AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Enhancing Secure Transaction and Identity Authentication Method Based on Mixed Fingerprint, Hmac Techniques and Qr-code in m-commerce

[1]DR.B.Vanathi, [2]K.Shanmugam, [3]DR.V.Rhymend Uthairaj

[1]Department of Computer Science, Chennai, Tamil Nadu, India,
[2]Department of Computer Science, Chennai, Tamil Nadu, India,
[3]Department of Computer Science, Chennai, Tamil Nadu, India

ARTICLE INFO

Article history:
Received 19 September 2014
Received in revised form
19 November 2014
Accepted 22 December 2014
Available online 2 January 2015

Keywords:
M-commerce, Quick Response code, AES algorithm

ABSTRACT

The current trend states mobile applications are essential for human personal and professional level. M-commerce will be next generation of wired e-commerce applications. M-commerce with the help of wireless environment leads to large number of user acquisition. For sure M-commerce will play major role in the internet industry invoking m-payments, m-booking, m-transactions. In m-commerce applications authentication is very vital. Biometric authentication is a unique authentication by using measurements of the human body and behavioral characteristics of the unique person. Biometrically secured mobile commerce system is much safe and secure and very easy to use, also no need to remember passwords and secret codes. Existing system use the idea of m-payment services in handheld devices using user name and passwords. Biometric authentication is used for accessing the handheld device and not for accessing applications. Our proposed system focus on analyzing multiple fingerprint algorithm and security. More security is proposed by implementing two different fingerprints at the image level in order to generate a new fingerprint. In this paper we propose two fingerprint algorithms ridge and minutiae matching algorithms. Finally the threshold level is found out by using fuzzy logic. Our architecture can also be applied to joint account holders. Also our proposed system includes embedding the fingerprint image using QR code and encrypting using AES algorithm. Data integrity is provided by shared secret key between the user and service provider. Quick Response (QR) code is used to send the customer and product details from the user to the server. The details are encrypted by using AES algorithm.

To Cite This Article: DR.B.Vanathi, K.Shanmugam, DR.V.Rhymend Uthairaj., Enhancing Secure Transaction and Identity Authentication Method Based on Mixed Fingerprint, Hmac Techniques and Qr-code in m-commerce. ***Aust. J. Basic & Appl. Sci.,*** *9(1): 149-164, 2014*

INTRODUCTION

The enormous potential of mobile commerce is the current trend meaning retail outlet in your customers pocket (2010) and (www.\\htttp.Wikipedia.com). M-commerce applications can be used anytime, anywhere by the user for m-payments and transactions (www.\\htttp.Wikipedia.com; Mehata K.M., 2011). Hence m-commerce has become the research hot spot and dramatic growth is emerging among the users (boston consulting group 2010; Mehata K.M., 2011; Vesselin Tzvetkov Arcor, A.G. and Co.K¨olner Strasse).The requirement of mobile commerce security is focused on confidentiality, authentication, integrity, authorization, availability, and nonrepudiation must be rigorously enforced (Vesselin Tzvetkov Arcor, A.G. and Co.K¨olner Strasse; Wen-Chen Hu, Jyh-haw Yeh,). Mobile commerce holistic approach is as shown in figure 1.

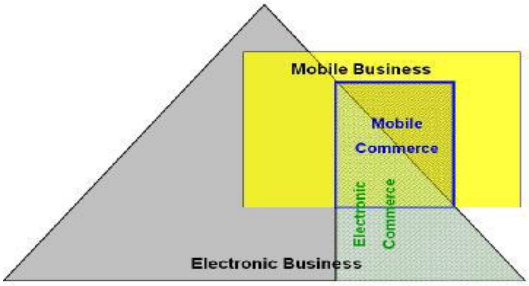


Fig. 1: A Holistic Perspective of M-Commerce (By Rajnish Tiwari1)

Corresponding Author: DR.B.Vanathi, Department of Computer Science, Chennai – 600025, Tamil Nadu, India

Hand held devices these days involve finger print, face recognition interface for authentication, transaction and accessing mobile banking services (Wan, S., *et al*., ; Mangala Belkhede, *et al*., 2012; Chang-Lung Tsai Chun-Jung Chen, 2012). Authentication of biometric is a unique identification of a person by using physical/behavioral characteristics of biometric classification (Hisham Al-Assam, *et al*., 2011; Nirav Jobanputra, ; Harini Jagadeesan,) show in figure 1(a).

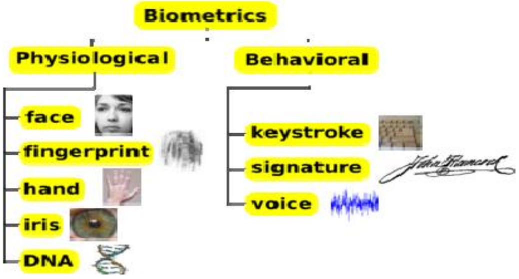


Fig. 1(a): Biometric classification (Hisham Al-Assam, *et al*., 2011; Nirav Jobanputra, ; Harini Jagadeesan, Junta Doi, Member, IEEE, 2005)

Password based authentication is widely used in mobile commerce. But it is not secure in password based authentication and possible to forget the password (Chang-Lung Tsai Chun-Jung Chen, 2012; Karthik Nandakumar, *et al*., 2007). This leads to a biometric authentication. Need for biometric authentication are practically impossible to forget and cannot be forgotten or stolen, borrowed (Mangala Belkhede, *et al*., 2012; Chang-Lung Tsai Chun-Jung Chen, 2012; Muzhir Shaban Al-Ani, 2013). User identification is very important and major issues in wireless services. Fingerprint authentication is widely used for user authentication process and unique finger print to each person (Lin Hong, *et al*., 1998; Sheng Li, *et al*., 2013; Muzhir Shaban Al-Ani, 2013). Finger verification and identification are two modes of fingerprint recognition. Finger Identification involves, finger image captured by mobile and acquired finger image compared by all users in database. Fingerprint verification is to verify the claimed identity of one person by using comparison with only those templates corresponding his finger print (Muzhir Shaban Al-Ani, 2013; Ravi Kumar1, L.,). Finger print is combining the ridges, furrows and minutiae points. Minutiae characteristics, are all composed by ridge terminations and ridge bifurcation. (Muzhir Shaban Al-Ani, 2013; Ravi Kumar1, L.,). The three main basic patterns of fingerprint ridges are the arch, loop, and whorl (Muzhir Shaban Al-Ani, 2013; Damien Dessimoz Jonas Richiardi,) as shown in figure 2:

- Arch: The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.
- Loop: The ridges enter from one side of a finger, form a curve, and then exit on that same side.
- Whorl: Ridges form circularly around a central point on the finger.

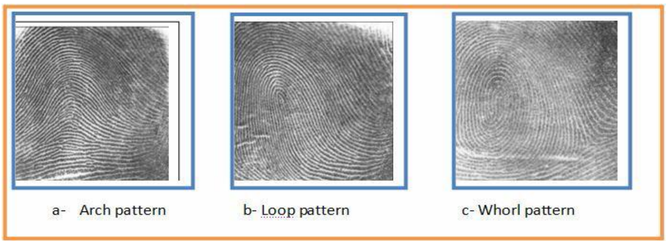


Fig. 2: Fingerprint patterns (Muzhir Shaban Al-Ani, 2013; Damien Dessimoz Jonas Richiardi,)

Two kinds of minutiae are adopted in matching: ridge ending and ridge bifurcation. For each minutia usually extract three features: type, the coordinates and the orientation. Figure 3 represents the, Where ɵ is the orientation and (x_0,y_0) is the coordinate of minutiae (Ravi Kumar1, L.,; Damien Dessimoz Jonas Richiardi; Hamzeh Khazaei, Ali Mohades, 2007; Naser Zaeri).

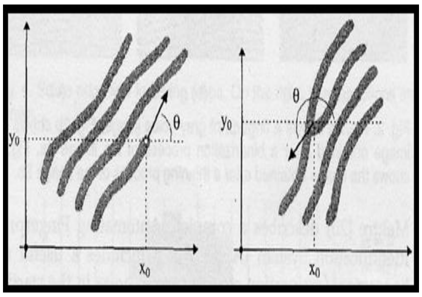


Fig. 3: Two types of minutiae, ridge ending and ridge bifurcation with their orientations (Hamzeh Khazaei, Ali Mohades, 2007; Naser Zaeri,)

A minutia type consists of termination and bifurcation (Lin Hong, *et al*., 1998; Hamzeh Khazaei, Ali Mohades, 2007; Naser Zaeri,). These two are more significant and lot of usage. Termination is an immediate ending of ridge. Bifurcation is the point on the ridge from which two branches derive (Ravi Kumar1, L.,; Damien Dessimoz Jonas Richiardi; Hamzeh Khazaei, Ali Mohades, 2007; Naser Zaeri,). An excellent quality fingerprint typically contains about 40–100 minutiae (Lin Hong, *et al*., 1998).

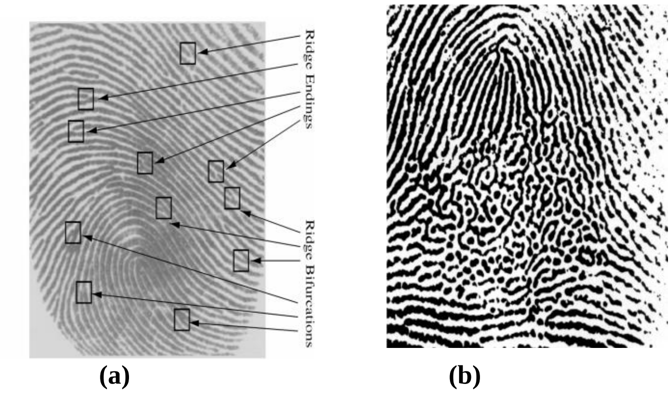


Fig. 4: (a) Minutiae overlaid on a fingerprint image (Lin Hong, *et al*., 1998) (b) Fingerprint images of poor Quality (Lin Hong, *et al*., 1998)

Poor quality of the fingerprint images shown in figure 4(b), in which ridge structures are completely corrupted ((Lin Hong, *et al*., 1998)).

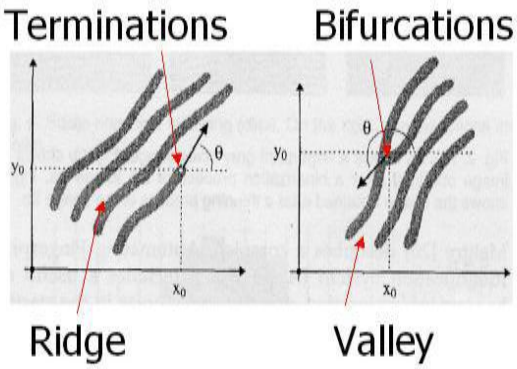


Fig. 5: Minutia types (Ravi Kumar1, L.,; Damien Dessimoz Jonas Richiardi)

A fingerprint can be described in three levels of features (Ravi Kumar1, L.,; Damien Dessimoz Jonas Richiardi). The first level concerns the general flow of the ridges. In a fingerprint, a core and up to two deltas can be generally observed (Naser Zaeri,). They are also considered as level1 features.

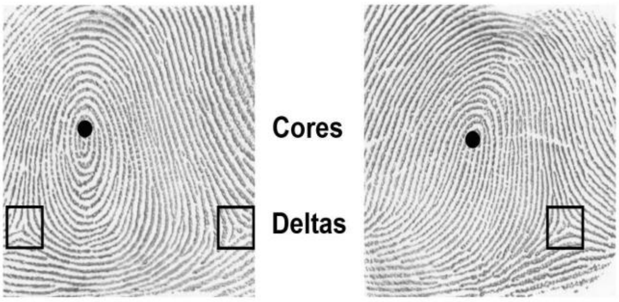


Fig. 6: Cores and Delta (Damien Dessimoz Jonas Richiardi; Naser Zaeri)

When the number and the position of these focal points (delta(s), core,. . .) change, the general ridge flow shape can differ (Damien Dessimoz Jonas Richiardi). The general shape can thus be classified (among other methods) according to the number and positions of the deltas and the position of the core. The different shapes can be classified as: left and right loop, whorl, arch and tented arch shown in figure 7.

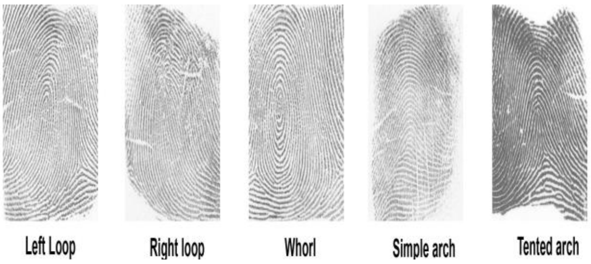


Fig. 7: General Shapes of Fingerprints (Ravi Kumar1, L.,; Damien Dessimoz Jonas Richiardi; Naser Zaeri)

Minutiae characteristics (Sheng Li, *et al*., 2013; Muzhir Shaban Al-Ani, 2013; Ravi Kumar1, L.,; Damien Dessimoz Jonas Richiardi) show in figure 7, which are all composed by ridge terminations and ridge bifurcations. Other characteristics such as wrinkles, creases and warts (Ravi Kumar1, L.,; Damien Dessimoz Jonas Richiardi; Hamzeh Khazaei, Ali Mohades, 2007).

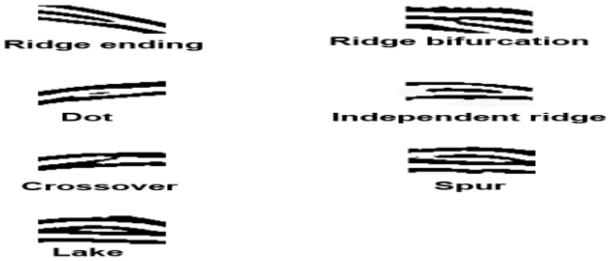


Fig. 8: Minutiae observed on finger print (Sheng Li, *et al*., 2013; Muzhir Shaban Al-Ani, 2013; Ravi Kumar1, L.,; Damien Dessimoz Jonas Richiardi; Naser Zaeri)

The general use of fingerprint recognition systems in various applications has caused concerns that compromised fingerprint templates may be used to make fake fingers, which could then be used to mislead all fingerprint systems the same person is enrolled in. Once compromised, the grayscale image (figure 9 [a]) is the most at risk (Naser Zaeri). Leakage of a phase image (figure 9: [b]) or skeleton image (figure 9: [c]) is also dangerous since it is a trivial problem to reconstruct a grayscale fingerprint image from the phase image or the skeleton image (Naser Zaeri). In contrast to the above three representations, leakage of minutiae templates has been considered to be less serious as it is not trivial to reconstruct a grayscale image from the minutiae image (figure 8: [d]) (Naser Zaeri).

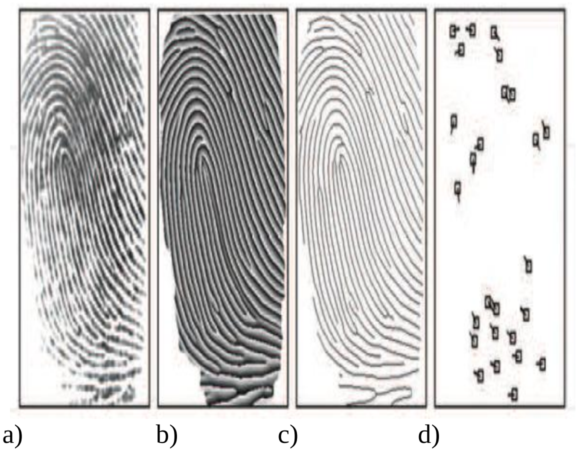


Fig. 9: Fingerprint Representation Schemes (Naser Zaeri)

II. Related Work:

a) Survey of the Paper:

Wan S. Yi, *et al*, proposed the fingerprint user authentication in mobile commerce. This proposed system provides the high risk of loss, high authentication factor and low computation time. Disadvantages of this system consists of not focused on the finger print matching threshold level ,finger print minutiae matching and pattern matching algorithm is not concerned. Finger print image is send to the biometric server. The way in which to found the user is authenticated person? What the solution of poor image finger print quality? and how to analyze the user fingerprint image? are not focused and do not provide solution to these question in this paper. Mangala Belkhede,*et al* (2012) proposed the online transaction by using fingerprint mechanism on android system. An advantage of in this Proposed System focused on the finger print image is how to analyze? That means fingerprint image is analyzed by using fuzzy logic at the server side but not focused on the threshold level(100%,60-99% or below 60%).Chang-Lung Tsai Chun-jung chen,Deng-jie Zhuang (2012) proposed the Onetime password(OTP) and unique biometric based finger authentication for mobile banking in mobile commerce. Disadvantages of this system do not provide the security at transmission level. Biometric verification process is not focused. Based on these disadvantages leads to the proposed level.

b) Process of fingerprint Recognition:

Process of fingerprint Recognition consists of two modes, one is Fingerprint Verification and identification (Ravi Kumar1, L.,; Damien Dessimoz Jonas Richiardi; Smital, D., *et al*., 2012) as shown in figure 10 and 11 respectively. Finger print identification is to specify unique person by user fingerprint. Fingerprint verification is to make sure the legitimacy of one person by his fingerprint.

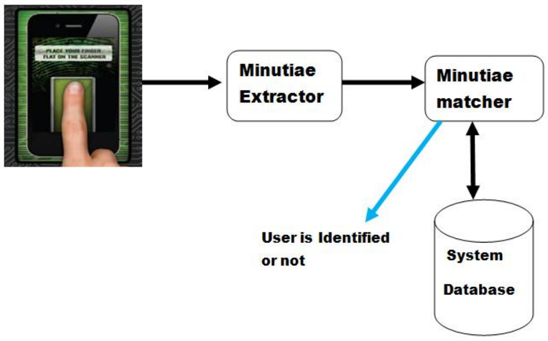

PLACE YOUR FINGER FLAT ON THE SCANNER
Minutiae Extractor
Minutiae matcher
User is Identified or not
System Database

Fig. 10: Fingerprint Identification

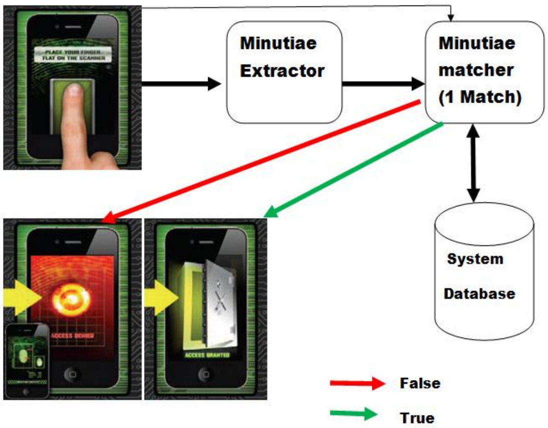


Fig. 11: Fingerprint Verification

c) Finger Print Preprocessing:

Extracting the ridge features, the following steps include typical feature extraction procedures as well as additional procedures for quality estimation and circular variance estimation (Heeseung Choi, *et al*., 2011) as shown in below figure 12.

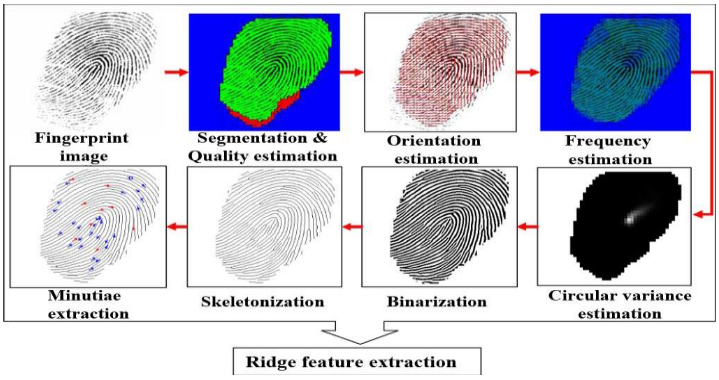


Fig. 12: Preprocessing Steps (Heeseung Choi, *et al*., 2011)

d) Preprocessing steps (Muzhir Shaban Al-Ani, 2013):

According to (Muzhir Shaban Al-Ani, 2013) the preprocessing steps are as follows:

- Image acquisition.
- Converting the input image into gray scale.
- Removing the unwanted parts from the image.
- Image orientation into exact position.
- Noise removal operation in which no effect on the fingerprint pattern.
- Image resizing into exact size.
- Image enhancement.

e) Fingerprint Enhancement Algorithm:

The flowchart of the fingerprint enhancement algorithm is shown in Fig. 13. The main steps of the algorithm include (Lin Hong, *et al*., 1998):

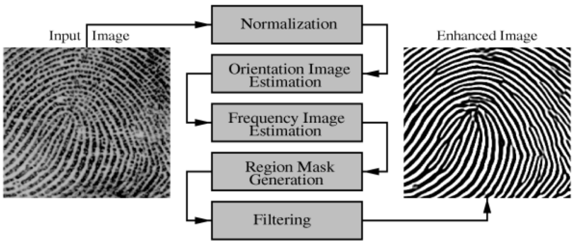


Fig. 13: Fingerprint Enhancement Process (Lin Hong *et al*., 1998)

1) *Normalization*:

It is used to pre specified the mean and variance by using normalization from input finger image.

2) *Local orientation estimation*:

Orientation image defines invariant coordinates for ridges and valleys in a local neighborhood and estimated from the normalized fingerprint.

3) *Local frequency estimation*:

The frequency image is computed from the normalized input fingerprint image and the estimated orientation image.

4) *Region mask estimation*:

The region mask is obtained by classifying each block in the normalized input fingerprint image into a recoverable or a unrecoverable block.

5) *Filtering*:

A bank of *Gabor filters* which is tuned to local ridge orientation and ridge frequency is applied to the ridge-and-valley pixels in the normalized input fingerprint image to obtain an enhanced fingerprint image.

III. Preliminaries:

a) Image Compression:

The algorithm using digitization and compression of grayscale fingerprint images by wavelet Scalar Quantization (WSQ) of image compression algorithm (Damien Dessimoz Jonas Richiardi). WSQ image compression algorithm consists of encoding and decoding functions.

1. WSQ Encoder:

It consists in too form of discrete wavelet transform (DWT) decomposition, a scalar quantization, and a Huffman entropy coding (Damien Dessimoz Jonas Richiardi).

2. WSQ Decoder:

It has to be able to decode these three processes and all variants of them that are allowed under the general specifications (Damien Dessimoz Jonas Richiardi).

b) Online Automatic matching process:

- ✓ Correlation based matching
- ✓ Minutiae based matching
- ✓ Ridge Based Matching

c) Processing steps of minutiae based system:

Minutiae based system consists of the following steps are (Asker, M. *et al*.,).

- ➢ Directional field estimation
- ➢ Adaptive filtering for noise reduction
- ➢ Thresholding to obtain a binary fingerprint image
- ➢ Morphological operations like thinning to obtain ridges that are only one pixel wide.
- ➢ Minutiae Extraction from the thinned image
- ➢ To reduce the number of false minutiae
- ➢ Registration of minutiae templates
- ➢ Matching Score Computation

d) Features of Ridge image Based matching:

Ridge image, also called thinned image or skeleton image, is an intermediate image in many feature extraction algorithms. Since minutiae are generally thought of as enough to identify a person, ridge image is just used to extract minutiae from it (Jianjiang Feng, Zhengyu Ouyang, Anni Cai, 2006).

Ridge image Features:

Features used to compare minutiae set points are given below (Jan Flusser, Filip ˇSroubek, and Barbara Zitov´a, 2007).

✓ Ridge image is an effective representation of the fingerprint image. From a ridge image, we can synthesize an image similar to the enhanced version of the original fingerprint image. On the contrary, it is definitely impossible to do so from a minutia set.

✓ Ridge image is also a compact representation of the fingerprint image. Ridge images can be efficiently approximated by polygonal lines, so the size of a template file is small.

- ✓ Similar minutiae patterns do not mean similar ridge patterns. Actually from experiments, we observed that the ridge patterns of most different fingerprints which have similar minutiae patterns are significantly different.
- ✓ The topology information in ridge patterns is reliable and invariant to nonlinear distortion.

e) Image Fusion:

The term fusion means (Jan Flusser, Filip ˇSroubek, and Barbara Zitov´a, 2007) in general an approach to extraction of information acquired in several domains. The goal of image fusion (IF) is to integrate complementary multisensor, multitemporal and/or multiview information into one new image containing information the quality of which cannot be achieved otherwise (Jan Flusser, Filip ˇSroubek, and Barbara Zitov´a, 2007).

Different Categories of image fusion:

Image fusion categories (Jan Flusser, Filip ˇSroubek, and Barbara Zitov´a, 2007) consists of multiview fusion, multimodal fusion, multi temporal fusion, multi focus fusion, fusion for image restoration and explanation (Jan Flusser, Filip ˇSroubek, and Barbara Zitov´a, 2007) is given below**.**

Multiview fusion of images from the same modality and taken at the same time but from different viewpoints.

Multimodal fusion of images coming from different sensors (visible and infrared, CT and NMR, or Panchromatic and multispectral satellite images).

Multitemporal fusion of images taken at different times in order to detect changes between them or to synthesize realistic images of objects which were not photographed in a desired time.

Multi focus fusion of images of a 3D scene taken repeatedly with various focal length.

Fusion for image restoration Fusion two or more images of the same scene and modality, each of them blurred and noisy, may lead to a deblurred and denoised image. Multichannel deconvolution is a typical representative of this category. This approach can be extended to super resolution fusion, where input blurred images of low spatial resolution are fused to provide us a high-resolution image.

f) Quick Response(QR)Code:

QR Code is a two-dimensional symbol. It was invented in 1994 by Denso, one of major Toyota group companies, and approved as an ISO international standard (ISO/IEC18004) in June 2000 (Tan jin soon, 2008). This two-dimensional symbol was initially intended for use in production control of automotive parts, but it has become widespread in other fields. Now QR Code is seen and used everyday everywhere in Japan for the following reasons (Tan jin soon, 2008):

- ➢ Several characteristics superior to linear bar codes: much higher data density, support Kanji/Chinese character, etc.
- ➢ It can be used by anybody free of charge as Denso has released the patent into the public domain.
- ➢ Data structure standard is not prerequisite for current usages.
- ➢ Most mobile phones in Japan equipped with cameras that enable reading of QR Codes can access Internet addresses automatically by simply reading a Uniform Resource Locator (URL) encoded in the QR Code.

g) Hash Message Authentication code(HMAC):

Message authentication is achieved via the construction of a message authentication code (MAC). MACs based on cryptographic hash functions are known as (HMACs). The purpose of a MAC ((HMAC)) is to authenticate both the source of a message and its integrity without the use of any additional mechanisms. HMACs have two functionally distinct parameters, a message input and a secret key known only to the message originator and intended receiver(s). Additional applications of keyed hash functions include their use in challenge-response identification protocols for computing responses, which are a function of both a secret key and a challenge message. An HMAC function is used ((HMAC)) by the message sender to produce a value (ie) MAC that is formed by condensing the secret key and the message input. The MAC is typically sent to the message receiver along with the message. The receiver computes the MAC on the received message using the same key and HMAC function was used by the sender. It compares the result computed with the received MAC. If the two values match, the message has been correctly received and the receiver is assured that the sender is a member of the community of users that share the key.

IV. Proposed Work:

Existing system consists of lot of disadvantages in M-commerce .They do not provide the more security, confidentiality and data integrity. Does not provide the fingerprint matching threshold level. Based on the performance, Stream cipher is better than block cipher (Naga suman Arepalli,s.srividya, 2012; Weerasinghe, T.D.B., 2012; Muazzam Ali Khan Khattak). Block cipher (AES algorithm) is better than RC4 and DES comparing the factors like, Image based Encryption and decryption time, CPU time, throughput and memory utilization (Naga suman Arepalli,s.srividya, 2012; Weerasinghe, T.D.B., 2012; Muazzam Ali Khan Khattak). Single fingerprint matching performance work is not focused in M-commerce. Does not provide the fingerprint matching algorithm in m-commerce. These problems are leads to the proposed work. Advanced Encryption Standard (AES) usually uses 10, 12, or 14 rounds. By implementing different types of transformation AES provides high security, these includes substitution, permutation, mixing and key adding each round except the last.

Process of Proposed work:

Process of proposed architecture is as shown in figure 14.

The steps involved are as given below.

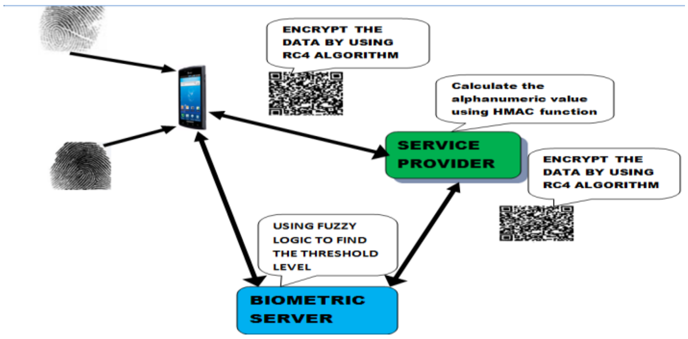

ENCRYPT THE DATA BY USING RC4 ALGORITHM
Calculate the alphanumeric value using HMAC function
SERVICE PROVIDER
ENCRYPT THE DATA BY USING RC4 ALGORITHM
USING FUZZY LOGIC TO FIND THE THRESHOLD LEVEL
BIOMETRIC SERVER

Fig. 14: Process of Proposed Architecture

Step 1:

The nonce request is sent to the Service provider using handheld device and handheld device acknowledge the nonce request. After nonce, Customer shared the secret key between the customer and Service provider. customer calculates the hash value by using HMAC$_D$(customer and product details + nonce + approve + cnt) technique (Krawczyk, H., *et al*., 1997) and send to the service provider. Process diagram shown in figure 15.

➤ Secure Details Transaction Techniques

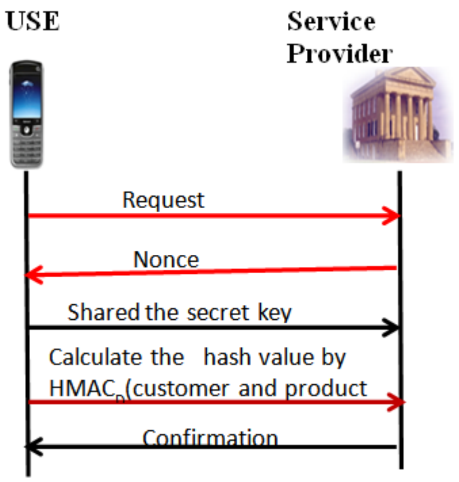


Fig. 15: Secure details Transaction techniques

Step 2:

User send the product and customer details is as shown figure 17,they are send to the Service provider (merchant).Customer and product details are converted into QR-code by using QR-code generation shown in figure 18. Details are encrypted by using AES algorithm and process diagram shown in figure 16.

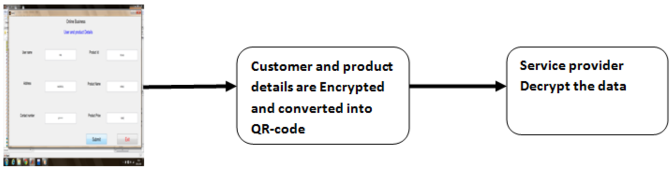
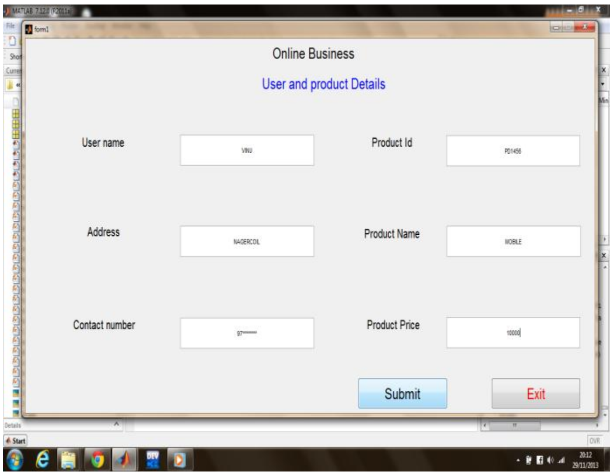

Customer and product details are Encrypted and converted into QR-code
Service provider Decrypt the data

Fig. 16: User sends the data to Service Provider


Online Business

User and product Details

User name: VINU

Product Id: PD1456

Address: NAGERCOIL

Product Name: MOBILE

Contact number: 97*******

Product Price: 10000

Fig. 17: User and Product Details

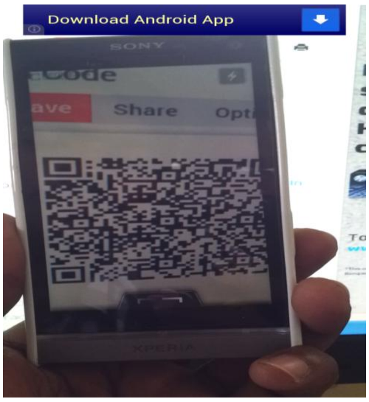
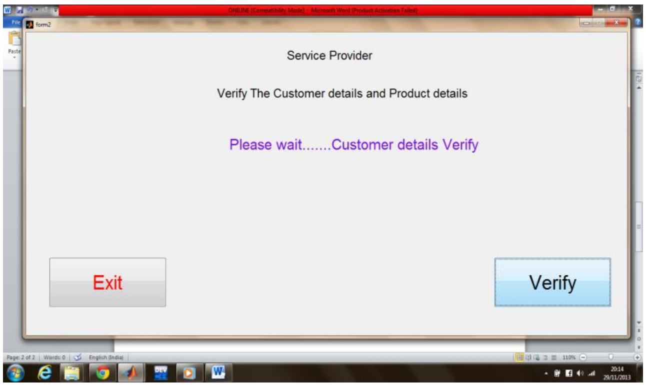


Fig. 18: After encrypt the customer and product details are converted into QR-code

Step3:

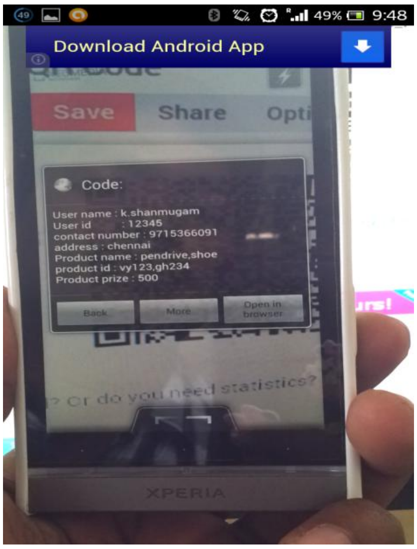
Service Provider Decrypt the Data and retrieve the data from QR-code and also verify the product and customer details, as shown in figure 19 and 20.


Service Provider

Verify The Customer details and Product details

Please wait.......Customer details Verify

Fig. 19: Customer and Product Details are verified by Service Provider



Code:

User name : k.shanmugam
User id : 12345
contact number : 9715366091
address : chennai
Product name : pendrive,shoe
product id : vy123,gh234
Product prize : 500

Fig. 20: Customer and Product details are retrieved from QR-code by Service provider

Step 4:

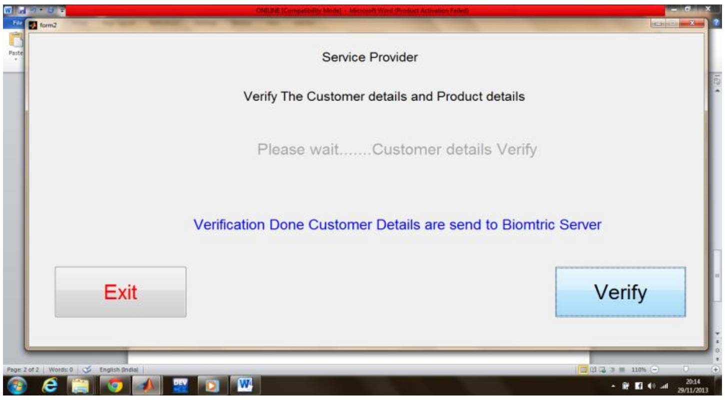
Service Provider calculates the hash value by using HMAC$_D$ (customer & product details + Nonce + check) technique (Krawczyk, H., *et al*., 1997). Service provider sends the hash value to the customer, shown in figure 14.

Step 5:

Customer calculates the confirmation hash value using same formula (step 4) as the service provider.

Step 6:

After verify the customer and Product details, service provider send the details to biometric server, as shown in figure 21.


Service Provider

Verify The Customer details and Product details

Please wait.......Customer details Verify

Verification Done Customer Details are send to Biomtric Server

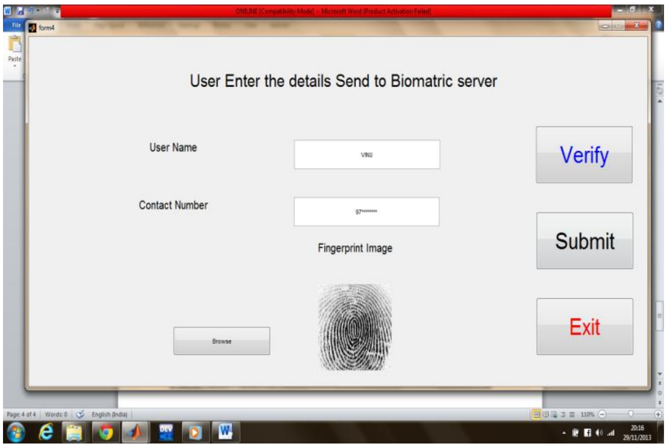
Fig. 21: Customer and product details send to the biometric server

Step 7:

Biometric server requests the customer details to the user.

Step 8:

Customers enter the details and send to the biometric server. User consists of Biometric mixed finger image, user name, contact number send to the biometric server, shown in figure 14 and 22.



User Enter the details Send to Biomatric server

User Name: VINU

Contact Number: 97********

Fingerprint Image

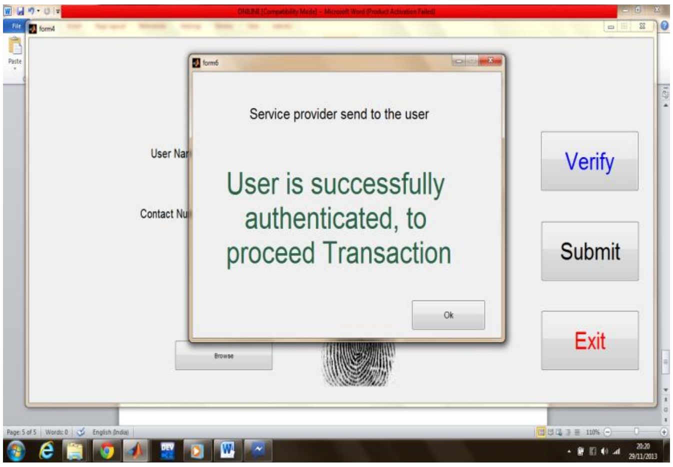
Fig. 22: User details send to biometric server by user

Step 7:

Biometric server verifies and compares the customer and service provider details. Biometric server sends the comparison result to the service provider.

Step 8:

Finally, Serviceprovider decide to access or deny the transaction, shown in figure 23.



Service provider send to the user

User is successfully authenticated, to proceed Transaction

Fig. 23: Service provider decision

a) Fingerprint image comparison process:

Mixed Fingerprint image send to the biometric server by using RC4 encryption are converted the QR-code. Biometric server decrypts the image and analyze with the previously stored finger print database. Finger 1 analyzed by using minutiae based matching algorithm. Finger 2 analyzed by using Ridge based matching algorithm. Finger 1 process consists of, first using the preprocessing process (Heeseung Choi, Kyoungtaek Choi, and Jaihie Kim, 2011) and next to extract the minutiae feature extraction. Minutiae method refers to bifurcation or termination points of ridges on the finger surface. Minutiae results indicate that there is some correlation between the distribution of minutiae and corresponding fingerprint classes. The minutiae feature representation reduces the complex fingerprint recognition problem to a point pattern matching problem. Among all the fingerprint features, minutiae point features with corresponding orientation maps are unique enough to discriminate amongst fingerprints robustly. Minutiae points compared to the existing fingerprint stored image in server database after feature extraction ,Enhancement process is done (Lin Hong, Student Member *et al*., 1998). Next to find out the threshold level. In similar, Finger 2 process consists of, first using preprocessing process and next extract the ridges (Heeseung Choi, Kyoungtaek Choi, and Jaihie Kim, 2011). Ridges are compared in server database. After feature extraction, enhancement is done. next to find out the threshold level.

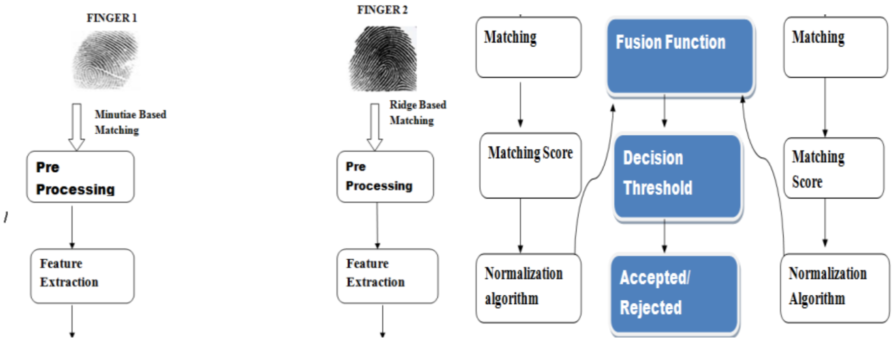
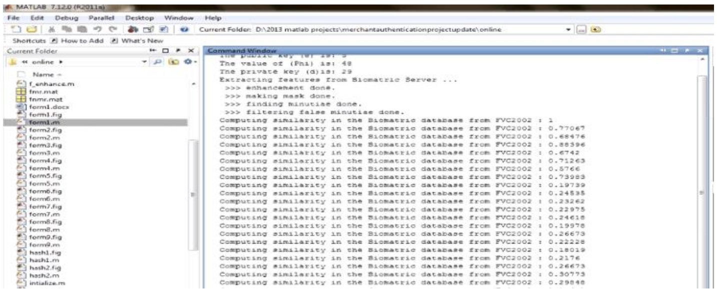


Fig. 24: Mixed fingerprint process



```
The public key (e) is: 5
The value of (Phi) is: 48
The private key (d)is: 29
Extracting features from Biomatric Server ...
 >>> enhancement done.
 >>> making mask done.
 >>> finding minutiae done.
 >>> filtering false minutiae done.
Computing similarity in the Biomatric database from FVC2002 : 1
Computing similarity in the Biomatric database from FVC2002 : 0.77067
Computing similarity in the Biomatric database from FVC2002 : 0.68476
Computing similarity in the Biomatric database from FVC2002 : 0.88396
Computing similarity in the Biomatric database from FVC2002 : 0.6742
Computing similarity in the Biomatric database from FVC2002 : 0.71263
Computing similarity in the Biomatric database from FVC2002 : 0.5766
Computing similarity in the Biomatric database from FVC2002 : 0.73983
Computing similarity in the Biomatric database from FVC2002 : 0.19739
Computing similarity in the Biomatric database from FVC2002 : 0.24535
Computing similarity in the Biomatric database from FVC2002 : 0.23262
Computing similarity in the Biomatric database from FVC2002 : 0.22975
Computing similarity in the Biomatric database from FVC2002 : 0.24618
Computing similarity in the Biomatric database from FVC2002 : 0.19978
Computing similarity in the Biomatric database from FVC2002 : 0.26673
Computing similarity in the Biomatric database from FVC2002 : 0.22228
Computing similarity in the Biomatric database from FVC2002 : 0.18019
Computing similarity in the Biomatric database from FVC2002 : 0.2176
Computing similarity in the Biomatric database from FVC2002 : 0.26673
Computing similarity in the Biomatric database from FVC2002 : 0.30773
Computing similarity in the Biomatric database from FVC2002 : 0.29848
```

Fig. 25: Extracting features, enhancement and false minutiae done process

b) Fusion process:

After find out the threshold level, finger1 minutiae points and finger2 ridges are mixed with CONTOURLET IMAGE FUSION algorithm and got the new fingerprint and also Encrypt the finger image by using RC4 algorithm and compared in biometric server database. Authentication phase is as shown in figure 24.

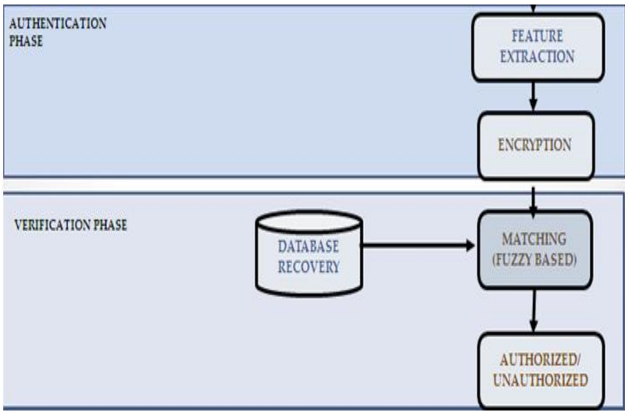
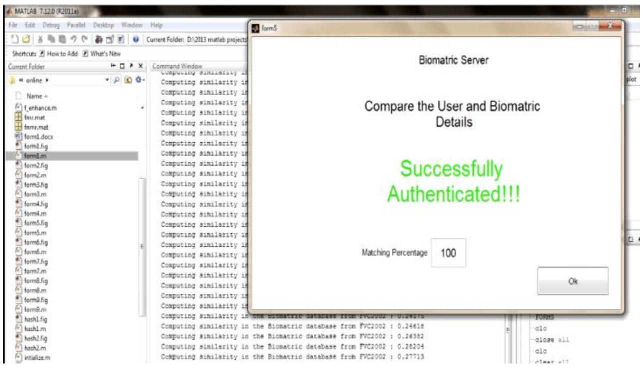


Fig. 26: Authentication and verification process

c) Verification process by using fuzzy logic:

Mixed finger image is compared in server database by using fuzzy logic. Fuzzy logic find out the threshold level and analyze the user is authenticated or not. Fuzzy logic matching percentage is 100% in this case provide the SMS authentication to the user. Fuzzy logic matching percentage is 60-99%, in this case One time password (OTP) and SMS authentication are provided for another authentication to secure transaction. Matching percentage is below 60%,in this case service provider does not use the transaction process so denied the process.



Biomatric Server

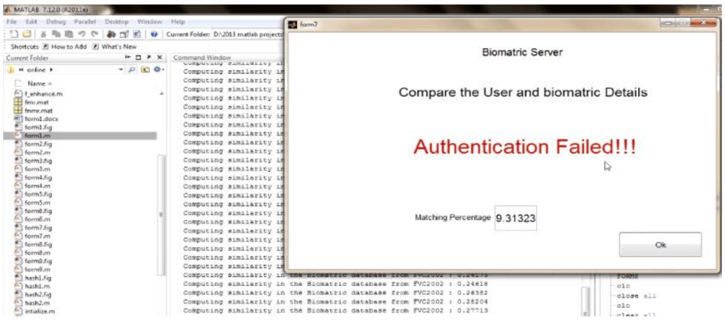
Compare the User and Biomatric Details

Successfully Authenticated!!!

Matching Percentage: 100

```
Computing similarity in the Biomatric database from FVC2002 : 0.24618
Computing similarity in the Biomatric database from FVC2002 : 0.26382
Computing similarity in the Biomatric database from FVC2002 : 0.28204
Computing similarity in the Biomatric database from FVC2002 : 0.27713
```

Fig. 27: Matching percentage analyzed by using fuzzy logic



Biomatric Server

Compare the User and biomatric Details

Authentication Failed!!!

Matching Percentage: 9.31323

```
Computing similarity in the Biomatric database from FVC2002 : 0.24618
Computing similarity in the Biomatric database from FVC2002 : 0.26382
Computing similarity in the Biomatric database from FVC2002 : 0.28204
Computing similarity in the Biomatric database from FVC2002 : 0.27713
```

Fig. 28: Matching percentage is below 60%-deny the process.

d) Advantages of Proposed System:

- Prevent the loss of personal information through the theft of cell phones by using the biometric authentication has been virtually eliminated the possibility of someone gaining access to a third party cell phone directly.
- Provide more security by exploring the possibility of mixing two fingerprints in order to generate new fingerprint, the mixed fingerprint is dissimilar from the original fingerprints and they provide virtual identity from the fixed fingerprints.
- Biometrically secured mobile payment system is much safe and secure and very easy to use, also no need to remember passwords and secrete codes. To provide ease of access from anywhere.
- To provide more security for mobile payment, mobile purchasing and mobile banking services.
- Reduce to remembering numerous Passwords.
- Prevent third party access by using the mixed fingerprint.
- This proposed system used for joint account holder.

e) Performance and Parameter Discussion of Proposed System:

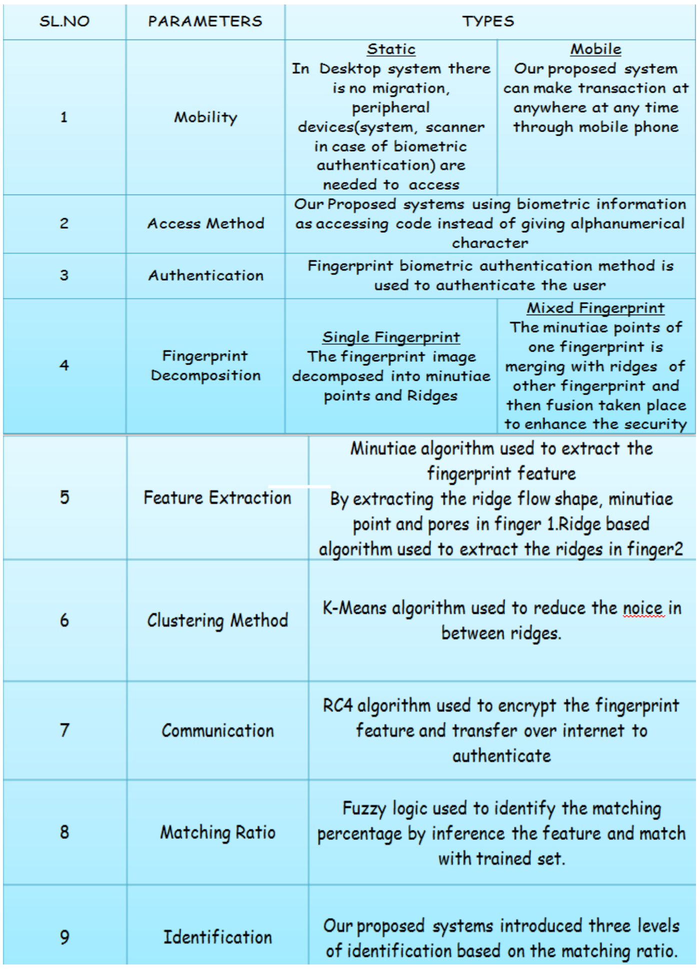
The performance and parameters discussed for the mixed fingerprint system are as shown in Table 1.

Conclusion:

The mixed fingerprint provides enhanced security for online secured transaction in m-commerce. Minutiae and Ridges mixed fingerprint feature explored the unique identity of individuals.

Fingerprint matching threshold levels are found out and provide more authentications for based on the threshold level so, provides more security in authentication and transaction. Protect from unauthorized user to access your personal information by hacking the secret code. User authentication is very essential in mobile commerce. User authentication is done by mixed fingerprint. Data integrity, confidentiality and non-repudiation are done by using QR-code and HMAC technique. In future, by using multimodal (Combination of finger and face or iris and finger or finger, face, voice etc..,) biometric mechanism for user authentication in mobile commerce will be considered.

Table 1: parameters of proposed missed fingerprint system



SL.NO	PARAMETERS	TYPES	
1	Mobility	Static In Desktop system there is no migration, peripheral devices(system, scanner in case of biometric authentication) are needed to access	Mobile Our proposed system can make transaction at anywhere at any time through mobile phone
2	Access Method	Our Proposed systems using biometric information as accessing code instead of giving alphanumerical character	
3	Authentication	Fingerprint biometric authentication method is used to authenticate the user	
4	Fingerprint Decomposition	Single Fingerprint The fingerprint image decomposed into minutiae points and Ridges	Mixed Fingerprint The minutiae points of one fingerprint is merging with ridges of other fingerprint and then fusion taken place to enhance the security
5	Feature Extraction	Minutiae algorithm used to extract the fingerprint feature By extracting the ridge flow shape, minutiae point and pores in finger 1.Ridge based algorithm used to extract the ridges in finger2	
6	Clustering Method	K-Means algorithm used to reduce the noice in between ridges.	
7	Communication	RC4 algorithm used to encrypt the fingerprint feature and transfer over internet to authenticate	
8	Matching Ratio	Fuzzy logic used to identify the matching percentage by inference the feature and match with trained set.	
9	Identification	Our proposed systems introduced three levels of identification based on the matching ratio.	

ACKNOWLEDGMENT

My sincere thanks to Stigmata Techno Solutions to complete this paper.

REFERENCES

Asker, M. Bazen, Gerben T.B. Verwaaijen, Sabih H. Gerez, A Correlation-Based Fingerprint Verification System.

By Rajnish Tiwari1, Stephan Buse2 and Cornelius Herstatt, From electronic to mobile commerce: Technology convergence enables innovative business services.

Chang-Lung Tsai Chun-Jung Chen, 2012. Secure OTP and Biometric Verification Scheme for Mobile Banking, IEEE.

Damien Dessimoz Jonas Richiardi,Prof. Christophe Champod Dr. Andrzej Drygajlo, Multimodal Biometrics for Identity Documents.

Hamzeh Khazaei, Ali Mohades, 2007. Fingerprint Matching and Classification using an Onion Layer algorithm of Computational Geometry, IEEE, 1: 1.

Harini Jagadeesan, Design and Verification of Privacy and User Re-authentication Systems

Heeseung Choi, Kyoungtaek Choi, and Jaihie Kim, 2011. Fingerprint Matching Incorporating Ridge Features With Minutiae,IEEE.

Hisham Al-Assam, Harin Sellahewa, Sabah Jassim, 2011. Accuracy and Security Evaluation of Multi-Factor Biometric Authentication, International Journal for Information Security Research (IJISR), Volume 1, Issues 1/2.

Jan Flusser, Filip ˇSroubek, and Barbara Zitov´a, 2007. Image Fusion:Principles, Methods, and Applications.

Jianjiang Feng, Zhengyu Ouyang, Anni Cai, 2006. Fingerprint matching using ridges.

Junta Doi, Member, IEEE, 2005. and Masaaki Yamanaka, Discrete Finger and Palmar Feature Extraction for Personal Authentication, IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, 54: 6.

Karthik Nandakumar, Student Member, IEEE, Anil K. Jain, Fellow, IEEE, 2007. Fingerprint-Based Fuzzy Vault:Implementation and Performance,IEEE.

Krawczyk, H., M. Bellare and R. Canetti, 1997. ”HMAC: Keyed-hashing for message Authentication”RFC 2104.

Lin Hong, Student Member, IEEE, Yifei Wan, and Anil Jain, Fellow, IEEE, 1998. Fingerprint Image Enhancement:Algorithm and Performance Evaluation, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, 20: 8.

Mangala Belkhede, Veena Gulhane, Dr. Preeti Bajaj, 2012. Biometric Mechanism for enhanced Security of Online Transaction on Android system: A Design Approach,icact.

Mehata K.M., 2011. improved pin distribution techniques in m-commerce,GCSE, Dubai,UAE

Muazzam Ali Khan Khattak, Encryption based secure data delivery.

Muzhir Shaban Al-Ani, 2013. A Novel Thinning Algorithm for Fingerprint Recognition, International Journal of Engineering Sciences, 2(2).

Naga suman Arepalli,s.srividya, 2012. image encryption and decryption based on AES and RC4,IOSR.

Naser Zaeri, Minutiae-based Fingerprint Extraction and Recognition

Nidhi Singhal, J.P.S. Raina, 2011. Comparative Analysis of AES and RC4 Algorithms for Better Utilization, International Journal of Computer Trends and Technology.

Nirav Jobanputra, Vijayendra Kulkarni, Dinkar Rao, and Jerry Gao, Emerging Security Technologies for Mobile User Accesses.

Norman, Y. Mineta, The Keyed-Hash Message Authentication Code (HMAC).

Ravi Kumar1, L., S. Sai Kumar 2, J. Rajendra Prasad3, B. V. Subba Rao4, P. Ravi Prakash, Fingerprint Minutia Match Using Bifurcation Technique.

Sheng Li, Student Member, IEEE, and Alex C. Kot, Fellow, IEEE, 2013. Fingerprint Combination for Privacy Protection, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 8: 2.

Smital, D., Patil, Shailaja A. Patil, 2012. Fingerprint recognition using minutia matching, World Journal of Science and Technology.

Tan jin soon,Overview of the QRcode,synthesis journal 2008.

The boston consulting group,mobile commerce winning the air consumer, 2010

Vesselin Tzvetkov Arcor, A.G. and Co.K¨olner Strasse 5, WAP Protocol Security Solutions for Mobile Commerce.

Wan, S., Yi1, Woong Go2, Dongho Won1, Jin Kwak2∗, Secure Authentication Protocol with Biometrics in an M Commerce Environment

Weerasinghe, T.D.B., 2012. Secrecy and Performance Analysis of Symmetric Key Encryption Algorithms, IJINS, 1(2): 77-87.

Wen-Chen Hu, Jyh-haw Yeh, Hanheld Devices and Computing and payment methods for mobile commerce.

www.\\htttp.Wikipedia.com