A SECURE ARCHITECTURE INVOKING FINGERPRINT, IRIS, DATA HIDING, ENCRYPTION TECHNIQUES FOR M-COMMERCE USERS

J.M.Vishnu Kumar[1],M.Yogeswaran [2], D.Uma M.E.,[3]

[1]*Student, Department of Electronics and Communication Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India.*

[2]*Student, Department of Electronics and Communication Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India.*

[3]*Assistant Professor, Department of Electronics and Communication Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India.*

ABSTRACT

This project delivers value added services to existing customers and creates new market opportunities. However, establishing a secure m-commerce platform that offers high level of service can be challenging. We propose a biometric-based authentication protocol with secure PIN distribution targeted at m-commerce applications. And a watermark is embedded in the captured biometric images. The embedding key of watermark is generated from mobile device parameters and is shared with the central server. M-Identity combines the identity of the mobile device into the biometric images. Only the genuine owner whose biometric information captured by his/her registered mobile device can pass m-identity authentication. Fingerprint biometrics is taken as an example, to show how secure it works. Also PIN distribution architecture design enhances the secure m-commerce applications. Mobile commerce is an emerging trend. Mobile commerce provides exciting opportunities for users to perform shopping , order food , m-Payments etc. This increasing in trend leads to security threads. This project is focused on user authentication service provider authentication and security. Existing system used for mobile payment services in handled devices doesn't involve biometric authentication. For IRIS recognition we use K-NN Classifier.

Keyword : *DWT- Discrete Wavelet Transform, K-NN Classifier,MM – Minutiae maps, OM- Orientation maps, PIN – Personal Identification Number*

---

1. INTRODUCTION

The mainstay of this project is to Purchase goods anywhere through M-Commerce applications with user authentication, Merchant authentication and Message authentication.

1.1 Mobility

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.

1.2 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 security like user authentication, merchant authentication, message authentication and building a complete solution for M-Commerce applications.

2. SYSTEM DESIGN

The User authentication, Merchant authentication and Message authentication is carried out in our proposed model where Biometric Server is provided for Finger print feature extraction of each customer subjected to online mobile shopping. An effective algorithm called Minutiae Matching and orientation map algorithms are selected for finger print feature extraction. The local ridges, terminations and bifurcations are accurately determined. The match succeeds after 12 similar matching of Query template with the storage template. The source for finger print feature extraction is the finger print of the user. The User Finger print is transformed to Biometric Server in a secure way using DWT algorithm. DWT stands for Discrete Wavelet Transform algorithm. Reversible Data Hiding technique is performed where the original cover can be losslessly restored after the embedded information is extracted. After User authentication PIN Distribution Architecture is provided. Research on implementing effective encryption algorithms among RC4, AES, DES, SDES, TWO FISH is been carried out

2.1 Advantages

- Reversible Data Hiding is used to improve Data hiding capacity and it retains good Stegno-image quality.
- Matrix format is **2**used for efficient matching in Minutiae.

2.2 System Architecture

The following are the steps

- Customer (user) sends the Product and customer details to the Service provider through the WAP gateway.
- Service provider verifies the Product & customer details and sends to the Biometric server through the WAP gateway.
- Biometric Server requests the customer details (Fingerprint & IRIS) to the customer.
- Customer sends the fingerprint & iris image and details to the Biometric server through the WAP gateway.
- Biometric server sends the Comparison result details to the Service provider. Analysing the matching score service provider decides access or denies the process of customer.
- Once the user is authenticated, the Pin distribution process is initiated based on the threshold level. OTP authentication is sent to the user by the service provider.
- After authentication process the user PIN (personal identification number) are send to the remote server 1 and remote server 2 in secure way.

- The result is sent to the bank for transaction process as an OK or Not OK message to the bank and bank will initiate the transactions.

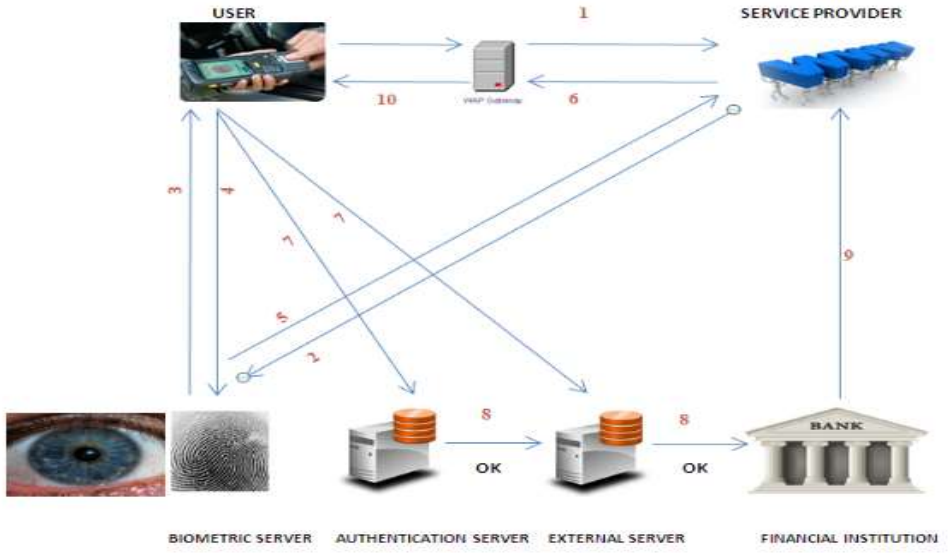

Fig -1: System Architecture

3. MODULE DESCRIPTION

For implementation the entire system has been divided into the following modules:

- Iris identification and matching
- Finger print identification and matching
- Data hiding technique using DWT
- PIN encryption and decryption

3.1 Iris identification and Matching

Iris Recognition is based on Circular Hough Transform. The captured eye image is preprocessed and the iris region is isolated from it which consists of iris/sclera boundary and iris/pupil boundary. Canny detection is used for detecting the edges after applying circular Hough Transform for calculating radius and center co-ordinates.

For testing the matching score of the input Iris data with the reference data at the server, K-NN classifier is used. The KNN classification algorithm predicts the test sample's category according to the K training samples which are the nearest neighbors to the test sample and judge it to that category which has the largest category probability.

Iris feature extraction is shown in Fig-2 and matching the input data with the reference data is shown in Fig-3 as obtained in MATLAB software.

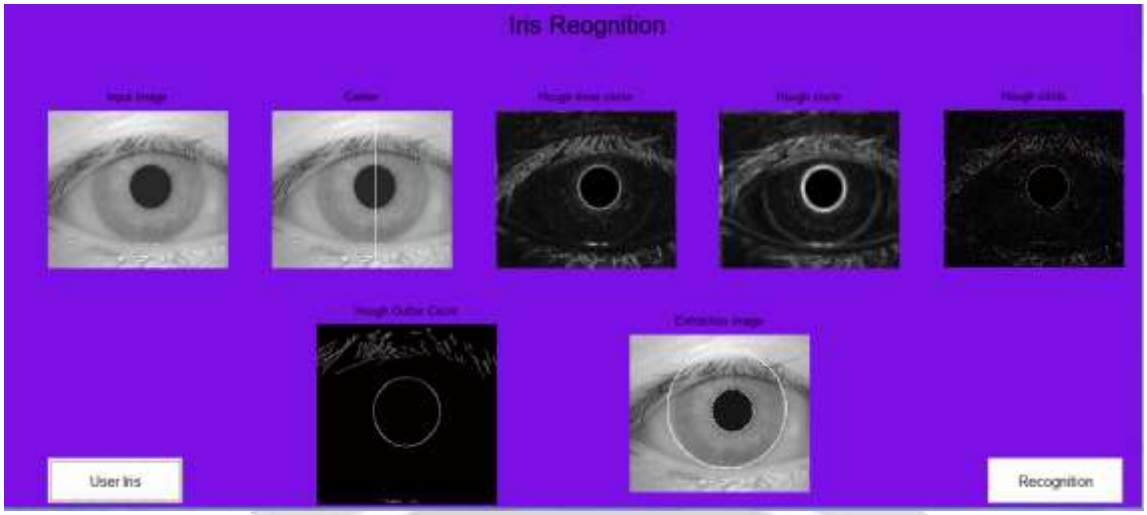

Fig -2: Iris Recognition

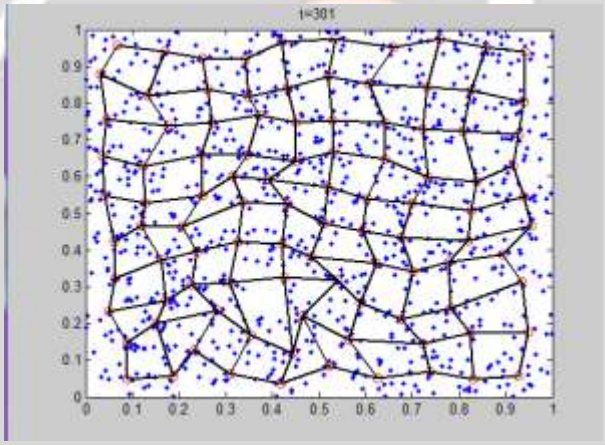

Fig-3: K-NN Classifier

3.2 Finger print identification and Matching

It is the method of identification using impression made by minute ridge formation or patterns found on finger tips. First stage is to find the center point which is of region of interest and then cropping is carried out. After that Binarization is an effect which converts grayscale 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.

Effective finger print extraction techniques MM, OM is used.

Minutiae Maps**:** Minutiae refer to the bifurcation or termination points of ridges on the finger surface. Two types of features are extracted from each sector: (1) the number of minutiae inside the sector, normalized by the total number of minutiae inside the largest circle, and (2) the average minutiae orientation within each sector**.**

Orientation Maps: Orientation maps describe the ridge flow in a fingerprint image. A square-shaped sub-region, centered at the core point, is used to form the feature vector. PCASYS algorithm is implemented which operates in the frequency domain. In this case, the frequency spectrum of each block is analyzed to determine the strongest orientation inside the block.

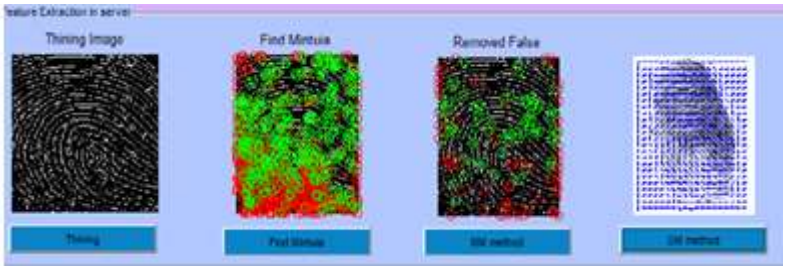

Fig-4: Finger Print feature extraction using MM and OM method

Number of Terminations: 58
Number of Bifurcations: 37

Table -1: Termination values

X	Y	Angle
1	25	1.00
65	1	92.00
1	110	1.00
127	1	137.00
1	146	1.00
160	1	222.00
2	169	2.00
175	2	181.00
2	199	17.00
180	17	199.00
18	44	18.00
91	19	218.00
20	116	23.00
180	31	143.00
32	106	36.00
28	36	139.00
40	168	48.00
146	52	104.00
54	98	55.00
227	58	1.00
58	88	59.00
45	62	227.00
69	157	73.00
228	74	12.00
78	1	79.00
60	80	118.00
84	15	90.00
213	91	233.00
97	145	98.00
18	102	1.00
102	180	107.00
221	108	49.00
110	96	119.00
100	121	20.00
125	27	126.00

201	131	44.00
137	226	137.00
233	138	30.00
138	61	

Table -2: Bifurcation values

X	Y	Angle 1	Angle 2	Angle 3
2	116	9.00	160.00	10.00
100	14	14.00	25.00	135.00
28	55	34.00	7.00	34.00
188	34	21.00	39.00	96.00
40	146	41.00	16.00	44.00
9	47	139.00	48.00	54.00
48	78	52.00	119.00	63.00
12	63	66.00	66.00	3.00
65	35	66.00	42.00	73.00
117	77	133.00	86.00	23.00
87	182	91.00	239.00	94.00
61	94	160.00	95.00	67.00
95	73	96.00	37.00	67.00
12	103	87.00	118.00	31.00
122	115	129.00	121.00	

3.3 Data hiding using DWT

The input user finger print is embedded in a duplicate image using DWT. DWT splits component into numerous frequency bands called sub bands known as LL – Horizontally and vertically low pass LH – Horizontally low pass and vertically high pass HL - Horizontally high pass and vertically low pass HH - Horizontally and vertically high pass Since Human eyes are much more sensitive to the low frequency part (LL sub band) we can hide secret message in other three parts without making any alteration in LL sub band.

3.3.1 Algorithm for Embedding Process

- Once image is loaded, apply skin tone detection on cover image. This will produce mask image that contains skin and non skin pixels.
- After this original image is also cropped of same area. Cropped area must be in an exact square form as we have to perform DWT later and cropped DWT.
- Apply DWT to only cropped area (Mc×Nc) not whole image (M×N).
- Perform embedding of secret data in one of subband we choose high frequency HH sub -band.
- Perform IDWT to combine 4 sub-bands. A cropped stego image of size Mc×Nc is obtained.

3.3.2 Extraction Process

Secret data extraction is explained as follows: 24 bit color stego image of size M×N is input to extraction process. We must need value of cropped area to retrieve data. All steps of Decoder are opposite to Encoder. Care must be taken to crop same size of square as per Encoder. By tracing skin pixels in HHH sub-band of DWT secret data is retrieved**.**

Fig-5: Input Image

Fig-6: Cover Image

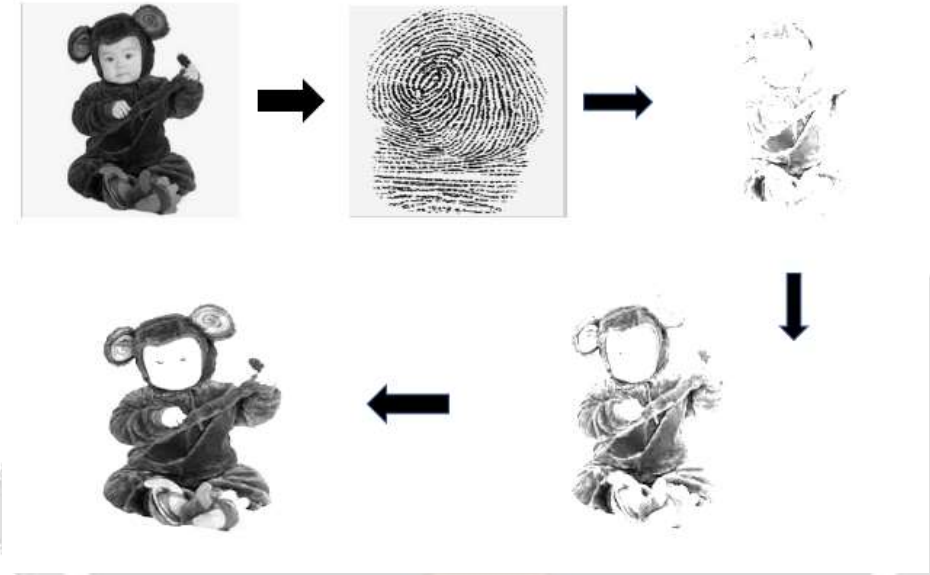

Fig-7: Data Hiding using DWT

Table -3: PSNR and MSE values

	VALUE	**EXTRACTION VALUE**
PSNR	188.8382	4.1222
MSE	7.2718e-09	46.5301

3.4 PIN encryption and decryption

Encryption and decryption is achieved by implementing RC4 algorithm. A variable-length key of from 1 to 256 bytes (8 to 2048 bits) is used to initialize a 256-byte state vector S, with elements S[0], S[1], …, S[255]. For encryption and decryption, a byte k is generated from S by selecting one of the 255 entries in a systematic fashion. As each value of k is generated, the entries in S are once again permuted.

The key-scheduling algorithm is used to generate the permutation array. The following actions are iterated 256 times after initializing i and j to 0:

• compute j = j + S[i] + key [i mod key length]

- swap S[i] and S[j]
- increment i

PIN is distributed to two different servers and the data is encrypted. Decryption takes place at bank server.

Fig-8: PIN Encryption

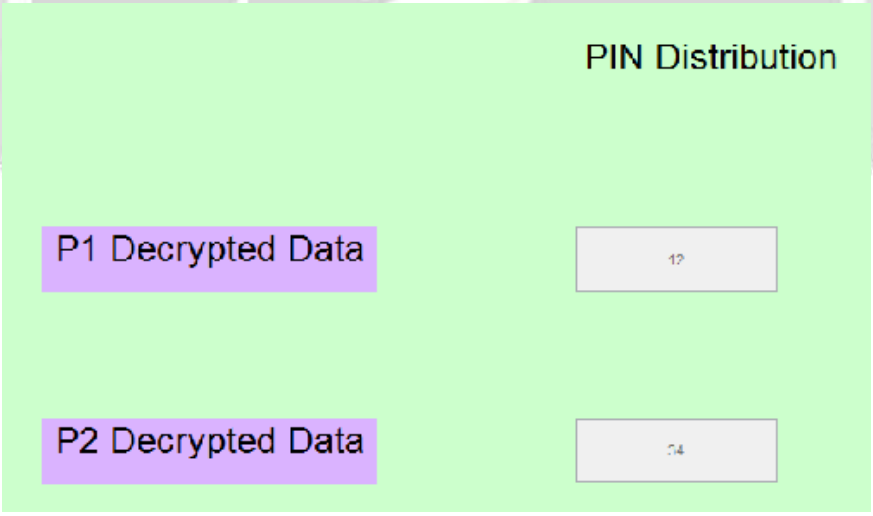

Fig-9: PIN Decryption

4. CONCLUSIONS

In spite of the limitations of a mobile device, the user authentication scheme is highly effective and provides immense security. The merchant's authentication makes sure the customer is transacting with the right person. Effective fingerprint feature extraction algorithms Minutiae Maps is implemented for user authentication. IRIS recognition is implemented using KNN classifier. The user information i.e., Fingerprint is sent to the biometric server in a secure way using data hiding technique. For data hiding we have implemented Discrete Wavelet Transform (DWT) for security. PIN distribution to the payment transaction concept will explain in next Phase.

5. REFERENCES

[1]. Arunprakash R., Mehata K.M. and Chellappan C., (2014), A Novel Hybrid Authentication Method Based On Orientation Maps and Server Aided Signature for M Commerce Secured Transactions, Journal of Theoretical and Applied Information Technology.

[2].Fengling Han and Ron van Schyndel, (2012), M-Identity and Its Authentication Protocol for Secure Mobile Commerce Applications, Springer, Cyberspace Safety and SecurityLecture Notes in Computer Science, vol: 7672, pp 1-10.

[3].Mangala Belkhede, venna Gulhane, Dr.preeti Bajaj, (2012), Biometric mechanism for enhanced security of online transaction on android system**,** ICACT.

[4].Morris Chang J., Joseph Williams, George Hurlburt, (2014), Mobile Commerce, IEEE computer society.

[5].Seth Earley, (2014), Earley & Associates, Mobile Commerce: A Broader Perspective, IEEE computer society.

[6].Uday Rajanna, Ali Erol and George Bebis, (2010), A comparative study on feature extraction for fingerprint classification and performance improvements using rank-level fusion, Springer, Pattern Analysis and Applications, vol. 13, Issue. 3, pp. 263-72.

[7].Vanathi B., Shanmugam, (2014), Enhancing secure transaction and user authentication method based on mixed fingerprint mechanism using fuzzy logic in m-commerce.