulting from higher terms in the Taylor series. In the above relations, $k \in R$ and $(\sqrt{(n+\lambda)P_x})_i$, the i-th row or column of the matrix is the square root of $(n+\lambda)P_x$, W_i is the weight which is associated with the i-th point and k also is used for adjusting the filter more accuracy [7].

Unscented transformation algorithm, first, each point of the set points by a nonlinear function for mapping to a new point and will obtain a new set of sigma points. Then, we can calculate the mean and covariance values of the new random variable. Consider the following nonlinear system:

$$x_k = f(x_{k-1}, u_{k-1}, \varepsilon_k) \quad (5)$$

$$z_k = h(x_k, u_k, \delta_k) \quad (6)$$

Where x is state vector and u is control input and ε, δ are the system noise and the measurement noise, respectively. In the first phase of implementing this filter, the augment state vector will become as the following form:

$$X_k^a = \begin{bmatrix} X_k \\ \varepsilon \\ \delta \end{bmatrix} (7)$$

In continue, we will see all the formulas which has been implemented in the UKF in which itself includes of two main from sections: Measurement update and Time update [11].

2.2.1 The Time Update

$$X_k^a = f(X_k^a, u_k, \varepsilon_k) (8)$$

$$\mu_k = \sum_{i=0}^{2n} w_i X_{i,k}^a (9)$$

$$P_k = \sum_{i=0}^{2n} w_i \left[X_{i,k}^a - \mu_k\right]\left[X_{i,k}^a - \mu_k\right]^T (10)$$

$$z_k = h(x_k, u_k, \delta_k) (11)$$

$$\overline{z_k} = \sum_{i=0}^{2n} w_i z_k (12)$$

2.2.2 The Measurement Update

$$P_{x_k x_k} = \sum_{i=0}^{2n} w_i \left[z_{i,k} - \overline{z_k}\right]\left[z_{i,k} - \overline{z_k}\right]^T (13)$$

$$P_{x_k y_k} = \sum_{i=0}^{2n} w_i \left[X_{i,k}^a - \mu_k\right]\left[z_{i,k} - \overline{z_k}\right]^T (14)$$

$$K_k = P_{x_k y_k} P_{x_k x_k}^{-1} (15)$$

$$\mu_k = \mu_k + K_k(z_k - \overline{z_k}) (16)$$

$$P_k = P_k - K_k P_{x_k x_k} K_k^T (17)$$

Where X_k^a, μ_k, P_k, z_k, $\overline{z_k}$, $P_{x_k x_k}$, $P_{x_k y_k}$ and K_k, are motion model, predicted mean, observation model, predicted observation, innovation covariance, cross correlation matrix and Kalman gain, respectively.

2.3 SLAM Using Unscented Kalman Filter

A solution to the SLAM problem using UKF, with many interesting theoretical advantages, is extensively described in the research literature. This is despite the recently reported inconsistency of its estimation because it is a heuristic for the nonlinear filtering problem. Associated with the UKF is the Gaussian noise assumption, which significantly impairs the UKF SLAM's ability to deal with uncertainty. With a greater amount of uncertainty in the posterior, the linearization in the UKF fails. An UKF based on a Bayes filter has two steps, prediction and correct, for SLAM using the measured sensor data of a mobile robot.

3. SLAM Algorithm Using Hybrid Filter

A new Hybrid filter SLAM with UKF is proposed here, augmented by an RBF acting as an observer to learn the system uncertainty online. An adaptive state estimation technique using an UKF and a RBF has been developed. The mean, μ_k which is derived from environmental information values $(xy\theta\varepsilon\delta)$ using the RBF algorithm, is entered to the prediction step, as shown in Figure 2.

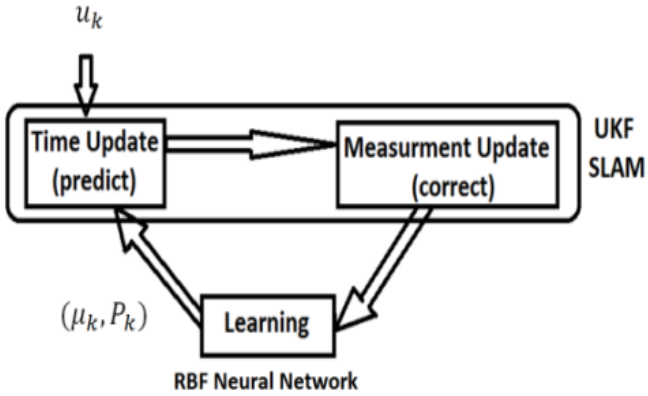


Figure 2. The architecture of the Hybrid filter SLAM

In this paper, Basic inputs are mean, covariance which are calculated by prior input, u_{k-1}, and present input, u_k. The robot calculates the prior mean and covariance in a prediction step, and then, in an observation step, it calculates a Kalman gain, present mean and covariance and defined features.

RBF neural network is very important, as the kernel of the Hybrid filter is the complementation of errors onto stochastic UKF SLAM processing through the training process. RBF neural network can operate as a fast and accurate means of approximating a nonlinear mapping based on observed data.

3.1 Time Update (Predict)

The Hybrid filter SLAM algorithm is described using a robot's pose and features, such as the location of landmarks. For the SLAM, the basic motion model of the mobile robot needs to be presented. A configuration of the robot with a state equation $X^a = (xy\theta\varepsilon\delta)^T$, has the form of Eq. (18) since it is assumed that the robot is equipped with encoders and exteroceptive sensors.

$$X_K^a = \begin{bmatrix} x_k \\ y_k \\ \theta_k \\ \varepsilon_k \\ \delta_k \end{bmatrix} = \begin{bmatrix} x_{k-1} + v_k \Delta t \cos(\theta_k) \\ y_{k-1} + v_k \Delta t \sin(\theta_k) \\ \theta_{k-1} + v_k \Delta t \sin(\frac{\Delta\theta}{L}) \\ \varepsilon_{k-1} \\ \delta_{k-1} \end{bmatrix} (18)$$

$$u_k = v_k + N(0, M_k) (19)$$

Where v_k is velocity of wheels, and L is the width between the robot's wheels, and Δt is the sampling period. Finally, M_k describes the covariance matrix of the noise in control space. The state equation for

landmarks, combined with the robot position, is denoted by the vector Y_k, where c is the number of landmarks. (0<i<c)

$$Y_k^a = \begin{bmatrix} X_k^a \\ m \end{bmatrix} = (x_k y_k \theta_k \varepsilon_k \delta_k, m_{k,x}^i m_{k,y}^i s_k^i 00)^T \quad (20)$$

The state transition probability of a Hybrid filter SLAM has the form of Eq. (21):

$$X_k^a = f(X_{k-1}^a, u_{k-1}) + N(0, \varepsilon_K) \quad (21)$$

Under the linearity assumption where f represents the nonlinear functions, ε_k is the process noise, and u_k is control input.

For the Taylor expansion of function, f its partial derivative is used with respect to X_k^a, as shown in Eq. (22).

$$f'(X_{k-1}^a, u_k) = \frac{\partial f(X_{k-1}^a, u_k)}{\partial X_k^a} \quad (22)$$

f is approximated at u_k and u_{k-1}. The linear xtrapolation is achieved by using the gradient of f at u_k and u_{k-1} as shown in Eq. (23).

$$f(X_{k-1}^a, u_k) = f(u_{k-1}, u_k) + f'(u_{k-1}, u_k)(X_k^a - u_{k-1}) \quad (23)$$

With the replacement values obtained from equations 1, 2, 3, 4, 5, prior mean and covariance have the following form of:

$$\mu_k = \sum_{i=0}^{2n} w_i X_{i,k}^a \quad (24)$$

$$P_k = \sum_{i=0}^{2n} w_i \left[X_{i,k}^a - \mu_k\right]\left[X_{i,k}^a - \mu_k\right]^T \quad (25)$$

As described in Eq. (26), the observation model, Z_k consists of the nonlinear measurement function h and the observation noise δ_k.

$$Z_k = h(Y_k^a) + N(0, \delta_k) = \begin{bmatrix} \sqrt{(m_{k,x}^i - x_k)^2 + (m_{k,y}^i - y_k)^2} \\ \tan^{-1}\left(\frac{m_{k,y}^i - y_k}{m_{k,x}^i - x_k}\right) - \theta_k \end{bmatrix} + N(0, \delta_k) \quad (26)$$

$$m^i = (m_x^i m_y^i)^T \quad (27)$$

$$\bar{z}_k = \sum_{i=0}^{2n} w_i Z_k \quad (28)$$

3.2 *The Measurement Update (Correct)*

To obtain the Kalman gain K_k, we need to calculate $P_{x_k x_k}$ and $P_{x_k y_k}$ in the feature-based maps. To obtain the values $P_{x_k x_k}$ and $P_{x_k y_k}$, it is necessary to calculate X_k^a, μ_k, Z_k, $\bar{z}_k$, that are calculated in equations 18, 24, 26, 28, with replacement of these values, we will have the following equations:

$$P_{x_k x_k} = \sum_{i=0}^{2n} w_i \left[z_{i,k} - \bar{z}_k\right]\left[z_{i,k} - \bar{z}_k\right]^T \quad (29)$$

$$P_{x_k y_k} = \sum_{i=0}^{2n} w_i \left[X_{i,k}^a - \mu_k\right]\left[z_{i,k} - \bar{z}_k\right]^T \quad (30)$$

$$K_k = P_{x_k y_k} P_{x_k x_k}^{-1} \quad (31)$$

In this following, RBF algorithm with UKF are considered to complete SLAM of the mobile robot. RBF algorithm is involved with train through input data and measurement values. In the training process, weights are decided based on the relation of input data and each hidden layers. RBF algorithm need higher weight to objective value on the higher relations between poses and heading angle with comparing to measurement. When applying the other case for RBF, it is the same to substitute inputs. The RBF algorithm generally consists of two weight layers; one hidden layer and the output layer. In addition, the second weight, ω_0, equals zero because the output offset is zero. Therefore, new estimated mean, can be described as in Eq. (32) [9]: (0≤j≤J-1)

$$\hat{\mu}_k^j = \omega_0 + \sum_{j=0}^{j-1} \omega_i \varphi_k^j(\mu_k^j) \quad (32)$$

$$= \xi\left(\sum_{j=0}^{j-1} \varphi_k^j(\mu_k^j)\right) = \xi\left(\sum_{j=0}^{j-1} \exp\left(-\frac{\|\mu_k^j - d^j\|^2}{2(\tau^j)^2}\right)\right)$$

μ_k is an n-dimensional input vector and d^j stands for the center of the j-th basis function with the same dimension of the input vector. In the equations considered, τ^j denotes the width of the basis function, N is the number of hidden layer's nodes, $\|\mu_k^j - d^j\|$ describes the Euclidean norm of representing the distance between μ_k^j and, d^j and $\varphi_k^j(x)$ means the response of the j-th basis function of the input vector with a maximum value at d^j. The next process to obtain the prior mean and the covariance is to update the results from Eq. (32). The process described in the above 5 steps repeats until the end of the navigation.

$$\mu_k = \hat{\mu}_k + K_k(z_k - \bar{z}_k) \quad (33)$$

$$P_k = P_k - K_k P_{x_k x_k} K_k^T \quad (34)$$

4. Simulations

To show the effectiveness of the proposed algorithm, the Matlab code, developed by Bailey [1], was modified. The simulation was performed with constraints on velocity, steering angle, system noise, observation noise, etc., for a robot with a wheel diameter of 1[m] and maximum speeds of 3[m/sec]. The maximum steering angle and speed are 25[°] and 15[°/sec] respectively.

The control input noise is assumed to be a zero mean Gaussian with σ_v(=0.2[m/s]) and σ_φ(=3[°]). For observation, the number of arbitrary features around waypoints was used. In the observation step, a range bearing sensor model and an observation model were used to measure the feature position and robot pose, which includes a noise with level of 0.1[m] in range and 1[°] in bearing. The sensor range is restricted to 15[m] for small areas and 30[m] for large areas, which is sufficient to detect all features in front of the mobile robot.

In this research, two navigation cases of the robot are surveyed: a Rectangular navigation, and a Widespread navigation. Specifications of the navigation maps are described in Table 1.

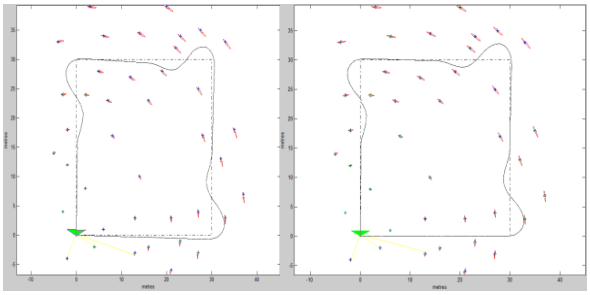
Table 1. Fundamental specification for navigation

Item	Rectangular	Widespread
Feature	40	35
Waypoint	5	18
Area[m]	30*30	200*160

4.1 Navigation on Rectangular map

In the case of rectangular navigation, the UKF based navigation and Hybrid filter based navigation are shown in Figure 3, where both results show distortions during navigation at the three edges. The mobile robot decides a direction for the navigation based on the information from the locations of landmarks detected, but it does not instantly turn because it has 1[°] in bearing when the robot tries to turn through the edges.

The dashed line, show the paths of robots should traverse and the bold black line is Robot path, based on data described by the actual odometry. In Figure 4, the dashed gray line and the bold black line are the x, y, and θ errors in the case of UKF SLAM and Hybrid filter SLAM with RBF algorithm, respectively.



UKFSLAM RBF UKFSLAM

Figure 3. Navigation result on rectangular map

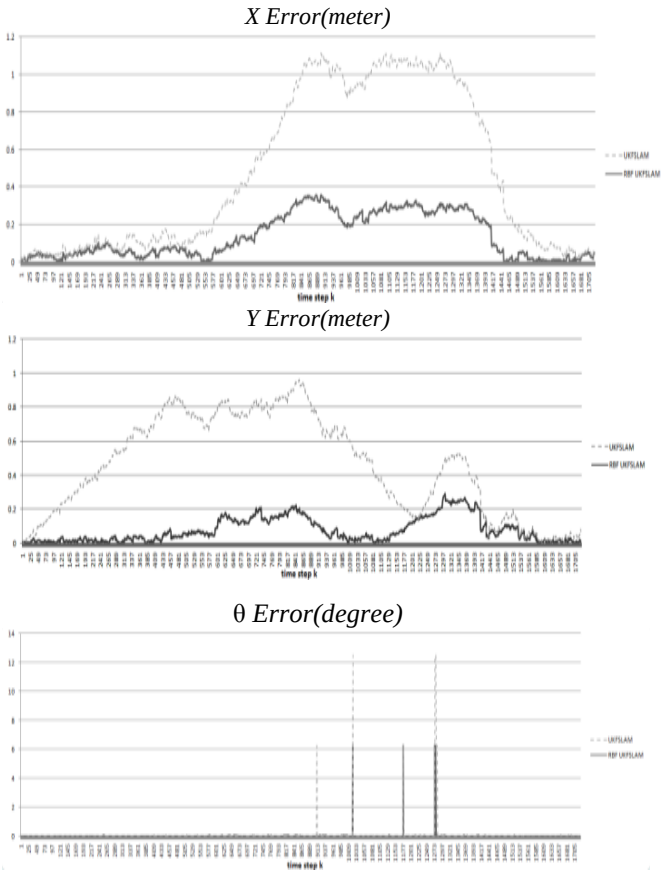
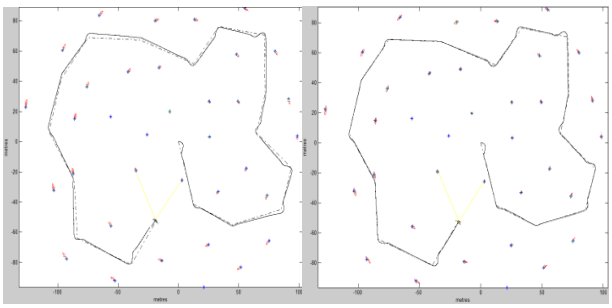


Figure 4. Navigation errors on rectangular map

4.2 Navigation on Widespread map

In the case of widespread navigation, the UKF based navigation and Hybrid filter based navigation are shown in Figure 5, where more diversions are shown in edges with larger angle during navigation. The mobile robot decides a direction for the navigation based on the information from the locations of landmarks detected, but it does not instantly turn in edges because unpredictable changes in incoming data. The dashed line, show the paths of robots should traverse and the bold black line is Robot path, based on data described by the actual odometry. In Figure 6, the dashed gray line and the bold black line are the x, y, and θ errors in the case of UKF SLAM and Hybrid filter SLAM with RBF algorithm, respectively.



UKFSLAM RBF UKFSLAM

Figure 5. Navigation result on widespread map

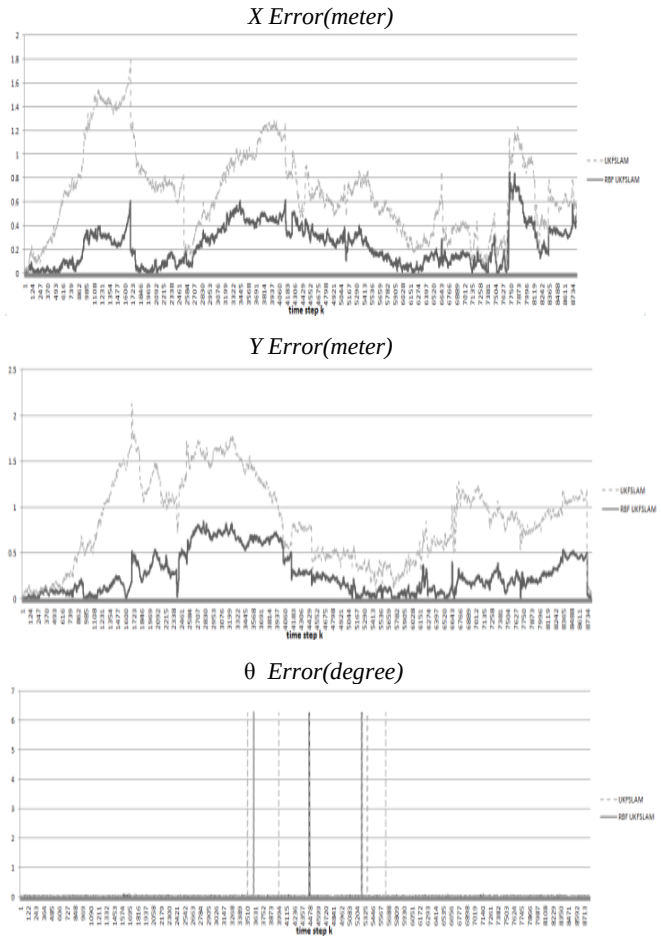


Figure 6. Navigation errors on widespread map

5. Conclusions

The SLAM is one of the most fundamental problems in the quest for autonomous mobile robots since the robot keeps track of its location by maintaining a map of the physical environment and an estimate of its position on that map. This paper proposes Hybrid filter SLAM methods, the RBF SLAM with UKF on a mobile robot, to make up for the UKF SLAM error inherently caused by its linearization process and noise assumption. The proposed algorithm consists of two steps: the RBF Neural Network and the UKF algorithm. The simulation results for two different navigation cases show that the efficiency of the proposed algorithm based on RBF as compared with the UKF SLAM and it also shown that provided algorithms has favorable results in wider environment but we need to use long range sensors. To verify the effectiveness of the proposed algorithm, simulation in Matlab with UKF and RBF are performed. Based on the simulation results, UKF SLAM has more errors than Hybrid filter SLAM. In addition, the results confirm the Hybrid filter SLAM is more stable for robot navigation in the simulation. Research under harsh and real-time condition is under way to verify the robustness of the proposed algorithm by fuzzy logic or changing structures of neural networks.

References

[1] Bailey,T., http://www.personal.acfr.usyd.edu.au/tbailey

[2] Choi, M. Y., Sakthivel, R. and Chung, W. K., "Neural network aided extended Kalman filter for SLAM problem," IEEE International Conference on Robotics and Automation, pp. 1686-1690, 2007.

[3] Cho, S. H., "Trajectory Tracking Control of a Pneumatic X-Y Tabel using Neural Network Based PID Control," Int. J. Precis. Eng. Manuf., Vol. 10, No. 5, pp. 37-44, 2009.

[4] Harb, M., Abielmona, R., Naji, K. and Petriul, E., "Neural networks for environmental recognition and navigation of a mobile robot," IEEE International Instrumentation and Measurement Technology Conference, pp. 1123-1128, 2008.

[5] Houshangi, N. and Azizi, F., "Accurate mobile robot position determination using unscented Kalman filter," 2005 Canadian Conference on Electrical and Computer Engineering, pp. 846-851, 2005.

[6] Hu, Y. H. and Hwang, J. N., "Handbook of Neural Network Signal Processing," CRC Press, pp. 3.1-3.23, 2001.

[7] Julier S.J., and Uhlmann J.K., "A New Extension of Kalman Filter to Nonlinear Systems". Proceedings of AeroSense: The 11th Int.Symp.on Aerospace/Defence Sensing, Simulation and Contro., 199**7.**

[8] Kim, J. M., Kim, Y. T. and Kim, S. S., "An accurate localization for mobile robot using extended Kalman filter and sensor fusion," IEEE International Joint Conference on Neural Networks, pp. 2928-2933, 2008.

[9] Kyung-Sik Choi,Suk-Gyu Lee, "Enhanced SLAM for a Mobile Robot using Extended Kalman Filter and Neural Networks", INTERNATIONAL JOURNAL OF PRECISION ENGINEERING AND MANUFACTURING Vol. 11, No. 2, pp. 255-264, APRIL 2010.

[10] R. Zhan and J. Wan, "Neural Network-Aided Adaptive Unscented Kalman Filter for Nonlinear State Estimation," *IEEE Signal Processing Letters*, Vol. 13, No. 7, pp. 445-448, 2006.

[11] Scott F.Page, "Multiple-Opbject sensor Managment and optimization". PHD thesis, in the faculty of Engineering, Science and mathematic School of Electronics and Computer science, June 2009.

[12] Vafaeesefat, A, "Optimum Creep Feed Grinding Process Conditions for Rene 80 Supper Alloy Using Neural network," Int. J. Precis. Eng. Manuf., Vol. 10, No. 3, pp. 5-11, 2009.

[13] Zhu, J., Zheng, N., Yuan, Z., Zhang, Q. and Zhang, X., "Unscented SLAM with conditional iterations," 2009 IEEE Intelligent Vehicles Symposium, pp. 134-139, 2009.

[14] Zu, L., Wang, H. K. and Yue, F., "Artificial neural networks for mobile robot acquiring heading angle," Proceedings of the Third Intemational Conference on Machine Laming and Cybemetics, pp. 26-29, 2004.

ojs.excelingtech.co.uk/index.php/IJLTC