International Journal of Latest Trends in

NETWORKS & COMMUNICATION

Volume 1 No.1
June, 2011

Web: excelingtech.co.uk
ojs.excelingtech.co.uk/index.php/IJLTNC

Editorial Board

Table of Contents

1. **Balanced Multiwavelet Based Mammogram Image Processing**.. 1

   D.M.Garge, Dr.V.N.Bapat

2. **Origin Authentication of Digitally Signed Message Using Joint Signature Scheme in Mobile Commerce** 6

   Aihab Khan, Malik.Sikandar Hayat Khiyal, Sara Ayub

3. **Non Repudiation in M- Commerce Using Joint Signature Scheme** 13

   Aihab Khan, Malik Sikandar Hayat Khiyal, Madiha Tariq

Balanced Multiwavelet Based Mammogram Image Processing

D.M.Garge[#1], Dr.V.N.Bapat[#2]

[#1] *Lecturer in Electronics, Government Polytechnic, Kolhapur, India,*
[#2]*Principal, A.D. College of Engineering, Ashta, India,*
[1]dattagarge@yahoo.com
[2]vbkanhaji@gmail.com

***Abstract*- This paper deals with the mammogram image processing using balanced multiwavelets. The property of balancing proves to be central to the different issues ,like the preservation of smoothness in images, improving the enrgy compaction ratio etc.Using balanced multiwavelets, one can avoid the steps of pre and post filtering, that is required with systems based on unbalanced multiwavelets. Medical researchers along with mathematicians and technologists are working with mammogram images to detect breast cancer at an early stage. Until recently, the wavelet and multiwavelet theory has been applied successfully in the domain of computer aided diagnostics of cancer. However, the analytical speculations indicate that the balanced multiwavelets have great potential in mammogram image processing. The present communication reports mammogram image processing using balanced multiwavelets implemented using MATLAB.**

Keywords- *Mammograms, Image Processing, Balanced Multiwavelet, MATLAB*

1. Introduction

Wavelet and multiwavelet transform is a useful tool for signal processing applications such as image compression and de-noising. Literature survey reveals extensive work in the field of scalar wavelets and multiwavelets. The latest entrant in the wavelet paradigm are the ‘Balanced Multiwavelets’. They have several advantages such as smotthness in scaling and wavelet functions, regularity of multiwavelets, particularly significant in signal processing applications; to name a few.[9] The present paper describes implementation and application of balanced multiwavelets for mammogram image processing, which would play a vital role in an early detection of the breast cancer. We report here a simple method to generate balanced multiwavelet of order one and two and its application in image denoising. Experimental results of application of balanced multiwavelets to mammogram images have also been presented in this paper.

While the authors have extensively dealt with the mammogram image processing with multiwavelets elsewhere [13], it is intended to present experimental results regarding processing of mammogram images using balanced multiwavelets in the present communication.

The paper is organized as follows. At the outset, the background information related to the breast cancer is presented along with the literature review of mammogram image processing techniques in Section II. Section III describes the focus of present work and section IV covers methodology adopted. Section V summarizes theory of balanced multiwavelets. At the end experimental results are presented.

2. Literature Survey and Prior Art

Literature survey reveals that the mammograms and their analysis by the way of image processing has found to be on up-surge the interest of good number of researchers. Being an interdisciplinary area of research, there are contributions from many disciplines such as statistics, mathematics, computer and medical professionals and social scientists. The role of application of statistical algorithm seems to be dominating in this area.

The pioneering work in this area is done by Woods K. S. et.al. [2] and Solka J. L. et. al. [3] in applying the computer aided detection (CAD) of the Brest cancer. Later, the techniques are refined by using various methods such a heuristics, fuzzy reasoning, Vector Space Machines, morphological approach and use of adaptive wavelet transform, CAD systems using filter banks etc. [4], [5], [6] The research work seems to be forging on several directions such as conceiving improved algorithms, development of novel analytical framework, development of custom hardware based on programmable logic design etc.

3. Focus of the Present Work

In spite of great deal of research work in this area briefly reviewed in section II, there are still challenges lying ahead due to inherent limitations of the scalar wavelets and multiwavelets. Some of the limitations are difficulty in combining the symmetry, orthogonality and second order approximation. Multiwavelet processing requires pre and post filtering of signal to be processed. Balanced Muliwavelets offer possibility of superior performance for mammogram image processing applications as compared with scalar wavelets and multiwavelets. Foundational work in conceptualizing the Multiwavelet system is reported by Geronimo, Hardin and Massopust (GHM) [7]. The basic technique of balanced multiwavelet has been evolved in many directions. One of the major directions is balanced Multiwavelet system with higher order balancing as reported by Lebrun and Vetterli (BAT01, BAT02).[9] Yet another interesting piece of work in this field is Orthogonal Balanced Multiwavelet (BAT 01); [14] that has great potential for denoising mammograms. The present work synergizes the above mentioned techniques viz. GHM, BAT01 and BAT 02, to pave the benefits of accurate classification of mammograms. The advantages of our implementation are evident from the results compared with the traditional Daubechies scalar wavelet (D4) used for the same purpose.

4. Methodology Adopted

Our methodology comprises of the following sequence of steps:

a. Scaling functions and wavelets for first order balanced and order 2 balanced multiwavelets are implemented in MATLAB.

b. The test mammograms for processing are taken from images available at http://www.cancer.org [10]

c. The test images are decomposed and reconstructed using wavelet, Multiwavelet and balanced multiwavelet systems mentioned earlier. Analytical measures like mean square error (MSE), root MSE, distortion, signal to noise ratio and energy compaction ratio (ECR) are used for experimentation.

d. Then test images are mixed deliberately with Gaussian noise, using function available in MATLAB [11]. These noisy images are decomposed by wavelet, multiwavelets and balanced multiwavelets.

e. Images are reconstructed using approximate coefficients only. Analytical measures mentioned in step 2 are calculated.

5. Balanced Multiwavelets

It is possible to design orthonormal linear phase FIR filter systems to construct multiwavelets. However, prefiltering step turns out to be crucial when applied to scalar valued data. To avoid prefiltering, concept of balancing is introduced in [15] which is extended to higher orders in [9]. Using these results, we have constructed orthonormal multiwavelets of order 1 using filter coefficients shown in table I. Figure 1 and figure 2 show scaling and wavelets constructed using these coefficients. In first order balanced multiwavelet, scaling function is flipped around 1 and wavelets are symmetric / antisymmetric, the length is three tap (2 X 2). In order 2 balanced multiwavelet, scaling function is flipped around 2 and wavelets are again symmetris / antisymmetric, the length is five taps (2 X 2).

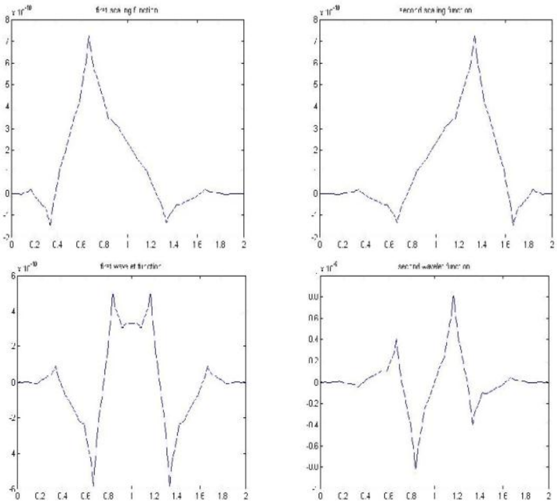

Figure 1. BAT01 scaling function and wavelets

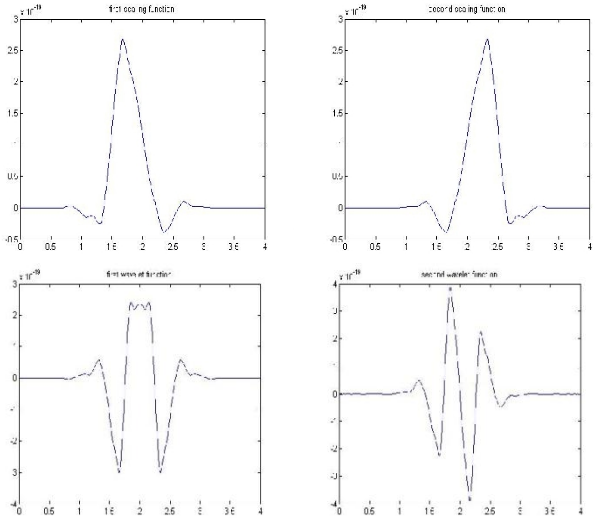

Figure 2. BAT02 scaling function and wavelet

Table 1. Coefficients of BAT01

	Hk	Gk
k=0	0 2+√7 0 2+√7	0 -2 0 1
k=1	3 1 1 3	2 2 -√7 √7
k=2	2-√7 0 2+√7 0	-2 0 -1 0
factor	1/4√2	1/4

6 Metrics Defined

In order to characterize the performance of the system, certain benchmarking parameters are required. This section formally defines all such parameters.

5.1 Mean square error (mse)

$$= \left[\frac{1}{(M \times N)}\right] \sum_{x=1}^{M} \sum_{y=1}^{N} (S(x,y) - (S'(x,y))^2$$

where S(x,y) is original mammogram image and S'(x,y) is denoised mammogram image.

5.2 RMSE = square root of MSE

$$\sum_{x=1}^{M} \sum_{y=1}^{N} (S(x,y) - (S'(x,y))^2$$

5.3 Distortion = $\sum_{x=1}^{M} \sum_{y=1}^{N} S(x,y)^2$

5.4 SNR = 1 / Distortion

5.5 ECR is defined as

$$\text{ECR} = \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} S'(x,y)^2}{\sum_{x=1}^{M} \sum_{y=1}^{N} S(x,y)^2}$$

where S(x,y) is coefficient matrix of mammogram consisting of approximate and detail coefficients, and S^(x,y) is coefficient matrix with approximate coefficients equal to zero.

5.6 Correlation as defined in MATLAB using function corr2( ).

7 Results and Discussion

Figures 3 to 12 reveals the wavelet, Multiwavelet and balanced multiwavelet based processing of mammogram image. Figure 3 shows original mammogram showing micro calcification. This mammogram is decomposed and reconstructed using D4 wavelet and multiwavelets as shown in figures 4, 5, 6 and 7. Table 2 shows statistical results obtained from these images. These results and figures clearly indicate the superiority of the balanced multiwavelets over the other wavelets for accurate classification of mammograms. Energy compaction ratio (ECR) also portrays more information concentrated in low pass part of Multiwavelet transform than in the low pass part of wavelet transform as seen from table 2. Original mammogram image is deliberately added with Gaussian noise of mean average value zero, to create noisy image as shown in figure 8. The subsequent processed denoised images are shown in figures 9, 10, 11 and 12.

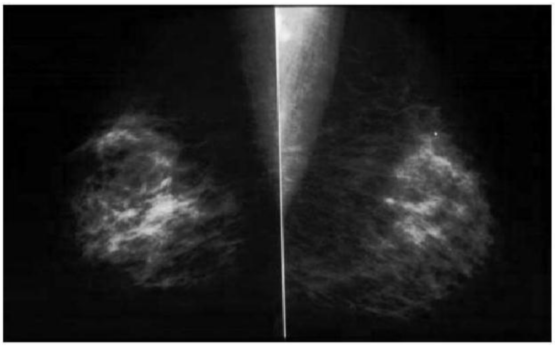

Figure 3. Original mammogram Figure

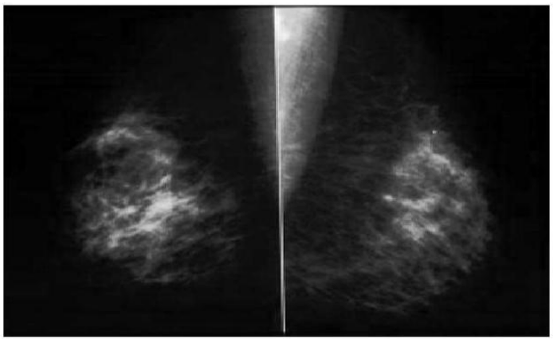

Figure 4. Mammogram reconstructed by D4 wavelet

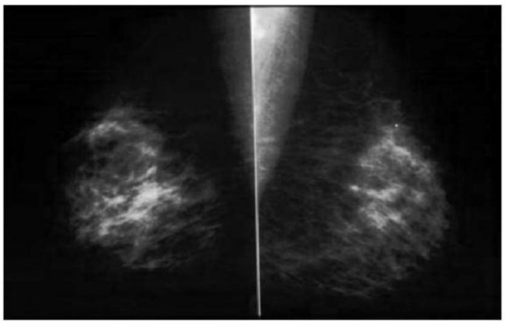

Figure 5. Mammogram reconstructed by GHM multiwavelet

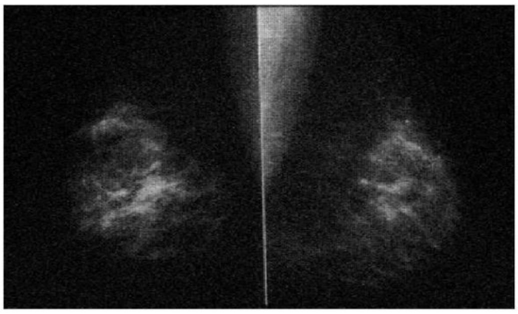

Figure 6. Mammogram reconstructed by BAT01 multiwavelet

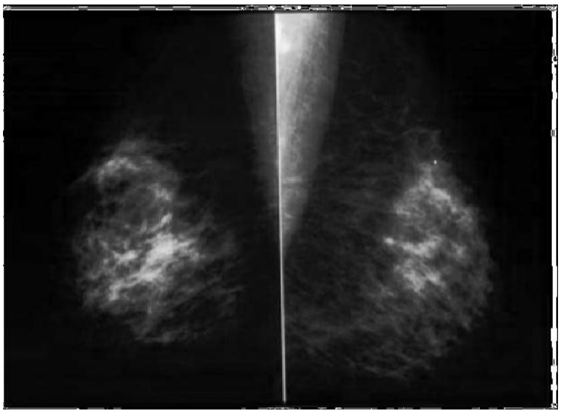

Figure 7. Mammogram reconstructed by BAT02 multiwavelet

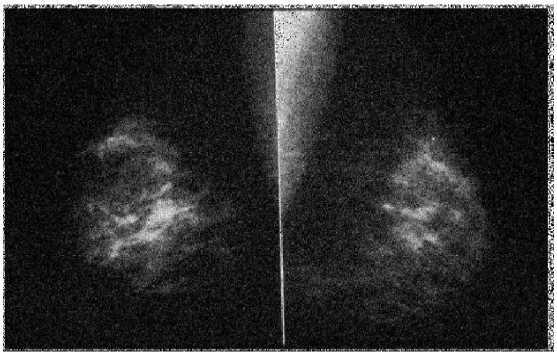

Figure 8. Noisy mammogram

Table 2. Statistical results of decomposition and reconstruction of image

Statistical Measures	D4	GHM	BAT 01	BAT 02
MSE	9.0193	3.8018	3.6238	3.3454
RMSE	3.003	1.949	1.9036	1.829
Distortion	0.0039	0.0016	0.0015	0.0013
SNR	256.106	607.5764	666.676	769.237
Correlatio	0.9967	0.9986	0.9987	0.9991
ECR	0.0039	0.002	0.0036	0.0039

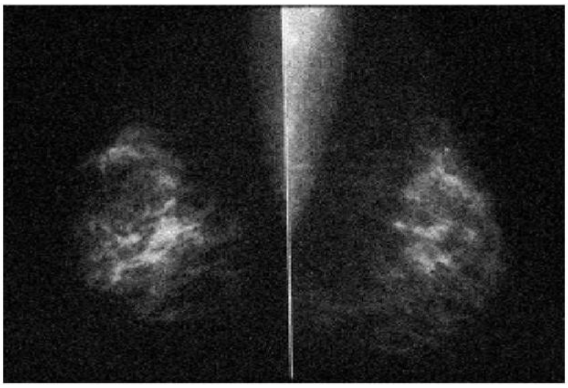

Figure 9. Denoised mammogram by D4 wavelet

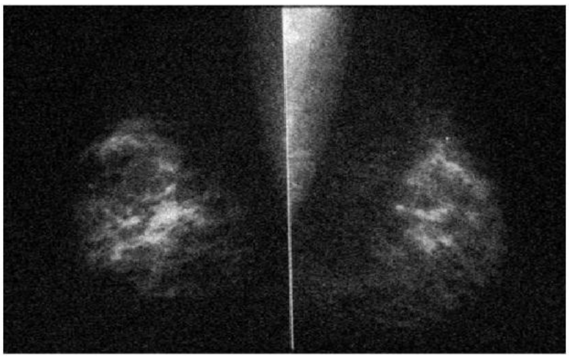

Figure 10. Denoised mammogram by GHM multiwavelet

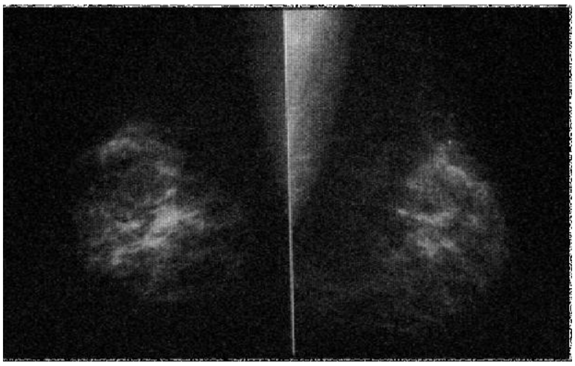

Figure 11. Denoised mammogram by BAT01 multiwavelet

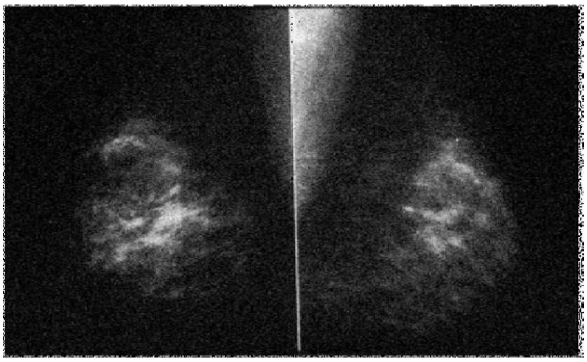

Figure 12. Denoised mammogram by BAT02 multiwavelet

8 Conclusion

After reviewing recent emergence of multiwavelets, we have examined the possibility of multiwavelets in mammogram image processing, especially for denoising application. We used simple method of decomposition – reconstruction of image using wavelet and multiwavelet transform to verify the superiority of balanced multiwavelets. From above results, it is seen that balanced Multiwavelets have been proved to be superior to other wavelets, both numerically and subjectively. Visually Multiwavelet schemes seemed to preserve the edge better and reduce Cartesian artifacts present in scalar wavelet denoising. This work perhaps might be possibly extended further in which other multiwavelets could be applied to mammogram images to find out most suitable multiwavelet for a particular mammogram.

References

[1] Gilbert Strang, "Short wavelets and matrix dilation equations*" IEEE transactions on signal processing*, vol. 43, No. 1, pp. 108-115, January 1995.

[2] Woods, K.S.,et.al. "Comparative evaluation of pattern recognition techniques for detection of microcalcifications in mammography", *International Journal of Pattern Rece. and AI,* vol 7, pp 1417-1436, 1993.

[3] Solka, J.L, et.al. "The detection of micro-calcifications in mammographic images using high dimensional features", *Proceedings of the 1994 IEEE seventh symposium on computer-based medical systems*, pp 139-145, 1994.

[4] Wan Mimi Diyana, et.al. "A comparison of clustered microcalcifications automated detection methods in digital mammogram" *IEEE ICASSP*, pp. II385-388, 2003.

[5] Liyang Wei, et.al. "A study on several machine-learning methods for classification of malignant and benign clustered microcalcifications" *IEEE transactions on medical imaging*, vol. 24, no. 3, pp. 371-380, March 2005.

[6] Ryohei Nakayama, et.al. "computer-aided diagnosis scheme using a filter bank for detection of microcalcification clusters in mammograms", *IEEE transactions on biomedical engineering*, vol. 53, no. 2, pp. 273-283, February 2006.

[7] J.S.Geonimo et.al. "Fractal functions and wavelet expansions based on several scaling functions", *J. Approx. Theory*, vol. 78, pp. 373-401, 1994

[8] C. K. Chui et. al. "A study of orthonormal multiwavelets" *J. Appl. Numer. Math.*, vol. 20, pp. 272-298, 1996

[9] Jerome Lebrun, et. al. "High order balanced multiwavelets: Teory, factorization, and design", *IEEE transactions on signal processing*, vol. 49, no. 9, pp. 1918-1930, September 2001

[10] Images of the breast cancer URL: http://www.cancer.org Retrieved on February 14, 2009.

[11] MATLAB Version6.5, image processing toolbox>functions

[12] Vasily Strela et. al. "The application of multiwavelet filterbanks to image processing", *IEEE transactions on image processing*, vol. 8, no. 4, pp. 548-563, April 1999

[13] D. M. Garge et. Al. "A Low Cost Wavelet based Mammogram Image Processing for Early Detection of Breast Cancer", *submitted to Journal of Indian Science and Technology*, December, 2008

[14] Jian-ao Lian et. al "Balanced multiwavelets with short filters", *IEEE signal processing letters*, vol 11, no. 2, pp 75 – 78, February 2004

[15] Jerome Lebrun, et. al. "Balanced multiwavelets: Teory and design", *IEEE transactions on signal processing*, vol. 46, no. 4, pp. 1119-1125, April 1998

Origin Authentication of Digitally Signed Message Using Joint Signature Scheme in Mobile Commerce

Aihab Khan, Malik.Sikandar Hayat Khiyal, Sara Ayub
m.sikandarhayat@yahoo.com, aihabkhan@yahoo.com, rosaseae@gmail.com

***Abstract*—In this era of advanced technology, mobile commerce has become popular due to rapid growth of communication technology but this requires maintaining secure communication and protection from threats. In this paper, we presented a mechanism for secure and authentic communication in mobile commerce based on joint signature scheme. We formulate this technique for the authentication of message originator who signs the message to buy a product online through its mobile operator. Proposed technique is efficient in mobile domain because it is less computative and can be used with limited resources in mobile commerce. An experimental analysis shows that proposed technique overcomes the major drawbacks of traditional digital signed message, such as computational load, communication load, complexity, public key operations, transaction etc.**

Keywords—Joint signature, M-commerce, Origin Authentication.

1. Introduction

The technology grows faster and faster, much advancement is done in information technology regarding communication, security, privacy etc. A mobile device is a wireless communication tool, including mobile phones, PDAs, wireless tablets, and mobile computers. Mobile commerce (M-commerce) can be defined as any electronic transaction or information interaction conducted using a mobile device and mobile networks, which leads to transfer of real or perceived value in exchange for information, services, or goods. M-commerce offers consumers convenience and flexibility of mobile services anytime and at any place, and is playing an increasingly important role in payments and banking [7].

Mobile communication is one of the prime aspects of telecommunication and this aspect turns into mobile commerce due to rapid growth of internet and digital technology. Security in mobile commerce is vital for its widespread usage. Encryption/decryption techniques, digital signature algorithms and other security measures are being develop to secure the m-commerce channel.

Authentication is a process to identify a mobile user, in order to authorize him/her to use system resources for specified purposes. Authentication involves negotiating secret credentials between prover, and verifier for protecting communications [1].Digital authentication systems become an essential part of electronic payments via public networks. These systems allow people and organizations to electronically certify the authenticity of an electronic document etc. Policies associated with these systems, raise important privacy and protection issues.

Digital signatures are based on certain types of encryption policies to ensure authentication. Encryption is the process of encoding data that one computer is sending to another, into a form that only the other computer will be able to decode [4]. Security is a crucial requirement of an m-commerce system due to the fact that the sensitive financial information that these systems transmit travel over untrusted networks where it is essentially fair game for anyone with local or even remote access to any part of the path followed [5].

Joint signature scheme used in mobile commerce for the secure transactions but it is not costly and computationally low. Joint signature scheme is based on hash functions and encryption/decryption algorithms to produce joint signature with message originator and message signer and also to authenticate the message originator for message signer and vendor (message verifier).This technique is new and not much work is done in this technique yet. Li-Sha HE et al[3] proposed joint signature scheme for the authentication of mobile user, but this technique is not implemented yet and also its results are hypothetical [3]. We have worked out on this technique and implement it for the authentication of mobile user by its network operator and vendor.

This paper is organized as follows. Section 2 elaborates related work and state of the art today. Section 3 provides the frame work overview of the proposed model. Section 4 discusses the technique of the research model. Performance parameters are discussed in Section 5 and Section 6 consist of Conclusion and future work of this research.

In this paper we introduce a joint signature scheme for the authentication of Mobile user in M-commerce. Major contributions are as follows:

- To formulate an algorithm for authentication of the origin of the message sent from a mobile user so as to prevent any fraudulent actions by the vendor or any other entities.

- To develop a model for authentication of the signature of the signer that has sent a message.

- To ensure that the content of the message are authentic and are being sent from the mobile user.

2. Related Work

Joint signature scheme is proposed by Li-Sha HE et al [3] in 2004 ACM Symposium on Applied Computing. This technique overcome the security issues related to m-commerce e.g. authentication, non-repudiation, confidentiality, integrity etc.But this technique was not implemented at that time, so we took this scheme as a base for the authentication of origin of digitally signed message by the mobile user for purchasing goods online. Very few works is previously done for the authentication but techniques which have been used for the authentication have several drawbacks. Also these techniques were based on traditional digital signature scheme like Diffie Helmen which has drawbacks in limited resources of mobile domain.

Server-aided technique proposed by Chin-Ling Chen et al [7] for the mobile commerce uses trusted proxy server to co-ordinate transactions between user and vendor. It is based on the Diffie Helmen scheme and involves the one-time password mechanism to establish session key in advance between user and vendor with the help of trusted proxy server. This technique is divided into two phases; negotiation phase and authentication phase. This technique discussed different aspects of security issues like anonymity due to high communication load involves in negotiation and in authentication phase communication between mobile user and trusted third party.

Another technique proposed by Wooseok Ham et al [6] secure one way payment system in mobile commerce. This technique uses two modular multiplications, one modular inverse and the second is hashing by the user using two public key pairs and keyed hash function for computation. In this technique only unilateral communication is sufficient between user and vendor to complete payment. This technique has three main functions; withdrawal, purchase and deposit. Also user does not need to participate in deposit phase so communication load and computation load is low in this scheme. As more than one transaction is involved so transaction overhead is present in this scheme.

3. Framework Overview

The proposed framework for the authentication of origin in mobile domain using joint signature scheme is shown in figure 1.

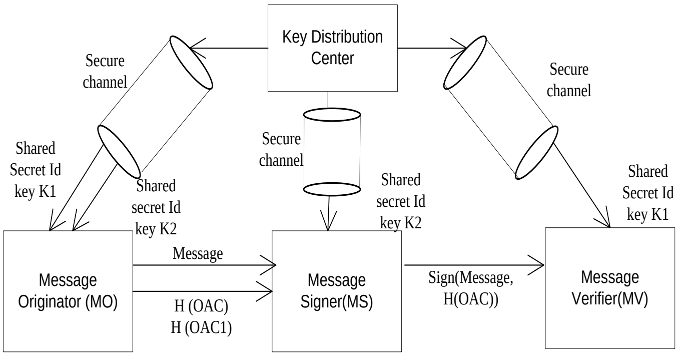

Figure 1: Proposed Abstract model for origin authentication using joint signature scheme

In a proposed model as shown in fig 1, three main entities are illustrated,

- The message originator which is a mobile station (MO).
- Server run by the network operator signed the message in its home environment(MS)
- And service provider which verifies the message and provides different services to the mobile user (MV).

The shared keys are securely distributed between these three entities. The message originator sends a message along with H(OAC) and H(OAC1) to the message signer which sign the message by its private key and send it to the message verifier which later on verifies the message and provide authentication for the message originator.

The notations used in the model are given in table 1

Table 1: Notations

Notation	**Description**
MO	Message Originator
MS	Message Signer
MV	Message Verifier
H(OAC)	Hash of Origin Authentication Code between MO and MV
H(OAC1)	Hash of Origin Authentication Code between MO and MS
Id K1	Secret key shared between MO and MV
Id K2	Secret key shared between MO and MS

A detailed discussion of proposed abstract model for origin authentication using joint signature scheme is given in following section.

The abstract model of figure 1 elaborated by more descriptive model is given below.

The Figure 2 explains as how message originator MO produces the hash functions and sends it to the message signer MS. Hash function H(OAC) and H(OAC1) is produced on key Id K1 and Id K2 respectively, and message but with different keys securely shared between these three entities. Message signer MS signs the message and produces the joint signature after verification of message originator MO. After verification message signer MS encrypts the message and sends it to message verifier MV. Message verifier MV decrypts the message and produces hash function of its own and then after comparing both hash functions provides the authenticity for the message originator MO.

4. Technique

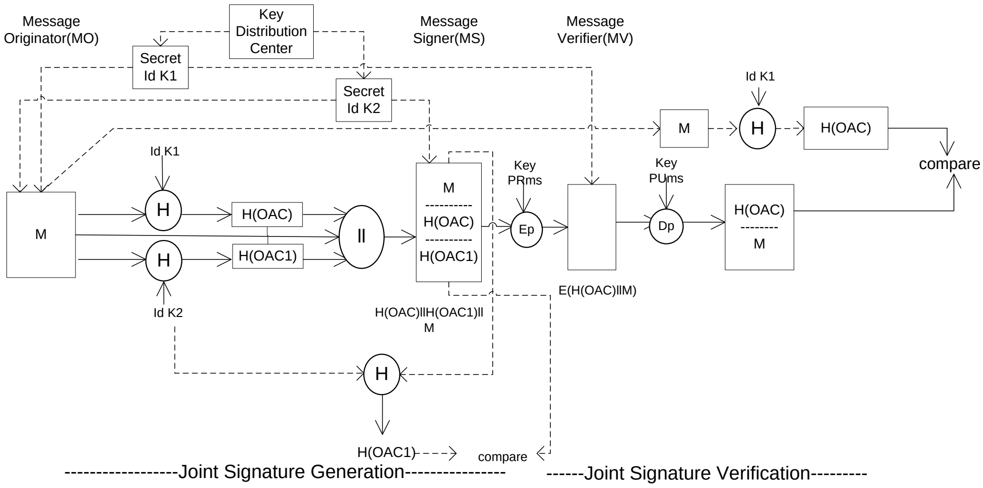

Figure 2: Descriptive model of origin authentication using joint signature scheme

The process of origin authentication using joint signature scheme consist of following four major steps.

Step 1 :(Sharing Secret Key)

The message originator (MO) sends the message and a shared secret key Id K1 to the message verifier (MV) and produces a joint signature on message with the help of message signer (MS) as shown in fig 3.

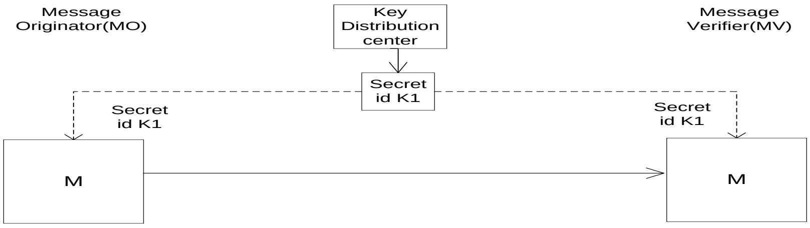

Figure 3: Distribution of secret keys between Message Originator and Message Verifier

Step 2: (Produce Hash Function)
The message originator (MO) sends the message to the message signer (MS) and produces a hash on Origin Authentication Code H(OAC) and Origin Authentication Code 1 H(OAC1) and sends it to the MS with message. Also a Secret key Id K2 is shared between MO and MS. Process is shown in fig 4

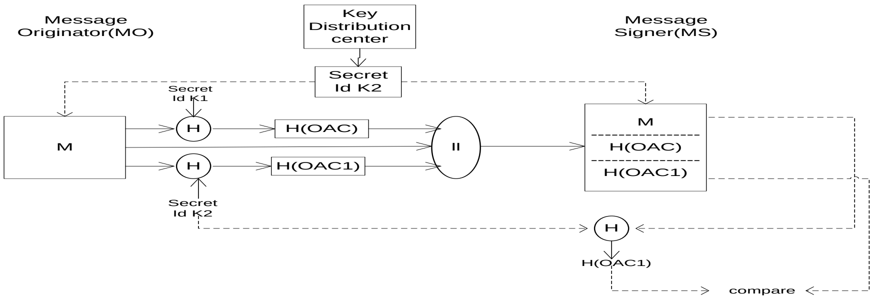

Figure 4: Production of Hash function by Message Originator

The algorithm developed for producing hash function is as follow:

```
Algorithm: Production of Hash function
Input: min, max, plaintext
Output: hash value
1.salt=random.next(min,max)          //min and max are integer values
2.plaintxtbytes=getbytes(plaintxt)
//converting from string to bytes
3.plaintxtwidsalt=plaintxtbytes+salt
//appending salt bytes
4. hash = SHA1 managed()
5.hashbytes= hash.computehash(plaintxtwidsalt)
//calculating hash value
6.hashvalue = convert.tobase64string(hashbytes)
//converting to string
```

Figure 5: Algorithm for producing hash function

Step 3: (Joint Signature Generation)

```
Algorithm: Origin Authentication
Input: hash value
Output: verify hash for origin authentication
1.hashwidsaltbytes=convert.frombase64string(hash value) // converting to bytes
2. if(hashwidsaltbytes.length < hashsizeinbytes) then
3. verify hash = false
4. end if
5. for I = 0 to saltbytes.lendth-1
//saltbytes is a difference between
//length of hashsizebits and hashsizebytes
6.saltbytes(I)= hashwidsaltbytes(hashsizeinbytes)
7. next I
8.expectedhash=computehash(plaintext,saltbytes)
// computing hash values to verify
9. verify hash = (hash value = expectedhash)
// comparing hash values
```

Figure 7: Algorithm for Origin Authentication

The message signer (MS) signed the message using its private key on Hash Origin Authentication Code H(OAC), a Hash Origin Authentication Code 1 H(OAC1) and message generated by the MO and sends it to the MV as shown in fig 6.

Step 4 :(Origin Authentication)
The message Verifier (MV) decrypts the message received from MS by public key of MS and verifies the origin of the message by H (OAC) with the help of message and shared secret key Id K1. And MS verifies the H (OAC1) with the help of secret key Id K2 shared between MO and MS.
The algorithm for the authentication of origin is shown in Figure 7

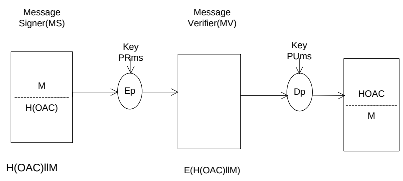

Figure 6: Joint signature generation by

The above steps can also be elaborated sequentially by using sequence diagram in fig 8 as:

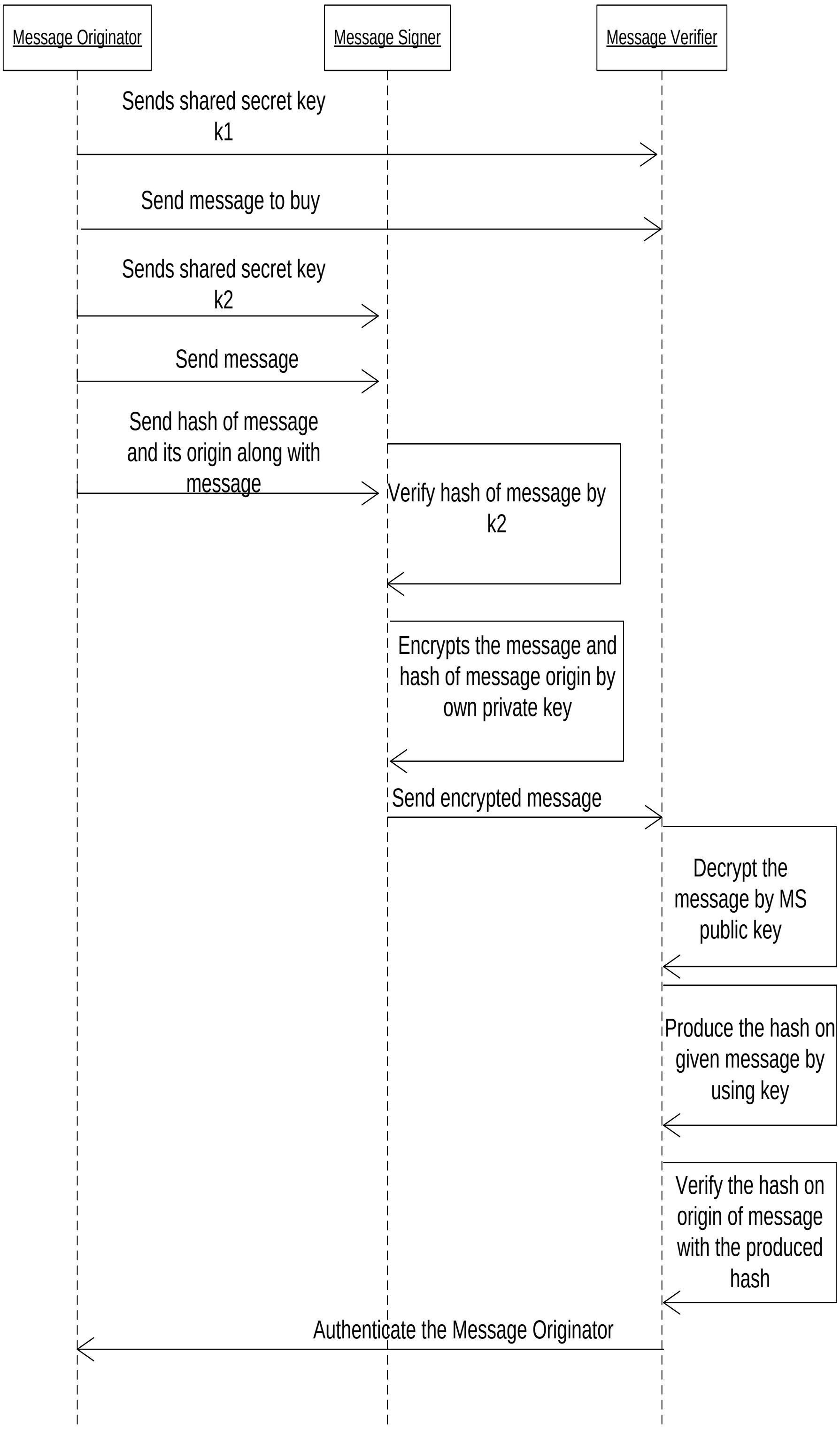
Message Originator
Message Signer
Message Verifier
Sends shared secret key k1
Send message to buy
Sends shared secret key k2
Send message
Send hash of message and its origin along with message
Verify hash of message by k2
Encrypts the message and hash of message origin by own private key
Send encrypted message
Decrypt the message by MS public key
Produce the hash on given message by using key
Verify the hash on origin of message with the produced hash
Authenticate the Message Originator

Figure 8: Sequence Diagram of working of model for Joint signature Origin Authentication

5. Performance Results

Performance of proposed technique is analyzed on parameters like computational load, communication load, complexity, public key operations, transactions with respect to other techniques and following observations were made.

Table 2: Performance measure of proposed Technique

	Joint Signature Scheme (Proposed Scheme)	Server Aided Signature Scheme	Secure one way mobile payment Scheme
Computational Load	In this scheme two hash function and one public key operation is used in computation which is very efficient in limited resources so computational load is Low in this scheme	Proxy server or trusted third party is involved in this scheme which performs complex operations, based on traditional digital signature scheme like Diffi Helmen which bears more computational cost in limited resources so computational load is High in this scheme.	One modular inverse, two modular multiplications and two hash functions are involved in computation which can effectively be implemented in mobile domain with limited resources. Also no exponentiation calculations are involved that are used in RSA and a Diffi Helmen technique, so computational load is Low.
Communication Load	In this scheme only one transaction is done from customer to the network operator so communication load is Low in this scheme.	Two way Communications are involved in negotiation phase and in authentication phase so more than one transaction is involved in this scheme so communication load is High in this scheme.	In this scheme customer does not need to be involved in deposit phase, so unilateral communication is done between customer and vendor to complete payment transaction. So communication load is Low in this scheme
Complexity	In this scheme only one public key operation is performed at service provider to verify the joint signature by network operator so public key operation is Low in this scheme.	Two public key operations are involved in this scheme, one to verify secret from original signer by public key of trusted third party and second to verify signature by public key of signature signer. So public key operations in this scheme is High.	In this scheme customer has two private and public key pairs for signing and verification. So two public key operations are involved in this scheme, so public key operation is High in this scheme.
Transactions	In this scheme only one transaction is required from customer to network operator so transaction in this scheme is Low	In this scheme two transactions are required between original signer and signature signer in negotiation and authentication phase so transaction in this scheme is High.	In this scheme more than one transaction is required in withdrawal, purchase and deposit phase so transaction in this scheme is High.

Experimental analysis shows that joint signature is much efficient and less complex than others schemes with low computation and communication load is which is very useful in mobile commerce as in mobile commerce resources are very limited as compare to other domains like banking, online purchasing etc, so joint signature scheme is efficient and can be used in mobile commerce for origin or client authentication. The comparison is shown in table 3.

Table 3: Comparison Analysis

Techniques	Computational Load	Communication Load	Public key operations	Complexity	Transactions
Joint Signature scheme	Low	Low	Low	Low	Low
Server-aided Signature Scheme	High	High	High	High	High
Secure One-way Mobile Payment	Low	Low	High	Low	High
Proposed Scheme	Low	Low	Low	Low	Low

6. Conclusion And Future Work

In this paper, we have presented a novel joint signature scheme for the authentication of origin of message that is digitally signed by the mobile user (message originator) with the help of its network operator(message signer),both jointly produce the signature which is going to be verified by the vendor(message verifier).Authentication is done on both entities i.e. message signer and message verifier which proved them that the message originator is the right person who sends message to vendor. Furthermore this technique is more efficient than other traditional schemes which are used for authentication in mobile commerce. In comparison with existing techniques mainly server aided scheme and secure one way mobile payment mechanism, this technique overcomes all major disadvantages of existing techniques.
In future, it is recommended to extend joint signature scheme for the authentication of message that is digitally signed by the user in order to avoid any fraud over the transmission line. Moreover this technique can be implemented for other security issues like confidentiality, integrity, non-repudiation etc.

References

[1] Babu.S.B, Venkataram.P, 2009, "**A Dynamic Authentication Scheme for Mobile Transactions",** Protocol Engineering Technology (PET) Unit, Department of Electrical Communication Engineering Indian Institute of Science, Bangalore, 560 012, India (Email: *f*bsb, pallapa*g*@ece.iisc.ernet.in) International Journal of Network Security, Vol.8, No.1, PP.59-74, Jan. 2009

[2] Chen C-L, Chen C-L**,** Liu L-C, Horang.G, 2007, **"A Server-aided Signature Scheme for Mobile Commerce",** Department of Computer Science and Information Engineering, Chaoyang University Technology,Taichung,Taiwan.clc@mail.cyut.edu.tw, Department of Mechatronics Engineering, National Changhua University of Education Changhua, Taiwan 500, ROC. d95631003@mail.ncue.edu.tw, Department of Computer Science, National Chung Hsing University , Taichung, Taiwan 402, ROC.0287@sun.epa.gov.tw, , Department of Computer Science, National Chung Hsing University , Taichung, Taiwan 402, ROC. gbhorng@cs.nchu.edu.tw. *IWCMC'07*, August 12-16, 2007, Honolulu, Hawaii, USA.

[3] He L.S, Zhang.N,(2004), **"A New Signature Scheme: Joint-Signature"**, Department of Computer Science the University of Manchester, Manchester UK, 0044-161-2756270 {hel, nzhang}@cs.man..ac.uk, SAC'2004, March 14-17, 2004, Nicosia, Cyprus.

[4] Kadhiwal.S, Usman.M.A, 2007, "**Analysis of mobile payment security measures and different standards"**, Shaheed Zulfiquar Ali Bhutto Institute of Science and Technology, Karachi, Pakistan.

[5] Kritzinger.F, Truter.D,(2003) , "**A Secure End-to-End System for M Commerce: Research Paper CS03-24-00",** October 12, 2003.

[6] Ham.W, Choi.H, Xie.Y, Lee,M, Kim.K, **'Secure One-way Mobile Payment System Keeping Low Computation in Mobile Devices',** International Research center for Information Security (IRIS) Information and Communications University (ICU) 58-4 Hwaam-dong, Yusong-gu, Daejeon, 305-732, S. Korea, School of management Information and Communications University (ICU).

[7] Nambiar.S, Lu.C-T, Liang.L.R, 2008 "**Analysis of Payment Transaction Security in Mobile Commerce'**, Department of Computer Science Virginia Polytechnic Institute and State University 7054 Haycock Road, Falls Church, VA 22043 {snambiar, ctlu}@vt.edu, Department of Computer Science University of the District of Columbia Washigton, DC 2008, lliang@udc.edu.

Non Repudiation in M- Commerce Using Joint Signature Scheme

Aihab Khan, Malik Sikandar Hayat Khiyal, Madiha Tariq
aihabkhan@yahoo.com, m.sikandarhayat@yahoo.com

***Abstract*—Being the hottest issue of today's time there as a lot of work to be done on mobile commerce .in mobile commerce mobile is used to avail a lot of services. One of these services includes online purchasing of different items. Mobile subscribers can by items anywhere at any time by using their mobile. The bills are compensated by their network operators. Different security issues are involved during such transactions. One of the issues that of non-repudiation. This service prevents the sender and receiver to deny their participation in the transaction and to ensure the integrity of the message. This paper represents the mechanism for non-repudiation in m-commerce using joint signatures. This mechanism is based on the use of hash functions and traditional digital signatures where network operators have trusted third party or an arbitrator to satisfy this requirement. This mechanism is efficient to be used in mobile domain having less resource due to low computation and communication load. Also it is simpler than traditional digital signature scheme. We formulate this approach to overcome the problem of non-repudiation in mobile domain.**

***Keywords*—Authentication, Joint Signatures, Mobile commerce, Non-repudiation.**

1. Introduction

Internet is used to share information along different channel. This information is shared along multiple channels through internet protocol security (TCP/IP).Network security consists of several provisions in computer network infrastructure, policies to protect their network from illegitimate user and continuous monitoring of network.

1.1 M-Commerce verses E-Commerce

M-commerce is unique from e-commerce having a show function. There are some similarities between m-commerce and e-commerce but as a whole m-commerce is different from e-commerce.

"Mobile commerce is any transaction, involving the transfer of ownership or rights to use goods and services, which is in initiated and/or completed by using mobile access to computer-mediated networks with the help of an electronic device."

When data is travelling over the network it needs to be protected. A lot of security features should be incorporated for the secure m-commerce for security reasons a lot of techniques like digital signatures, hash functions, encryption etc. are used. Digital signature is a type of asymmetric cryptography. It helps the receiver to make sure that message is send from legitimate users.

1.2 Digital Signatures in m-communication

Existing digital signature schemes are costly to be used in m-commerce. Digital signature generation is most time and resource consuming operation to be performed by mobile devices. Different asymmetrical payment methods have been developed for mobile users to buy goods online. These methods require less resource to perform the transactions but there is a major problem with these approaches that network operator may abuse the trusts. Therefore these approaches must be outfitted with a strong security level so that everyone involved in the transactions should be accountable. As digital signature generation is computationally expensive for a mobile device, which has considerably less computing resources then a desktop, so another scheme may b used i.e. joint signature scheme [7].The model presented in this paper is derived from the research work of Li-Sha HE et al that was presented in ACM Symposium on Applied Computing in 2004.in there research they have presented a model for implementing joint signature schemes in m-commerce. Here three entities are involved. The originator generates the message and applies hash on message with shared secret id key K1 and K2 and sends the message along with two hash values (joint signatures) to the signer. The signer signs the joint signature with its private key and sends this signed joint signature to the verifier where verifier decrypts to authenticate the origin this model is a hypothetical model that is not implemented. Our research is based on the implementation of this model along with addition of some security services may have developed a mechanism for implementing non-repudiation of both sender and receiver in m-commerce using signature scheme and incorporated our mechanism to their hypothetical model and also implemented there model. This research is intended for implementing non-repudiation in m-commerce using joint scheme. Objective of this research is to develop a mechanism for non-repudiation in m-commerce scheme. This mechanism caters the prevention of denial from sender and receiver about their participation in the transactions and ensures the integrity of the message. The proposed mechanism is applicable in mobile domain with limited resources. The reminder of this paper is organized as .In section 2 named as 'Related Work' brief discussion of different signature scheme is represented. In the section 3 'Proposed Framework Model'. Our proposed model is described. The explanation of our proposed model is given in section 4 'Technical Description of Proposed Model'. In the section 5 'Performance Results' the performance of our proposed mechanism is discussed. Section 6 as conclusion is followed by the 'Future Work'

2. Related Work

In this section we introduce three important signature schemes proposed by Li Sha HE et al [1], Ching-ling Chen et al[2] and Guilin Wang et al[3].Joint signature scheme [1] is an extension of digital signature scheme as this scheme is based on the use of hash functions and traditional digital signatures. In joint signature scheme there is no concept of proxy signer and only one public key operation is involved so there is less communication and computational overhead. In mobile domain there are limited resources so this scheme is efficient to be used in mobile domain. Digital signature scheme is used where there is large number of resources hence on mobile domain with limited resources using digital signature scheme is not that much efficient. Server aided signature scheme [2] involves hash functions and traditional digital signature scheme. Here signature server is required, signature server and original signer require a round trip-communication. Signature server verifies the signature on received public key. In this technique there is a computation and communication overhead for signature generation. Hence time required to generate a signature is increased. Due to all these reasons this technique is not efficient to be used in mobile domain. In proxy signature scheme [3] the proxy signer is introduce to produce a digital signature on behalf of the original signer. Proxy signature scheme has three categories named as full delegation, partial delegation and delegation by warrant. In full delegation the proxy signer signs the message with original signer keys, in partial delegation new proxy key is generated from the original key by the original signer and sent to the proxy signer. Proxy signer then uses this proxy key for purpose of signature generation. In delegation by warrant there is higher processing overhead as original signer has to sign certificate with its private key. This scheme also has higher processing overhead and high communication and computation load. In this paper we introduce several security services as authentication, message integrity, and non- repudiation in m-commerce to a scheme named as joint signature scheme. Other security services like confidentiality etc can also be implemented using this scheme.

3. Proposed Framework Model

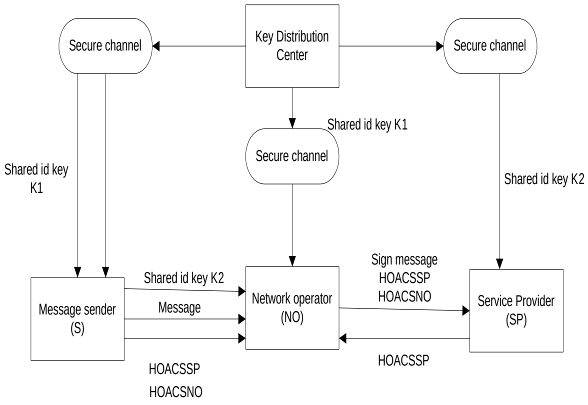

Figure 1: Framework Model

The proposed framework model shown in fig 1 explains that key distribution center distributes the key with the message sender(S), network operator (NO) and the service provider(SP).message sender(MS) sends a message, compute hash of it by using shared key and send it to NO.NO signs the message, verifies it, and send it to SP.SP then verifies that non repudiation is not occurring by using its shared key.

Description of the terms involved in proposed model are given below:

Table 1 Notations

S	Message sender
NO	Network operator
SP	Service provider
M	Message being sent by the message sender
K1	Shared id key between message sender and network operator
K2	Shared id key between message sender and service provider
H	Used for hash function
||	Sign of concatenation
PRNO	Private key of network operator
PUNO	Public key of network operator
HOACSSP	Hash origin authentication code between sender and service provider
HOACSNO	Hash origin authentication code between sender and network operator
EP	Public key encryption
DP	Public key decryption

4. Technical Description of Proposed Model

Technical description of the proposed model Is given below:

Step 1:

The message sender(S) sends the message to service provider (SP) and produce a joint signature on message with the help of network operator. (NO)

Step 2:

The network operator (NO) signs the message using its private key on hash origin authentication code between sender and service provider HOACSSP, a hash origin=n authentication code between sender and network operator (HOACSNO) and message, NO will also verify the hash function in order to verify that the message is actually sent from the legitimate sender i.e. origin authentication. Also it verifies HOACSNO for the sake of message integrity and origin authentication. Once the origin is authenticated it cannot deny its participation in the transaction. It is done for the non-repudiation of the origin.

Step 3:

The service provider **(**SP) decrypts the message

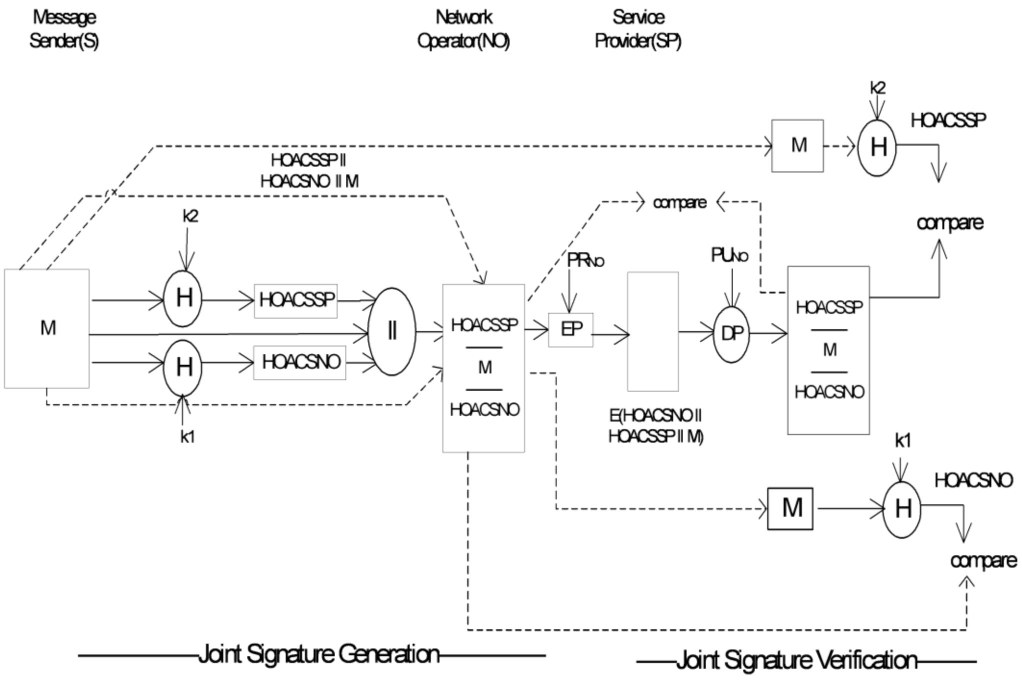

Figure 2 : Proposed Model

using NO's public key to authenticate the network operator. Network operator cannot deny its participation in the transaction. Also it verifies the message for the message integrity by comparing the message from NO to the message sent by the sender. SP will also verify hash function in order to verify that the message is actually sent from the legitimate sender .i.e. origin authentication.

Step 4:

The service provider (SP) after receiving HOACSSP from the network operator (NO) will send it back to the NO in order to get authenticated by the network operator. Once the SP is authenticated it cannot deny its participation in the transaction. It is done for the non-repudiation of the receiver.

In the above shown fig 2, message sender (MS) sends a message, compute hash by using keys, and then concatenated message to these is send to NO. Till here joint signature is generated. Then NO encrypts

This concatenated message by using its private key. At SP end this encrypted message along with hash is decrypted by using public key of No. At SP end the original message and hashes i.e HOACSNO and HOACSSP is compared to verify non repudiation

Step 1 (sharing secret key)

Key distribution center distributes the secret shared id key K1 and secret shared key K2 among the message sender (S),network operator(NO) and the service provider.K1 and K2 are sent to the message sender through a secure channel also K1 is sent to the NO and K2 is sent to the SP through secure channel by key distribution center. This is shown in fig 3.

Step 2 (Message Generation)

Message sender generates the message and sends this message to the service provider (SP) as well as network operator (NO).

Step 3 (Production of hash on Message)

The message sender (S) generates message and produces HOACSNO, Hash Origin Authentication code between the sender and network operator and HOACSSP. Hash origin authentication code between sender and service provider with the help of shared secret key K1 and K2 respectively on message and sends both HOACSSP and HOACSNO to the network operator (NO) as shown in fig 4.

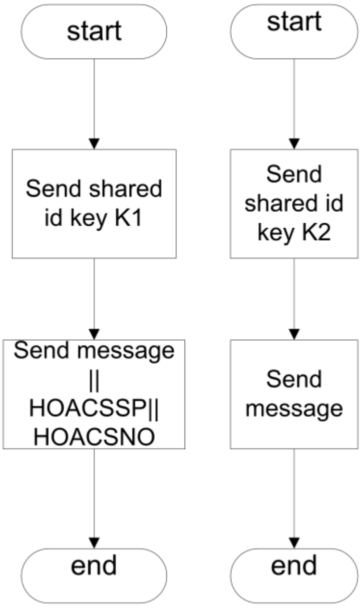

Figure 3

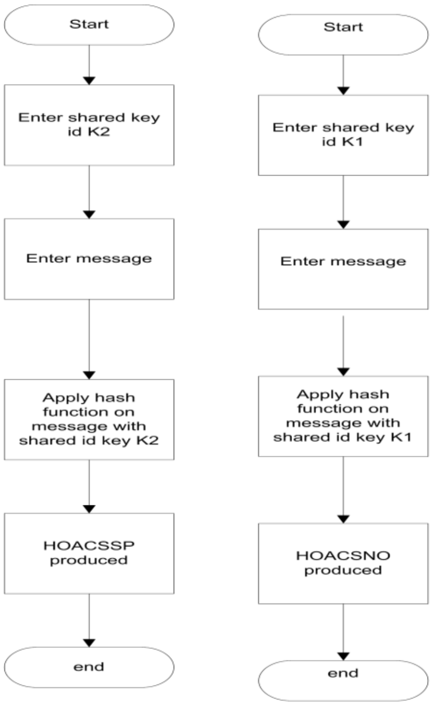

Figure 4

Step 4 (Joint Signature Generation)

The network operator (NO) signs the message using its private key on HOACSSP, HOACSNO and message generated by the S and sends it to the Service provider (SP).this shown in fig 5.

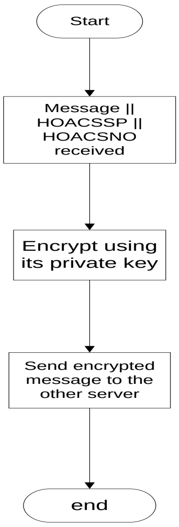
Start
Message \|\| HOACSSP \|\| HOACSNO received
Encrypt using its private key
Send encrypted message to the other server
end

Figure 5

Step 5(Authentication)

The service provider (SP) decrypts the message received from NO by public key of NO and verifies the origin of the message by HOACSSP with the help of message and shared secret id key K1.this is done on order to cater the non-repudiation of origin. NO verifies the HOACSNO with the help of shared secret id key K2 between S and NO as shown in fig 6.

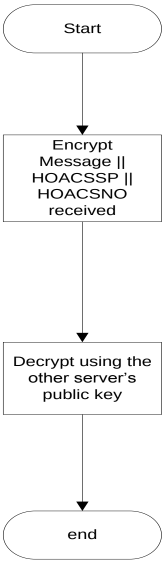
Start
Encrypt Message \|\| HOACSSP \|\| HOACSNO received
Decrypt using the other server's public key
end

Figure 6

Step 6(Non-Repudiation)

The service provider (SP) when decrypts the message that is sent from NO gets HOACSSP.SP sends this HOACSSP back to the NO for the purpose of its authentication. This is a concept on hand shaking which is implemented in order to cater the non-repudiation of receiver. This is shown in fig 7.

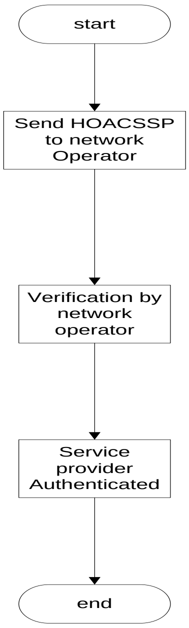
start
Send HOACSSP to network Operator
Verification by network operator
Service provider Authenticated
end

Figure 7

5. Performance Results

The results demonstrate that joint signatures cam be efficiently used in m–commerce.

Computational load

In proposed scheme two hash functions are used for computation, and hash function can easily implement in mobile domain with limited resources so in proposed scheme computational load is low.

Communication Load

In propose scheme only one transaction is required from message originator to message signer for producing joint signature so in proposed scheme communication load is low.

Public key operations

In proposed scheme only one public key operation is required by message verifier to verify the joint signature from message signer. So in proposed scheme public key operation is low.

Complexity

In proposed scheme trusted third party is no involved (NO is behaving as a trusted third party) in communication so proposed scheme is less complex than other schemes.

Transactions

In proposed scheme one transaction is done between message originator and message signer for producing joint signature scheme so in proposed scheme transaction overhead is low. Thus joint signature scheme is much efficient and less complex than other scheme, in joint signature scheme computation and communication load is low which very useful in mobile commerce as resources are limited in mobile domain as compare to other domains like banking, online purchasing etc, so joint signature scheme is easy and effective and can be used in mobile commerce for authentication non-repudiation and message integrity.

6. Conclusion and Future Work

In this paper we have presented a mechanism for non-repudiation in m-commerce using joint signature scheme. In situations where there is not complete trust between sender and receiver something more than authentication is needed. Basically it is the need of non-repudiation. The mechanism that we have presented is a type of arbitrated digital signature. Our mechanism gives an efficient solution to the problem of repudiation. In order to make the transactions securer inclusion of this feature is very important. The reason due to which we selected joint signatures for implementing non-repudiation in m-commerce is that in mobile domain we have limited resources. Joint signature scheme best fits in the domain having fewer resources. Also this scheme is more efficient than the existing scheme as it involve less public key operations and transactions. Due to this reason the scheme is simpler and less expensive. For future we've planned to work on other security issues like confidentiality etc. to incorporate in this scheme.

References

[1] Li-Sha He, Ning Zhang, **"An Asymmetric Authentication Protocol for M-Commerce Applications,"** Eighth IEEE Symposium on Computers and Communications, ISCC, pp.244, 2003

[2]Ching Ling Chen et al **'A Server-aided Signature Scheme for mobile commerce'**, Department of Computer Science and Information Engineering, Chaoyang University of Technology,Taichung,2007,Taiwan.clc@mail.cyut.edu.tw

[3]Guilin Wang et al **'Proxy Signature Scheme with Multiple Original Signer for Wireless E-Commerce Applications'**, Infocomm Security Department, Institute for Infocomm Research (I2R),2004

[4]Chung et al **'Adaptation of proxy certificates to non-repudiation protocol of agent-based mobile payment systems'**, Springer Science Business Media, LLC 2007

[5]Chin et al **'A fair and secure mobile agent environment based on blind signature and proxy host'**, Department on Computer Science and Information Management, Providence University, Department of Computer Science and Information Engineering National Chung Cheng University,2004

[6] Jonker **'M-commerce and M-payment combining technologies',** 2003

[7] http://en.wikipedia.org/wiki/Mobile_commerce

International Journal of Latest Trends in Networks & Communication

Call for Paper

The journal welcomes high quality original research papers, survey paper, review paper, tutorial, technical notes as well as the discussion papers.

Communication QoS and Performance Modeling

Multimedia Processing and Communications

BAN, PAN, LAN, MAN, WAN, Internet, Network Interconnections

Biologically inspired communication

Bluetooth, IrDA, RFID, WLAN, WMAX, 3G

Broadband and Very High Rate Networks

Cognitive Radio Systems

Communication and Information Theory

Cooperative Communications and Networking

Cross-layer Design and Optimization

Data Networks and Telephone Networks

Emerging Communication Technology and Standards

Fault tolerance, dependability, reliability, and localization of fault

Formal Methods in Communication Protocols

Information, Communications and Network Security

Internet Services, Systems and Applications

Multimedia Communications

Multimedia networks

Network Architecture and Design

Network Technologies, Services and Applications

Next Generation Mobile Networks

Next Generation Networks

Optical Systems and Networks

Parallel and Distributed Computing

Pervasive Computing and Grid Networking

Satellite and Space Communications

Signal Processing for Communications

Wireless Ad Hoc and Sensor Networks

Wireless Communications & Networking

Wireless Telemedicine and E-Health