Fingerprint Extraction and Comparison for Payment Transaction in Mobile Commerce

[1]S.celin sindhya, [2]Dr.B.vanathi,[3]K.Shanmugam
[1]PG Scholar [2]Professor&Head,[3]Assisstant Professor
Department of Computer Science and Engineering, Valliammai Engineering College
Kattankulathur, Chennai, India

***Abstract* - This study focuses on an advanced mobile security system to provide rapid and highly secure human friendly M-Commerce transaction. M-commerce transaction works in multistep process. The process involves User authentication, Merchant authentication, Message authentication, secure payment details transaction authentication. M-commerce provides availability, reliability and security in transaction phases. In Proposed method consists of, more security, efficiency and accuracy levels are provided by using Minutiae Maps (MM) in fingerprint feature extraction level. User send the finger image to the biometric server by using discrete wavelet transform method and water marking techniques, hence finger image can be hidden. User finger image is checked and also compared with MM methods using biometric server. The comparison, fingerprint intensity level is recognized then the threshold level is (60-99%) means the process is successfully done.**

***IndexTerms* - Payment, Water Marking, Mobile Commerce**

I. INTRODUCTION

The main aim of this project is to purchase goods anywhere through Mobile Commerce applications with user authentication and message authentication. Mobile commerce have exploded in the last five years. In fact, Bank of America predicts US$67.1 billion in purchases will be made from mobile devices by European and US shoppers in 2015.1 Several factors are driving this rapid growth of mobile commerce. Another driving factor is consumer demand for applications for buying and selling goods and services, as well as for online banking and bill payment. Nowadays, most banks and brokerage firms provide mobile apps for their customers to support online banking and trading. The final factor is the rapid adoption of online commerce due to stronger security practices. For example, authentication techniques that use multiple factors or out-of-band verification are common practices now. A variety of m-commerce products and services have thus emerged. These include mobile money transfer, mobile Automated Teller Machine (ATM), mobile ticketing, content (video and audio) purchase and delivery, and location-based services (local discount offers) [1]. New applications are also developing quickly. Mobile payments can be made directly inside of a mobile app running on a Smartphone. Such in-app purchases can be a recurring revenue stream for developers. Mobile commerce defined as "the delivery of electronic commerce capabilities directly into the hands, anywhere, via wireless technology" and "putting a retail outlet in the customer's hands anywhere".The Mobile commerce means purchase from everywhere and it is much easier than Electronic commerce. E-commerce means purchase from home/ working place. E-commerce needs Internet connectivity. M-commerce does not need any connectivity. Video conferencing can be done in M-Commerce, which is not possible in E-commerce. Electricity is not a main factor in Mobile commerce. But it is a main factor in E-Commerce. M-commerce and its related technologies offer many different application fields, such as Location Based services (LBS), Mobile ticketing, Mobile shopping, Mobile Financial services, Mobile Marketing and Mobile Entertainment. Mobile Commerce users can do multitasks at the same time. Mobile Commerce users expect immediate response and provide the exact result based on context. M-Commerce occurs through the use of wireless devices such as cell phones, pocket Personal Computer (PC's), and Personal Digital Assistant (PDAs). It allows a user to purchase goods and services on the move, anytime, and anywhere.

M-Commerce is becoming a larger part of the internet commerce experience. Juniper Research performed a study that predicted that by 2009, global M-Commerce revenue will exceed 88 billion dollars. A Morgan Stanley report found that in 2005 there was 19.5 billion dollars in M-Commerce transactions [1]. These included revenue from people buying ring tones, cell phone personalization, games, and services. With the large amount of revenue potential, companies are quickly moving into the mobile marketplace. In many countries of the world it is more likely that an individual will have a cell phone rather than a computer with internet connectivity. McKinsey research firm reported that in 2005, there was an estimated 85% penetration rate for mobile phone usage in Europe but in Asia there were over 310 million mobile devices .The Morgan Stanley research report mentioned earlier shows that in many areas of the world the number of mobile users exceeds the number of PC users. These scenarios are highly attractive to companies because it provides an opportunity to expand their customer bases. This means there is a potential to reach millions of new customers and expand on revenues.

The biggest benefit that M-Commerce provides to consumers is mobility. As long as their mobile device network is in range then M-Commerce transactions can be made. In order to meet these demands, cell phone companies across the world are continually upgrading their networks and increasing the speed and bandwidth of these networks.

Security Trust

Authentication

Each party should authenticate its Counterpart.

Integrity

Each party should make sure that the received messages are not altered

Confidentiality

Each party wants to keep the content of its communication secret.

Scope of the Project

It enhances the security of the trusted device and minimizes the possibility of security breach in Authentication scheme. Provides greater amount of security in M-Commerce transactions such as Location Based Services, Mobile Ticketing, Mobile Shopping, Mobile Financial Services, Mobile Marketing, Mobile Entertainment and so on. For promotion of mobile transaction among users a secure M-Commerce Architecture has been built, providing three way securities like user authentication, merchant authentication, and message authentication and building a complete solution for M-Commerce applications.

II.LITERATURE SURVEY

A.Enhancing secure transaction and identity authentication in M-Commerce

In last few years, Mobile commerce had seen extreme growth. But to be focused the lot of privacy, security and integrity challenges. This paper proposes, to send the user Pin number and payment details in secure way. Pin number is encrypted by Amalgam encryption. Amalgam encryption means, Encrypt the pin number by using combination of Triple data Encryption standard (3-DES) and Ron's Code (RC4) algorithm. Amalgam encryption is does not used for secure transaction in Mobile commerce so current system will be used in this encryption process. User Pin number is divided into two halves(pin1 and pin2).The two halves of the pin are encrypted by using amalgam encryption to be separately. By using amalgam encryption, to provide the more security and increasing the encryption secrecy value [1] as shown in figure 1.

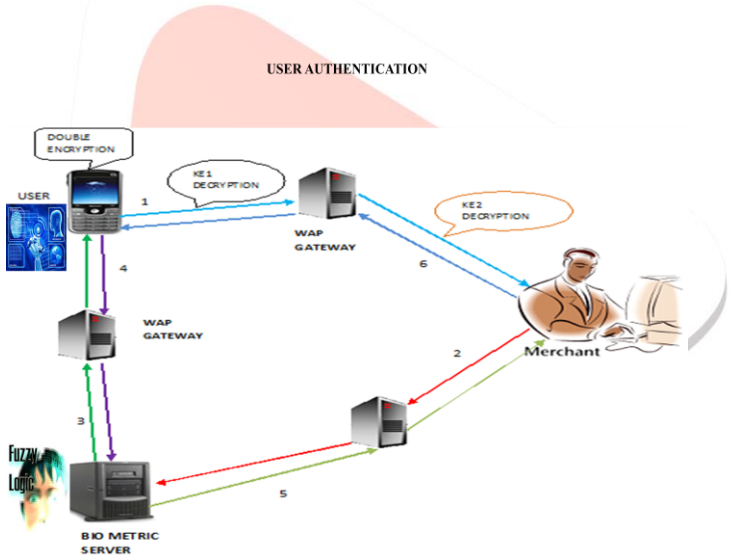

Figure 1: User Authentication Architecture[1]

Step 1:

The USER sends the mobile phone number and service and product information (vy102) to the SERVICE PROVIDER to utilize the service or products.

E(K1(E(k(9715366091,vy102)))) } MOBILE TERMINAL

↓ D(k1)

E(K(9715366091,vy102) } WTLS

↓

E(K2(E(k(9715366091,vy102)))) } WAP GATEWAY

↓ D(K2)

E(K(9715366091,vy102) } TLS

↓ D(K)

9715366091,vy102 } SERVER

Step 2:

The SERVICE PROVIDER (SP) sends his identification and user's mobile phone number to the BIO METRIC SERVER by double encryption model, and requests verification of the user's identity. The BIOMETRIC SERVER verifies the SERVICE PROVIDER identification.

Step 3:

The BIO METRIC SERVER requests biometric information for authentication from the user by sending his identification and SP identification. The user verifies the BS identification whether or not s/he first registered with that institution. The SP identification is used to validate the SP whether or not s/he requested products or services from that provider.

Step 4:

The user captures and hashes biometric information using the mobile device, and sends it with the mobile phone number to the BS.

Step 5:

The BS compares the received and stored hashed biometric information to verify the right user. The BS sends the result of the comparison with the user's phone number to the SP. The user's phone number is used to ascertain whose biometric information is to be checked.

Step 6:

The SP accepts or denies service to the user as a result of the comparison if the user authentication is completed.

Double encryption model

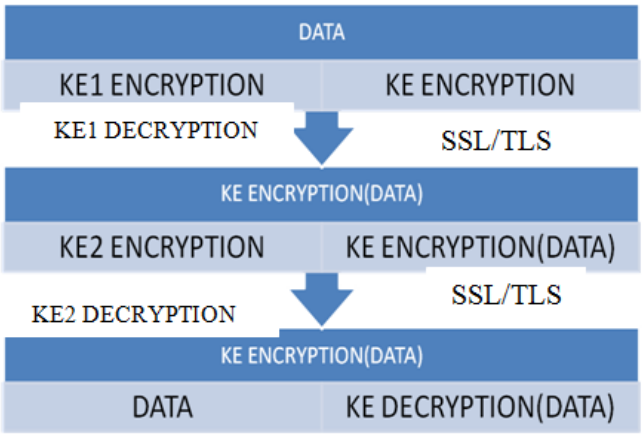

Figure 2: Double Encryption Model[1]

It consists of the information flow moves from the mobile terminal to the content server. Two parts of the secure WAP transaction process consists of Mobile terminal, WAP gateway and server. Mobile terminal sends the message encrypted by Wireless Public Key Infrastructure (WPKI), Wireless Application Protocol (WAP) gateway decrypts it with WPKI ,then converts it into a corresponding format which can transmit between gateway and server.WAP gateway encrypt the message with PK2,the content server uses PK2 to decrypt and read the message content[1] as shown in figure 2.

Advantages of double encryption model

To use the WAP gateway, it provides improved security based on Double encryption model, major advantages by this solution consists of:

1. To reduce the communication cost of the encryption between mobile terminals and servers Short time and increase the connection speed and security.
2. Easy to implement. Data confidentiality is achieved by using the distributed the PIN.
3. The PIN is divided into two parts and sent. Even if the impostor with the succeeds to trap one half of the PIN, it becomes plentiful to crack the other half of the PIN simultaneously.
4. The cracking of the entire PIN becomes extremely difficult and a tedious process providing enhanced security to this system.

Disadvantage

Easy to acquire someone's PIN by through shoulder surfing, camera's placed in the environment, compromised debit or credit card terminals.

B.Secure Authentication Protocol with Biometrics

Existing biometric techniques used for user authentication is unique. User authentication is achieved by mobile device. The main advantages of this technique are as both users and service provider recognizes without an additional device by merits of using (ECC) for encryption method is, the process is small, efficient and requires low power [2]. The Limitations in biometric techniques are, as it uses only encryption method for user and payment details for secure transfer of the data. By not using a security conversation mechanism such as WAP gateway data are not more secured. No Merchant authentication is available in this technique. The limitations of using ECC consists of, difficulty in counting the number of points on the curve and generating suitable curves. ECC is not yet fully understood and relatively has slow signature verification [2].

Advantages

The main advantages of this technique are as both users and service provider recognizes without an additional device by merits of using (ECC) for encryption method is, the process is small, efficient and requires low power.

Its provided the lot of security and authentication schemes.

Disadvantage

Key size is large memory storage and decryption time increases Theft/**Loss of device and information** data stored in the device is easily accessed physically if the device is lost or stolen.

C. Secure One Time Password (OTP) and Biometric Verification

In this process user authentication is verified by One Time Password (OTP) and biometric method [3]. But it authenticate only use rafter receiving the service request, the server side will then request the client side to capture personal biometric such as fingerprint, iris, photo, and etc. Immediately for further verification with the existed data stored in the server side to prevent the M-banking embezzling. If the personal biometric has been verified as an old one, the M-banking will immediately terminated by the server side. As the verification is finally done by the server side, the client side then can perform transaction via M-banking smoothly. The proposed scheme not only can provide secure M-banking, but also can clearly define the process. Therefore, if there are any M-banking arguments occurred due to internet hacking or mobile phone stealing for M-banking, both of the server side and client side could protect their rights and interests. One Time Password OTP operation is costlier than QR-TAN techniques. In OTP, only exact matching is considered as success [3].

Advantage

The client side can perform transaction via M-banking smoothly by One Time Password (OTP).

Disadvantage

The Major disadvantage is they have not discussed/used any secure algorithm for encryption method at transmission level.

D. Biometrics Technique

According to Wikipedia, 'Bio' means 'life' and "metrics" means 'measurement'. Biometrics is the measurement of characteristics of human being. The major Classification of biometric characteristics is as shown in figure 3[4].

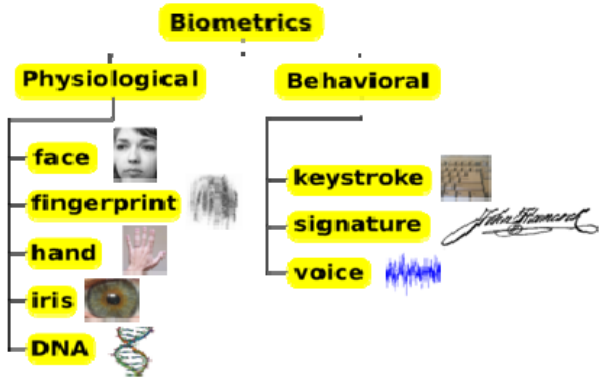

Figure 3: Classification of Biometrics characteristics[4]

Existing biometric techniques used for user authentication is unique. User authentication is achieved by mobile device. The main advantage of this technique is as both users and service provider recognizes without an additional device. The merits of using ELLIPTIC CURVE CRYPTOGRAPHY (ECC) for encryption methods are the process is small, efficient and requires low power.

The **Limitations in biometric techniques** are, it uses only encryption method for user and payment details for secure transfer of the data. By not using a security conversation mechanism like WAP gateway, data's are not more secured. No Merchant authentication is available in this technique.

The **limitation of using ECC is** difficulty in counting the number of points on the curve and generating suitable curves. ECC is not yet fully understood and relatively has slow signature verification.

E. The Online user Supervision Architecture

A generic supervision process begins when a user sends a request to an Service provider (SP) to carry out an action over a resource (often a service or a piece of information). Afterward, an element independent of the user decides whether this action, characterized by a 3-tuple (user, action, and resource), is subject to supervision. If so, a supervision phase, which might involve other human or computer elements, determines whether to let the user perform the action.

Involving the Service Provider

One of the most popular approaches to online user control is content filtering. A major limitation of content filtering rests on its independence from SPs, which is one of its foundations. This means the filtering system doesn't achieve full knowledge of the services, which ultimately prevents it from understanding what the supervised users want to do. The increasing complexity of online services, many times spanning providers from different administrative domains, only worsens this situation. SPs also remain agnostic of supervision procedures and often won't adapt their contents to supervised users. All this leads to unsuccessful user supervision and a bad user experience.

Oversee is based on the principle that SPs can request that users provide special attributes or personal traits to access resources. Should a user not meet the requirements, SPs can demand that a supervisor accompany the user by giving explicit authorization. In this way, SPs act as supervision enforcement points, characterizing the action 3-tuples and choosing which ones are subject to evaluation. Basically, oversee comprises a user, a supervisor, an SP, and the online actions manager (OAM), which is the main actor during supervision as shown in figure 8. The OAM maintains links between the user and supervisor. It also authenticates the user and supervisor and notifies the supervisor about online actions requiring evaluation. Finally, it informs the SP about the supervision phase's outcome. Oversee employs a user-centric identity management system that orchestrates the information exchange between the different actors in a manner that respects privacy.

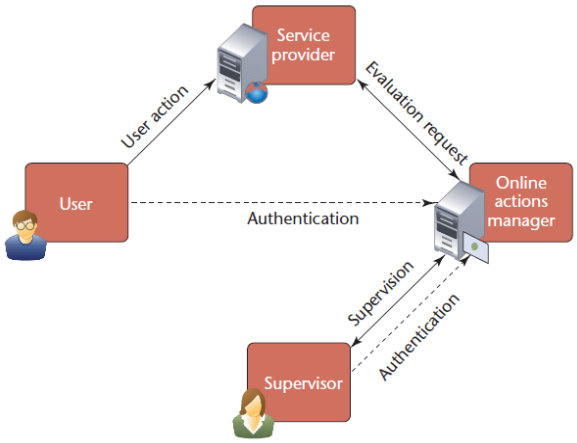

Figure 4 : Oversee[5]

Figure 4[4] shows the general supervision workflow that run on a per-user-action basis.

Step1:

The user requests a certain resource (a piece of information or a service) from the SP.

Step2:

The SP consults its security policies and determines that, to allow the user (previously authenticated or not) to access that resource, it needs a set of identity attributes (for example, that the user is of legal age or belongs to a private group). If so, the SP asks the user for a piece of digital data that asserts the required attributes or that's authorized by someone who does. It also sends details on the current action 3-tuple, which might include information about the possible outcomes of allowing the action.

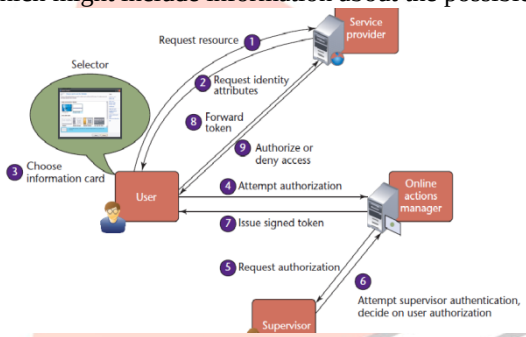

Figure 5: Online user supervision workflow[5]

Step3:

The user, after receiving such a request, selects an information card, previously issued by the OAM, from the card selector that meets the requirements. If no plain card meets the requirements (for example, because the user isn't of legal age), the user must choose a different supervised card.

Step 4:

The user authenticates himself or herself with the OAM. If authentication is successful and no supervision is required, the workflow skips to the seventh step.

Step 5:

If the selected information card requires supervision, the OAM informs the supervisor and requests authorization. It also forwards details about the action 3-tuple to the supervisor.

Step 6:

The supervisor authenticates himself or herself with the OAM, evaluates the action 3-tuple and the requested claims, and decides whether to authorize the action. The supervisor sends its decision to the OAM.

Step 7:

The OAM issues a digitally signed token containing either user identity information or supervisor authorization along with supervisor and user identity information.

Step 8:

The selector forwards the signed token to the SP.

Step 9:

Finally, the SP checks the validity of the token and its digital signature. If the user meets the requirements, the SP authorizes access. If the user doesn't meet the requirements but the supervisor does and has authorized the user, the SP gives the user access to the resource on behalf of the supervisor. If the supervisor has denied the user access, the SP might offer the user an alternative resource [5].

In this process, it is assumed that the user has a card selector and several information cards, including at least one supervised information card. In fact, before any online user supervision procedure, the supervisor must log in to the OAM and request a supervised information card for the user. The OAM links the supervisor identity to this card.

F. Fuzzy Logic in Biometrics

Fuzzy logic is conceptually easy to understand. The mathematical concepts behind fuzzy reasoning are very simple [5]. Fuzzy logic is a more intuitive approach without the far-reaching complexity. Fuzzy logic is flexible. With any given system, it is easy to layer on more functionality without starting again from scratch. Fuzzy logic is tolerant of imprecise data. On closely inspecting everything is imprecise. Fuzzy reasoning builds this understanding into the process rather than tacking it onto the end. Fuzzy logic can model nonlinear functions. Fuzzy logic is not a cure-all. It is a convenient way to map an input space to an output space. If it's not convenient, try something else. If a simpler solution already exists, use it. Fuzzy logic is the codification of common sense. Use common sense when you implement it and you will probably make the right decision. Many controllers do a fine job without using fuzzy logic The limitation is that it consumes enormous time while matching and hard to develop a model from fuzzy system.Using the Fuzzy logic in biometric Server, to check the existing stored finger print image with present finger print image. If comparing result is 60-99% threshold level, the user is right person then below 60 % the user is not a right person and not authenticated [6].

Advantage

Fuzzy logic is conceptually easy to understand. The mathematical concepts behind fuzzy reasoning are very simple. Fuzzy logic is a more intuitive approach without the far-reaching complexity. Fuzzy logic is flexible

Disadvantage

Processing level is low.

G. WAP Protocol Security in Mobile Commerce

Mobile payment is the process of two parties exchanging financial value using a mobile device in return for goods or services. This paper is an analysis of the security issues in mobile payment for m-commerce. This paper introduces m-commerce and mobile payment. It discusses the public key infrastructure as a business for secure mobile technologies. It also study the features for different security technologies employed in current m-commerce market, including Wireless Application Protocol (WAP), Subscriber Identity Module (SIM) application toolkit and Java 2 Micro Edition (J2ME). This paper also compares the effectiveness of these security technologies in supporting a secure mobile payment, and discusses research issues to enhance the security of mobile payment for large scale deployment of m-commerce [11].Some of the protocols and technologies that facilitate the handling and transmitting of sensitive payment information to and from the mobile devices in an M payment transaction are given below:

Wireless Application Protocol (WAP)

The WAP forum has specified a series of protocols, which cover all the protocol layers from the transport level to the presentation layer. The functional areas related to security in WAP considered include Wireless Transport Layer Security (WTLS), Wireless Identity Module, WAF Public Key Infrastructure (PKI), WML Script sign Text, and End-to-End Transport Layer Security, The WTLS (Wireless Transport Layer Security) protocol is a PKI-enabled security protocol, designed for securing communications and transactions over wireless networks. It is used with the WAP transport protocols to provide security on the transport layer between the WAP client in the mobile device and the WAP server in the Wireless Application Firewall (WAF) gateway. The security services that are provided by the WTLS protocol are authentication, confidentiality and integrity. WTLS provides functionalities similar to that of Internet Transport Layer Security systems (TLS) and Secure Sockets Layer (SSL). It has been largely based on TLS, but has been optimized for narrow-band communications and incorporates datagram support. WTLS is implemented in most major micro-browsers and WAF servers. WAP 1.x series use the WTLS protocol to protect messages in the wireless network part and some way into the wired network, that is, between the wireless device and WAF Gateway. The WAP gateway transforms the WAP 1 .x stack to/from the wired TCP/IP stack, relays the data between the wireless and wired network, and communicates with the Web Server that the mobile device is accessing.

Wireless Identity Module (WIM) is used in performing functions related to WTLS and application level security by storing and processing information like secret keys and certificates needed for authentication and non-repudiation. To enable tamper resistance, WIM is implemented as software on a microprocessor-based smart card. WML script sign Text includes support for digital signatures of WML (display format of data in wireless world analogous to HTML) coded content. Sign Text function allows a wireless user to digitally sign a transaction in a way that can be verified by a content server. This provides end-to-end authentication of the client, together with integrity and non-repudiation of the transaction. The WPKI architecture for WAP 1.x series is shown in Figure 6[7].

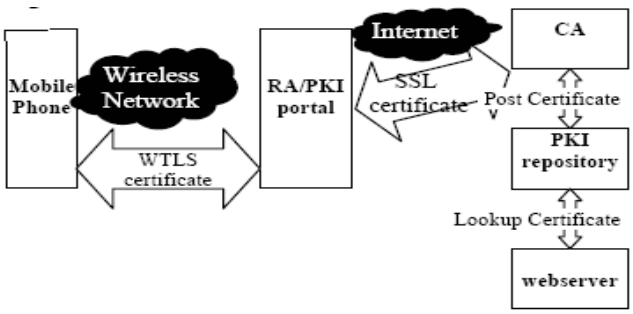

Figure 6: WPKI architecture for WAP 1.x series[7]

Analysis of current techniques

In WAP**,** security is provided through Wireless Transport Layer Security (WTLS) protocol (WAP 1.0) and Transport Layer Security (TLS) protocol (WAP 2.0). They provide data integrity, privacy, and authentication. The feature of data integrity ensures that the content of messages is not altered during transmission. Privacy makes sure that only the intended recipients can read the original content. Authentication verifies the identities of communication participants. **One security problem, known as the "WAP gap," is caused by the existence of a WAP gateway in a security session.** Here the encrypted messages sent by end systems might temporarily become clear text on a WAP gateway when messages are processed. In SIM toolkit, security requirements cover the usual transport layer security issues such as peer authentication, message integrity, replay detection and sequence integrity, proof of receipt, and message confidentiality. Each application message is divided into packets that are individually secured by protecting the payload and adding security header.

H. Fingerprint Image Enhancement

Fingerprint recognition is one of the most popular and successful methods used for person identification, which takes advantage of the fact that the fingerprint has some unique characteristics called minutiae; which are points where a curve track finishes, intersect with other track or branches off. A critical step in studying the statistics of fingerprint minutiae is to reliably extract minutiae from the fingerprint images [8]. However, fingerprint images are rarely of perfect quality. They may be degraded and corrupted due to variations in skin and impression conditions. Thus, image enhancement techniques are employed prior to minutiae extraction to obtain a more reliable estimation of minutiae locations. The goal of this paper is to represent a complete process of fingerprint feature extraction for minutiae matching [8].

Advantages

The finger print image enhancement techniques are employed prior to minutiae extraction to obtain a more reliable estimation of minutiae locations.

The goal of this paper is to represent a complete process of fingerprint feature extraction for minutiae matching.

Disadvantage

Assumption is not true for fingerprint images of poor quality

I. Authorization Mechanisms for Mobile Commerce Implementations

Mobile commerce (m-commerce) provides an exciting set of new capabilities that service providers can leverage to grow their revenue base while attracting new services that enhance the end-user experience. With these new opportunities the risk of new security threats that need to be addressed also arises. In this paper[4], security issues in particular, those dealing with service and subscriber authorizations in enhanced prepaid implementations for m-commerce is discussed. These products typically provide an enriched rating engine and a highly configurable feature set for service and content charging in wireless networks. Client application and subscriber-level authentication and authorization are key mechanisms that serve to regulate access to, and usage of content-based transactions in mobile commerce. Solution architectures and a discussion of authorization criteria are presented.

Advantage

Security issues in particular, those dealing with service and subscriber authorizations in enhanced prepaid implementations for m-commerce are discussed.

Disadvantage

Confidentiality is low because of Key mechanisms in regulated access.

III.IDENTIFYING AND DATA HIDING TECHNIQUES

User send all the it's relevant details to merchant. The information about the user that is stored in the merchant is sent to the Biometric server. Biometric servers send a request to the user for retrieving the information about the finger print. User response to the server by hiding the information using DWT algorithm. If the hided information about the finger print matches 60%-99%, then it moves to next process. Merchant request to the user for accessing the Pin Number. User sends the four digit Pin number to the remote server1 and remote server 2. The verification process done by remote server2after verification, remote server2 sends the "OK" message to bank. Finally bank release the amount to the merchant after all the verification process completed successfully

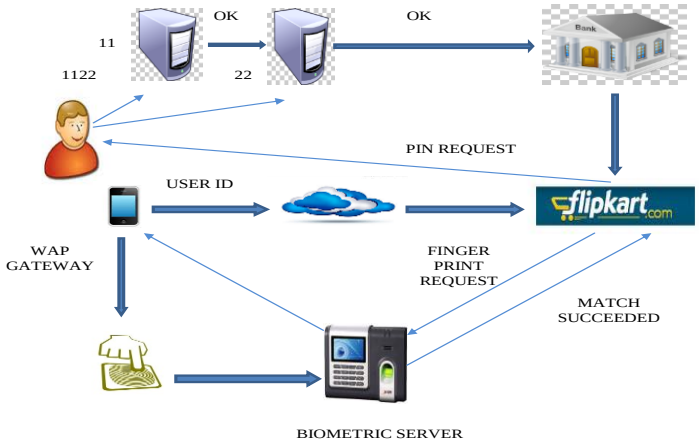

Figure 7: System Architecture .

A. Finger Print Identification

It is the method of identification using impression made by minute ridge formation or patterns found on finger tips. No two persons have exactly same arrangement of ridge patterns, due to distinctiveness, compactness and compatibility Minutiae based representation is used. Uniqueness of fingerprint is determined by local ridge characteristics and their relationship because it is an infallible means of personal identification.

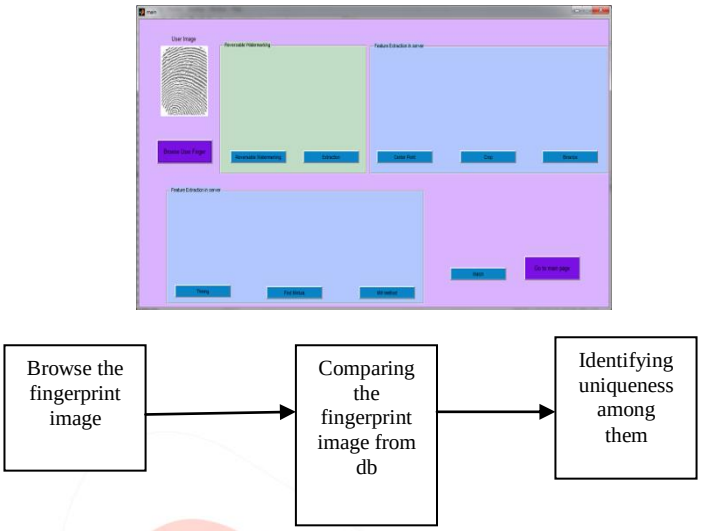

Figure 8: Finger Print Identification

B. Data Hiding Technique

Reversible data hiding is a technique where the original cover can be lossless restored after the embedded information is extracted. The user finger print is transferred to the biometric server in a secure way using DWT algorithm. DWT stands for "DISCRETE WAVELET TRANSFORM". DWT is used to improve data-hiding capacity and retain good stegno - image quality. The secret message is inserted directly into the pixels. Our proposed method is to embed secret data into the coefficients after quantizing and rearranged in the quantization factors using wavelet filter for a cover image, and to recover the original image.

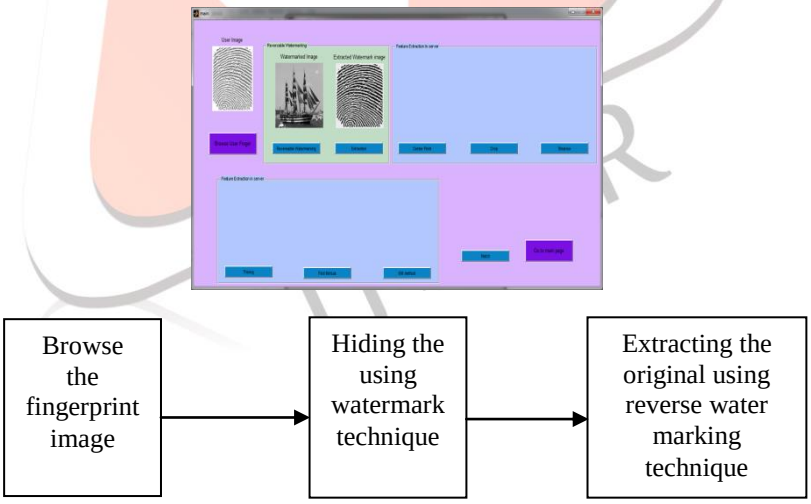

Figure 9: Data Hiding Technique

IV.EXTRACTION AND COMPARISON

A.Finger Print Extraction

Minutiae points are the locations where a ridge becomes discontinuous. A ridge can either come to an end, which is called as termination or it can split into two ridges, which is called as bifurcation. A number of techniques is been carried over in minutiae based finger print extraction. First stage is to find the centre point which is of region of interest and then cropping is carried out. After that Binarization is an effect which converts greyscale image to binary image by fixing the threshold value, pixel value above and below threshold value are said to be '0' and '1'. Binary image is thinned using Block filter to reduce thickness of all ridge lines to single pixel width to extract minutiae points effectively as in figure 4.

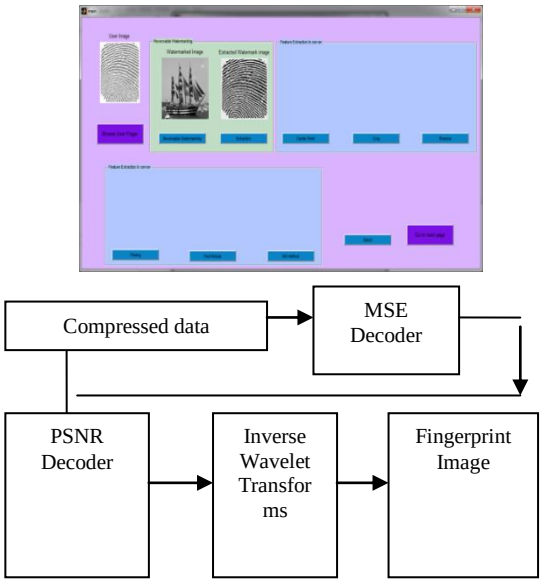

Figure 10: Discrete Wavelet Transforms (DWT) Decoder

B.Finger Print Comparison

Finger prints of customers will be recorded on a database for personal identification said to be known as the reference database. Finger prints of customers will be recorded on a database for personal identification said to be known as the reference database. Minutiae-based fingerprint matching system usually returns the number of matched minutiae on both query and reference fingerprint and uses it to generate similarity scores.

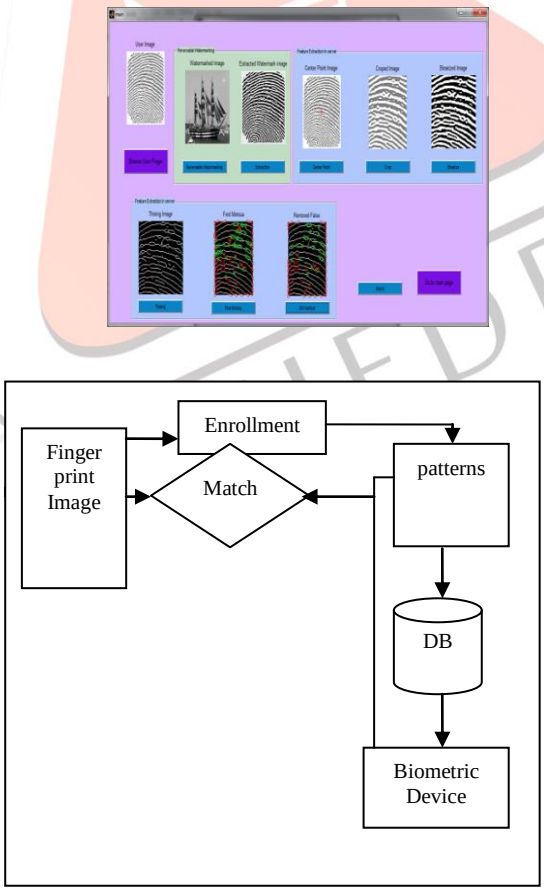

Figure 11: Fingerprint Matches

When two fingerprints have a minimum of 12 matched minutiae, they are considered to have come from the same. So the minutiae based comparison gives the accurate results in user authentication. Matrix format is used for efficient matching in minutiae as in figure.

C.Discrete Wavelet Transforms (DWT)

We propose an optimal discrete wavelet transform (DWT) based steganography. First decomposition is done on a host image and the secret information is hidden by manipulating the transform coefficients of the decomposed image. In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency *and* location information (location in time). He discrete wavelet transform has a huge number of applications in science, engineering, mathematics and computer science. Most notably, it is used for signal coding, to represent a discrete signal in a more redundant form, often as a preconditioning for data compression. Practical applications can also be found in signal processing of accelerations for gait analysis,[6] in digital communications and many others.It is shown that discrete wavelet transform (discrete in scale and shift, and continuous in time) is successfully implemented as analogy filter bank in biomedical signal processing for design of low-power pacemakers and also in ultra-wideband (UWB) wireless communications.

Pseudo code:

PSNR:

```
Function [out] = PSNR (pic1, pic2)
e = MSE (pic1, pic2);
m = max (max (pic1));
Out = 10*log((double(m)^2)/e);
End
```

MSE:

```
Function [ out ] = MSE( pic1,pic2 )
e = 0;
[m n] = size(pic1);
For i = 1: m
        For j = 1: n
         e = e + double ((pic1 (i,j)-pic2(i,j))^2)
End
Out = e/(m*n);
End
```

V.CONCLUSION AND FUTURE WORK

In this process deals in spite of the limitations of a mobile device, the user authentication scheme is highly effective and provides immense security. Effective fingerprint feature extraction algorithms Minutiae Maps is implemented for user authentication. User send the finger image to the biometric server by using discrete wavelet transform method and water marking techniques, finger image is hided.The user information i.e., Fingerprint is sent to the biometric server in a secure way using data hiding technique. For data hiding implemented Discrete Wavelet Transform (DWT) for security. PIN distribution to the payment transaction concept will explain in next Phase. .

REFERENCES

[1]K.Shanmugam, Dr.B.Vanathi, K.Ganesan**, Enhancing Secure Transaction and User Authentication Method Based On Fingerprint Mechanism Using Fuzzy Logic and Amalgam Encryption for PIN Distribution Process in M- commerce**.

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

[3] Chang-Lung Tsai Chun-Jung Chen,Deng-Jie Zhuang, **Secure OTP and Biometric Verification Scheme for Moblie Banking**,2012 IEEE.

[4] Chang-Lung Tsai Chun-Jung Chen, Deng-Jie Zhuang, **Secure and Biometric Verification Scheme for Mobile Banking,2012 IEEE.**

[5] Mangala Belkhede, Veena Gulhane, Dr. Preeti Bajaj, **Biometric Mechanism for enhanced Security of Online Transaction on Android system:** A Design Approach, Feb. 19~22, 2012 ICACT2012.

[6] Suzhen Wang, Lijie, **Fuzzy Logic in Biometrics**, Jan 2012, Journal Vol. 1.

[7] Vesselin TzvetkovArcor AG & Co.K¨olner Strasse 5, **WAP Protocol Security Solutions for Mobile Commerce**.

[8] Pankaj Bhowmik, Kishore Bhowmik, Mohammad Nurul Azam, Mohammad Wahiduzzaman Rony, **"Fingerprint Image Enhancement and it's Feature Extraction for Recognition"**, June 2012, Vol. 1.

[9]Meeker, Mary **Global Technology Internet Trends** Morgan Stanley, November 15,2005.

[10]Seema Nambiar,Chang-TienLu,Lily,R.Liang,"Analysis of Payment Transaction Security in M-commerce. Information Reuse and Integration", 2004, IRI 2004. Proceedings of the 2004 IEEE International Conference on PublicatioYear:2004,Page(s):475-480,Cited by: Papers (7) .

[11] MasterCard Inc.: (1997), **SET Secure Electronic Transaction Specification**, Book 1: Business Description, MasterCard Inc., May 1997.

[12] Pratiksha Y. Pawar and S. H. Gawande, Member, IACSIT,**Mobile commerce Security Using Random LSB Steganography and Cryptography,** International Journal of Machine Learning and Computing, Vol. 2, No. 4, August2012.

[13] Jerry Gao, Vijay Kulkarni, Himanshu Ranavat, Lee Chang, **A 2DBarcode-Based Mobile Payment system,** 2009 IEEE, DOI 10.1109/MUE.2009.62.