Asian Journal of Information Technology 15 (2): 232-242, 2016
ISSN: 1682-3915

A Secure M-Commerce Architecture for Service Provider to Improvize Quantity and Quality of the Products Using Fingerprint Authentication and Gender Classification

B. Vanathi, K. Shanmugam and V. Rymand Uthairaj
Department of CSE, Valliammai Engineering College, Chennai, Tamil Nadu, India

Abstract: This study focuses on an advanced mobile security system for M-commerce users to provide highly secured user friendly M-commerce transaction process. In previous researches propose security for M-commerce users invoking OTP. Also, there is analyzing system to identify the type of gender who uses the M-commerce application and forecast the demand in accordance. This study proposes finger print based biometric server extraction technique using Minutiae Map (MM) technique. In addition to that fingerprint from the user is sent in a secure way to the biometric server using Discrete Wavelet Transform (DWT). Every time a key is generated to authenticate the user from the service provider. Once the OTP is verified, user PIN is requested. The PIN is sent in a secure way using RC4 encryption algorithm. Also, gender classification is performed using Neural Network (NN). The fingerprint information is send to the service provider which improves the product quality and forecast the demand of the market. Gender classification done by ridge count, ridge thickness, White lines count and ridge count asymmetry and patterntype. Thus, our experimental results states NN provides improved accuracy in identifying gender classification.

Key words: M-commerce, discrete wavelet transform, gender classification, RC4 encryption, India

INTRODUCTION

People started using smart phones for accessing internets, downloading apps, sending and receiving mails, getting location based information and for online transactions (Bartunek *et al*., 2006). Online purchasing eases the work of people and also provides secure transactions. Mobile commerce (M-commerce) is a type of e-commerce technology, attracted billions of users over the past few years. M-commerce is an emerging technology where users can interact with the service providers through a mobile device with wireless network for information/service request, retrieval and transaction process. M-commerce is defined as "The delivery of trusted transaction services over mobile devices for the exchange of goods and services between consumers, financial institutions and merchants" mobile devices also have the potential to provide unauthorized users with access to corporate networks and to introduce viruses and other harmful software into these networks. M-commerce is subjected to several security vulnerabilities such as information, Clone, Hijacking, Malicious software (Malware) and phishing and wireless connection vulnerabilities.

Enabling high security and gender classification is considered as the success of M-commerce applications. Thus, implementing high security in M-commerce applications would invite many users to perform m-payment/transactions immediately and irrespective of infrastructures (Shanmugam and Vanathi, 2014).

In this study, we examine fingerprint based biometric authentication for performing M-payment like shopping, bill/bank payments, ticket booking, etc. To recognize a unique person, the human trait should be unique and not subject to change. Now a days, most banks and brokerages at firms provide mobile apps for their customers to support online banking and trading. In the existing system authentication, transaction and accessing mobile banking services are provided by password based authentication which is widely used for mobile commerce applications. The existing system is not secure because password based authentication is possible for the users to forget their password. This leads to a biometric authentication need for practically impossible to forget and cannot be forgotten or stolen, borrowed. User identification is very important and major issues in wireless services. Fingerprint authentication is widely used for user authentication process. 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

Corresponding Author: B. Vanathi, Department of CSE, Valliammai Engineering College, Chennai, Tamil Nadu, India

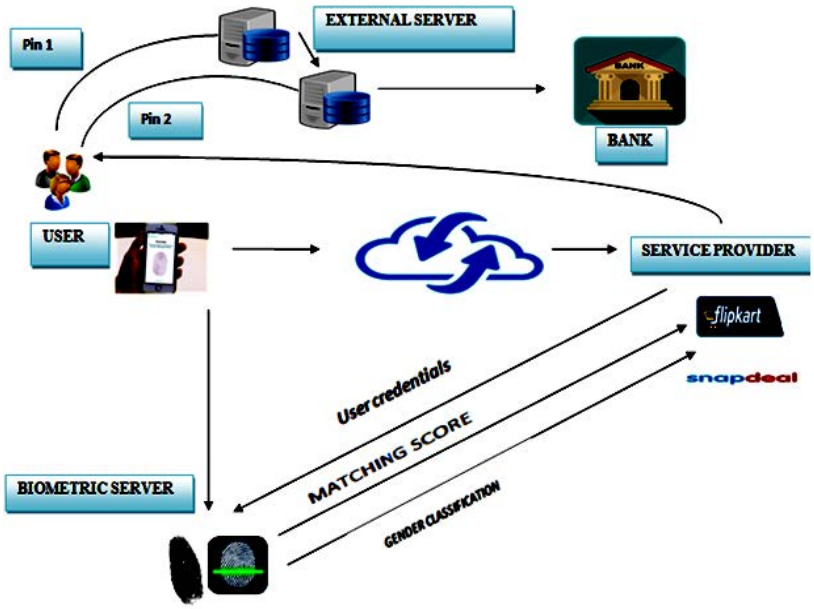


Fig. 1: Proposed M-commerce architecture

verify the claimed identity of one person by using comparison with only those templates corresponding his finger print. Using Discrete Wavelet Transform (DWT), the data is hide in a secure way and transferred to the biometric server. Biometric server uses MM fingerprint feature extraction techniques. In the biometric server, the decoding process is carried out and the matching score is analyzed. If the matching score is above the threshold value an OTP message is send to the user. Once the OTP is verified, user PIN is request is initiated for the transaction process. The user PIN is sent to the external server or bank in a secure way using RC4 encryption algorithm. Then transaction process by using QR code also available and also proposed the fuzzy logic is used for analyze the finger image. Security point of view WAP2.0 is best compare than WAP1.0. Mobile commerce process also analyze the more trends in internet security.

In this study, we propose gender classification in which the fingerprint is separated gender wise male/female this information is verified by the biometric server to avoid security issues for further process. This information improves the product quality and forecast the demand of the market for the service provider. Gender classification done by identifying the ridge count, ridge thickness, White lines count and ridge count asymmetry and pattern type. Many methodologies can be used for gender classification which are Fuzzy C-Means (FCM), Linear Discriminant Analysis (LDA) and Neural Networks (NN).

By comparing these methods, neural network gives more accuracy statistics and states Females have high ridge density and has less ridge count. Males have high ridge breath and has high count. Further, we study the statistical information with Ridge Thickness to Valley Thickness Ratio (RTVTR) and we stated that gender classification by neural network as the most accurate methods than LDA and FCM (Gornale *et al*., 2013) (Fig. 1).

Proposed system architecture: The user requests the product/service from the respective M-commerce service providers. Once, the request is placed, the user details are sent to the biometric server for user authentication (Shanmugam and Vanathi, 2014). On receiving the user credentials, user fingerprint is requested from the biometric server. The user sends the fingerprint using the biometric sensor integrated within the mobile phone. The fingerprint features are extracted using MM algorithm and the matching score is identified. The biometric server sends the matching score to the service provider. The service provider verifies the matching score with the thre shold value which is pre-defined. If the matching score is above the threshold value, the user is permitted to do transaction. The service provider sends an OTP to the respective user mobile number which was used during user registration. Once the OTP is verified, user PIN is requested. An effective PIN distribution technique has been proposed using two external servers. If the PIN verification is success the transaction is complete.

MATERIALS AND METHODS

Finger print feature extraction: Our previous research proposes a biometric finger print mechanism to secure the mobile payment also provides the security at the transmission level (Shanmugam and Vanathi, 2014). In this proposed research, our architecture uses fuzzy logic technique for comparison and if the fingerprint matching percentage is in the range of 60-99%, a Onetime Password (OTP) is automatically generated at server side. Else, the system will ask some security questions that are already stored in the database system during registration process. If the OTP is correct, SMS Authentication is generated. By using, the SMS authentication, only valid users will receive the SMS from the authentication server. After getting the SMS, a user can acknowledge with the choices (Yes/No). When the authentication server receives "YES" it knows that the user is valid and that the user has approved to initiate the transaction and if "NO" is the reply the user has denied the transaction. SMS confirmation is a final approval to initiate online payment transactions. The security of the system also depends on the security of the messages sent by SMS. The SMS and OTP are encrypted and protected with RC4 algorithm.

The proposed model for fingerprint feature extraction consists of three separate modules.The first method is fingerprint image, second method is reversible data hiding technique and Third method is fingerprint feature extraction.

Fingerprint image: The fingerprint image is captured using a biometric device integrated with the mobile phones. The fingerprint authentication, OTP and Message authentication is performed in the biometric server to all customers during online mobile shopping (Tsai *et al*., 2012). An effective algorithm called Minutiae Map (MM) algorithm is 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 user finger print is transformed to the biometric server in a secure way.

Watermarking techniques: The user fingerprint image is sent to the biometric server in a secure way using optimal Discrete Wavelet Transform (DWT) based steganography technique (Jiang *et al*., 1999). First decomposition is done on a host image and the secret information is hidden by manipulating the transform coefficients of the decomposed image (Tom *et al*., 2013).

The fingerprint image is hidden in a cover page using discrete wavelet Transform. The stego image quality is analyzed by MSE (Mean Square Error) and PSNR (Peak Signal To Noise Ratio):

$$PSNR=10\log_{10}(R^2/MSE)$$

$$MSE=\sum M,N\,[I_1(m,n)-I_2(m,n)]^2/M\times N$$

Where:

M and N = The numbers of row and columns in the input image
R = The maximum pixel value
I1 = The cover image and
I2 = The stego image

Fingerprint feature extraction: Many finger print extraction algorithms like OM (Orientation Map), MM (Minutiae Map), Core point detection, Gabor filter can be used for identifying fingerprint feature extraction. Among the feature extraction algorithms MM (Minutiae Map) is best algorithm because of its more accuracy. Before finding the minutiae, preprocessing techniques are implemented which are described below.

Preprocessing techniques

Histogram equalization: Histogram equalization increases the overall contrast of the images, especially when the usable data of the image is represented by close contrast values.

Binarization: A binary image is a digital image that has only two possible values for each pixel. Typically, the two colours used for a binary image are black and white though any two colours can be used. The colour used for the object in the image is the foreground colour while the rest of the image is the background colour. This means that each pixel is stored as a single bit is 0 or 1 and black and white.

Thinning: Thinning is a morphological operation that is used to remove selected foreground pixels from binary images, some what like erosionor opening. It can be used for several applications but is particularly useful for skeletonization. In this mode, it is commonly used to tidy up the output of edge detectors by reducing all lines to single pixel thickness. Thinning is normally only applied to binary images and produces another binary image as output (Bhowmik *et al*., 2012).

Feature extraction: In the proposed system, MM algorithm is proposed for fingerprint feature extraction

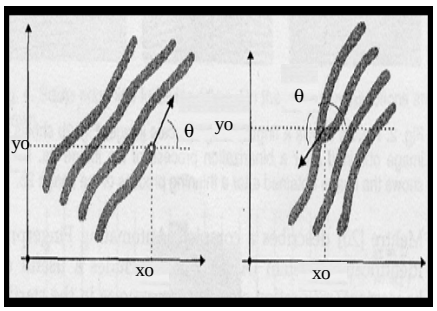


Fig. 2: Two types of minutiae, ridge ending and ridge bifurcation with their orientations

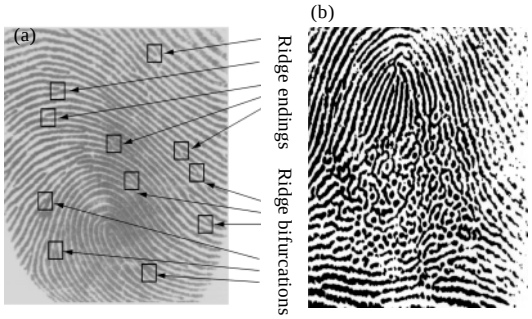


Fig. 3: a) Fingerprint images of poor quality; b) Minutiae overlaid on a fingerprint image

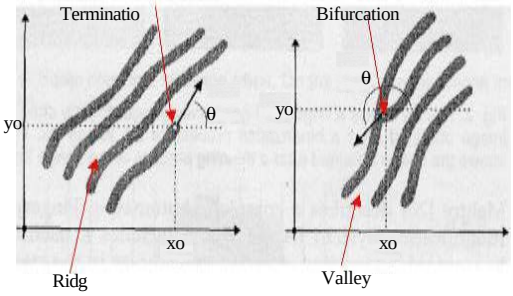


Fig. 4: Minutia types

Table 1: The CN for a pixel

Values	1	2
P4	P3	P2
P5	P	P1
P6	P7	P8

The input image is processed using MM method simultaneously and the output images are saved separately for each user.

Two kinds of minutiae are adopted for analyzing: ridge ending and ridge bifurcation (Fig. 2). For each minutia usually extract three features: type, coordinates and orientation. Figure 3 represents the where θ is the orientation and (x_0, y_0) is the coordinate of minutiae.

A minutia type consists of termination and bifurcation. 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. An excellent quality fingerprint typically contains about 40-100 minutiae. Poor quality of the fingerprint images shown in Fig. 3b in which ridge structures are completely corrupted.

For fingerprint feature extraction, we consider the white pixels as 1 and black pixels as 0. The algorithm uses 3×3 windows to scan the image and the bifurcation and termination in the final output image shall be represented by a dot. Also, the concept of Crossing Number (CN) is applied for extracting the minutiae (Ponnarasi and Rajaram, 2012) (Fig. 4). The CN for a pixel P is calculated as follows Table 1:

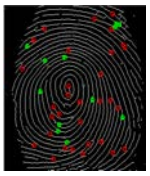
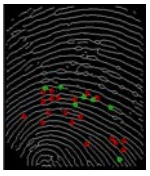
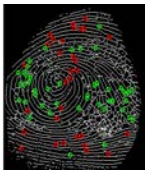
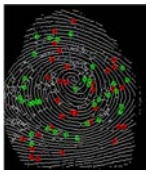
$$CN = \frac{1}{2}\sum_{i=1}^{|8} |P_i - P_{i+1}$$

where, P_i is the binary pixel value in the neighborhood of P with P_i = (0 or1) and P9 = P1. Based on the CN value, we can consider the minutiae point will have ridge ending or bifurcation.

Reversible data hiding: 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 technique. 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 (Zebbiche *et al*., 2006). (Table 2).

Gender classification algorithm: Fingerprint is a new identity potentially used for authentication. The proposed project proposal raises the quantity and quality of products based on gender preference. Many methodologies like Discrete Wavelet Transform (DWT), Fuzzy C-means Clustering (FCM), Linear Discriminate Analysis (LDA), Neural Network (NN) can be used for gender classification. The proposed architecture serves to provide a high level security because at each stage a more improved mechanism is introduced to ensure a complete reliable and secure transaction (Fig. 5 and 6).

Table 2: The MM algorithm performance on fingerprints and minutiae point extraction process

The fingerprint image	Minutiae image	Termination	Bifurcation	Total number of minutiae
		32	12	44
		22	7	29
		31	45	76
		35	33	68

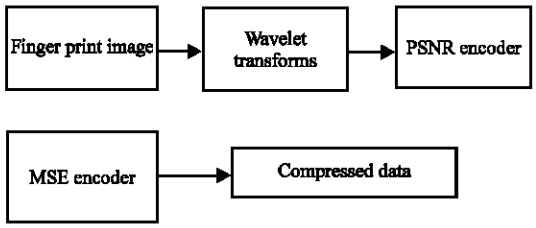


Fig. 5: Discrete Wavelet Transforms (DWT) encoder

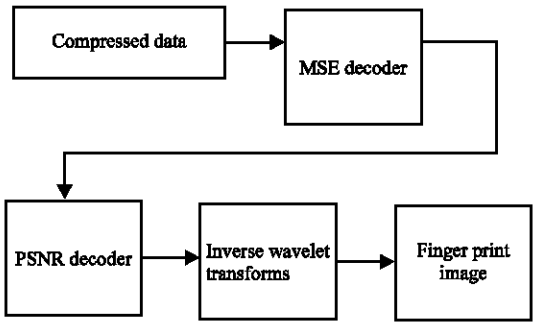


Fig. 6: Discrete Wavelet Transforms (DWT) decoder

Gender classification by using following factors (Bhowmik *et al*., 2012; Gornale *et al*., 2013).

Males:

- Males have a higher incidence of whorls
- Males have a slightly higher ridge count than females
- Males have higher ridge breadth
- Males have high ridge density and less ridge count

Females:

- Females have a higher incidence of loops
- Arches were found to be more frequent in females
- The females have a higher ridge thickness to valley (minutiae) thickness ratio than the males
- Females have higher ridge density
- Females fingerprints are significantly of lower quality than male fingerprints
- Females having higher white lines count and ridge count, ridge thickness to valley thickness ratio than the males
- Females have high ridge density and less ridge count

Blood groups:

- Blood groups A and B were found to be the most common among males
- Blood group O was the most commonly seen blood group in females
- A, B, AB and O blood groups persons have high frequency of loops, moderate of whorls and low of arches

- A blood group persons have more of loops
- AB blood group persons had more of whorls
- Whorls are more common in blood group O negative
- Loops and arches are seen in blood group

Mean: A fingerprint database or biometric server maintaining the finger image mean information about each filter image i and target image t_i is denoted as the following:

$$m_i = \{m_1, m_2, ..., m_n\}$$
$$mt_i = \{mt_1, mt_2, ..., mt_m\}$$

Variance: A fingerprint database or biometric server maintaining the finger image variance information about each filter image i and target image t_i is denoted as the following:

$$V_i = \{v1, v2,...,v_n\}$$
$$Vt_i = \{vt_1, vt2,...,vt_m\}$$

Contrast: A fingerprint database or biometric server maintaining the finger image contrast information about each filter image i and target image t_i is denoted as the following:

$$C_i = \{C1, C2,...,C_n\}$$
$$Ct_i = \{Ct_1, Ct2,...,Ct_m\}$$

Thickness: A fingerprint database or biometric server maintaining the finger image Thickness information about each filter image i and target image t_i is denoted as the following:

$$T_i = \{T1, T2,...,T_n\}$$
$$Tt_i = \{Tt_1,Tt_2,...,Tt_m\}$$

Interval: A fingerprint database or biometric server maintaining the finger image Interval information about each filter image i and target image t_i is denoted as the following:

$$I_i = \{I_1, I_2,...,I_n\}$$
$$It_i = \{It_1,It_2,...,It_m\}$$

Singularity: A fingerprint database or biometric server maintaining the finger image singularity information about each filter image i and target image t_i is denoted as the following:

$$S_i = \{S_1, S_2,...,S_n\}$$
$$St_i = \{St_1,St_2,...,St_m\}$$

Minutiae: A fingerprint database or biometric server maintaining the finger image minutiae information about each filter image i and target image t_i is denoted as the following:

$$M_i = \{M_1, M_2,...,M_n\}$$
$$Mt_i = \{Mt_1,Mt_2,...,Mt_m\}$$

Based on these sets to find out the mean values, variance, contrast, thickness, interval values, singularity, minutiae vales and also find out the mean fitness, Variance fitness, contrast fitness, thickness fitness, Interval fitness, singularity fitness and minutiae fitness:

$$Mf_i=(\{M_1-Mt_1\},\{M_2-Mt_2\},...\{M_n-Mt_n\})\times weight(W_1)$$
$$Vf_i=(\{V_1-Vt_1\},\{V_2-Vt_2\},...\{Vn-Vt_n\})\times weight(W_2)$$
$$Cf_i=(\{C_1-Ct_1\},\{C_2-Ct_2\},...\{C_n-Ct_n\})\times weight(W_3)$$
$$Tfi=(\{T1-Tt_1\},\{T_2-Tt_2\},...\{T_n-TMt_n\})\times weight(W_4)$$
$$If_i=(\{I_1-Itl\},\{I_2-It_2\},...\{I_n-It_n\})\times weight(W_5)$$
$$Sf_i=(\{S_1-St_1\},\{S_2-St_2\},...\{S_n-St_n\})\times weight(W_6)$$

$$Minutiaef_i=\left(\{Min_1-Mint_1\}\right),\{Min_2-Mint_2\},... \left(\{Min_n-Mint_n\}\times Weight(W_7)\right)$$

Fingerprint image fitness:

$$F_{f(i)} = Mf_i + Vf_i + Cf_i + Tf_i + f_i + Sf_i + Minutiaefinger$$

Classification: A multi-layer back propagation neural network was used for the gender classification analysis. We used the RTVTR and the white lines count features as the inputs for the neural network. Add in gasymmetry and/or concordance features was found to decrease the classification performance significantly. This is due to the fact that these features do not show significant statistical variations between males and females (Ponnarasi and Rajaram, 2012).

The variation among females and males in the membership of the fingerprints to the different pattern types and the average ridge count for fingers belonging to each pattern type are very small and thus are statistically insignificant. Male's and female's finger prints are characterized by a naver age right ward a symmetry in the ridge count, i.e., the ridge count of a finger in the right hand is most likely greater than the ridge count of its corresponding finger in the left hand but the re is no significant difference in the degree of a symmetry between males and females and thus, the a symmetry is not a good candidate for the classification process. The pattern type concordance between left and

right corresponding fingers doesn't show significant statistical variations between females and males. We found that the most significant features are: the RTVTR and the white lines count averaged over the individual's fingerprints with the females having higher white lines count and RTVTR than the males. These two features have shown high significance in the classification process using FCM and neural networks classifiers. Neural network classifier has a higher classification rate than Linear Discriminant Analysis (LDA). The average ridge countis slightly high er in males than in females with high standard deviation among subjects of both genders. We found that adding this feature to the white lines count, and RTVTR slightly improves the performance of the classification process using neural network and LDA while it degraded the performance of the Fuzzy C-Means (FCM) classifier.

RESULTS

The fingerprint feature extraction and reversible data hiding is carried out using Matlab v6.5.0. Figure 7 and 8 shows the GUI to perform fingerprint feature extraction and reversible data hiding. The process of fingerprint feature extraction, reversible data hiding and gender classification is described. Figure 9-17 describes the preprocessing techniques/process for fingerprint feature extraction.

Fig. 7: GUI for fingerprint feature extraction and reversible data hiding

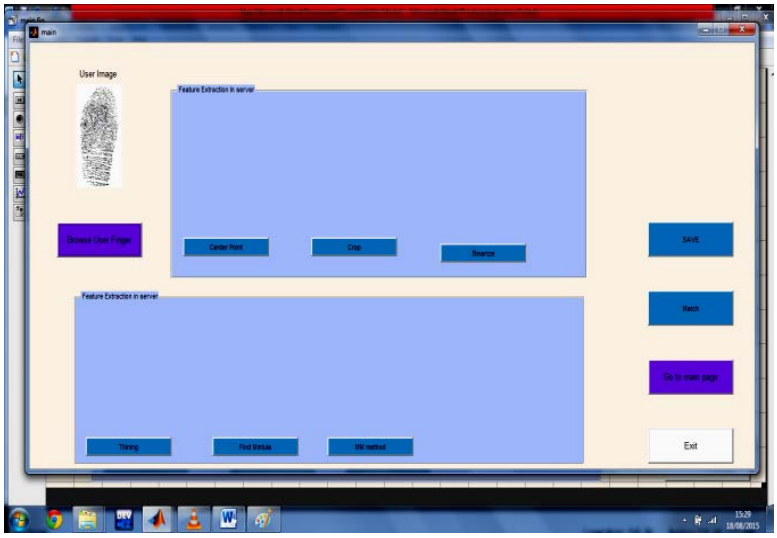


Fig. 8: Input fingerprint image

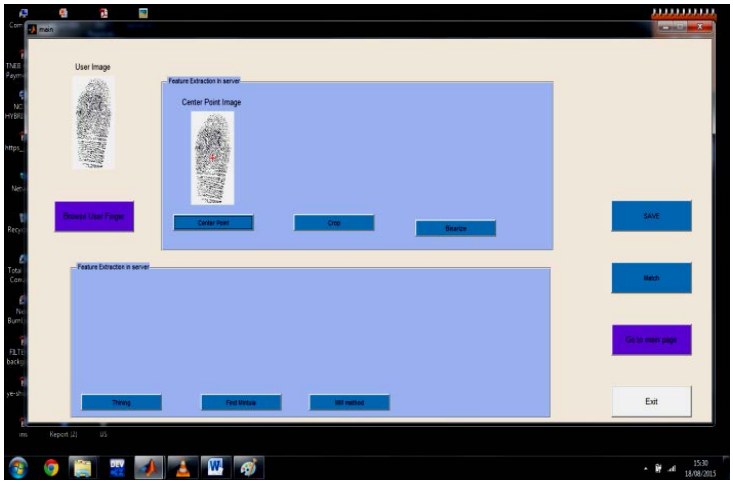


Fig. 9: Center point identification

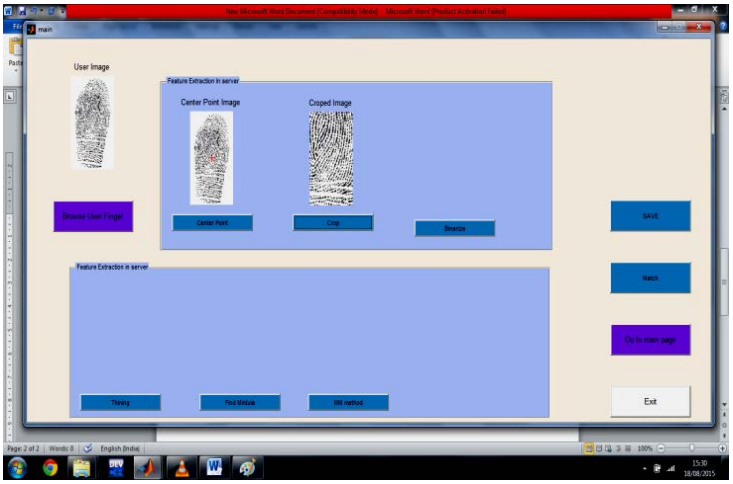


Fig. 10: Cropping

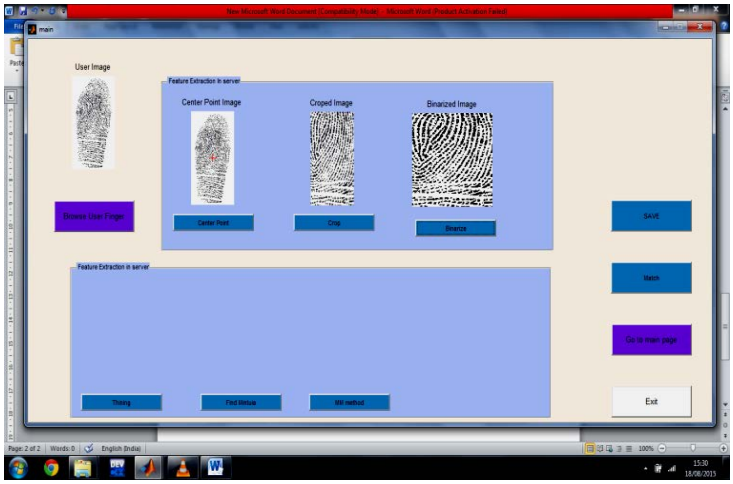


Fig. 11: Binarization

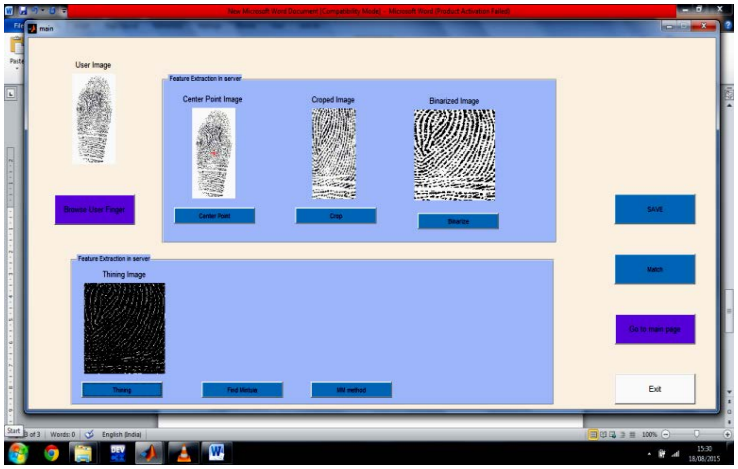


Fig. 12: Thinning

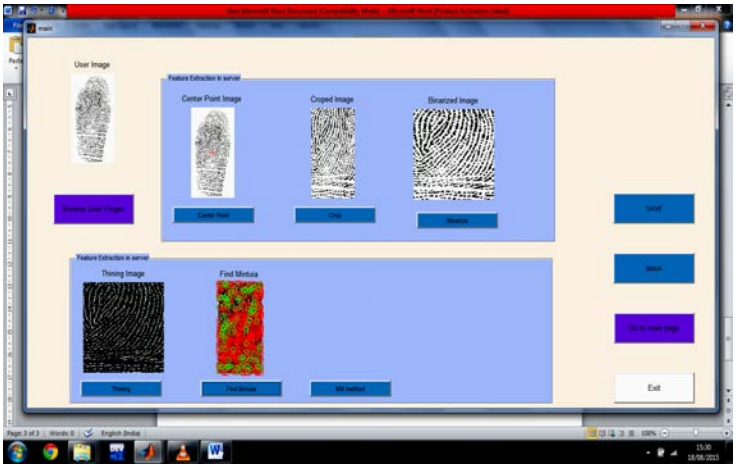


Fig. 13: Minutiae extraction

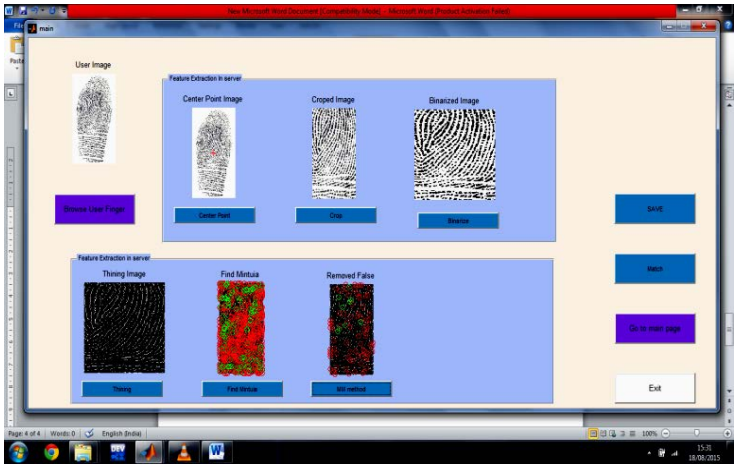


Fig. 14: False minutiae removal using minutiae map technique

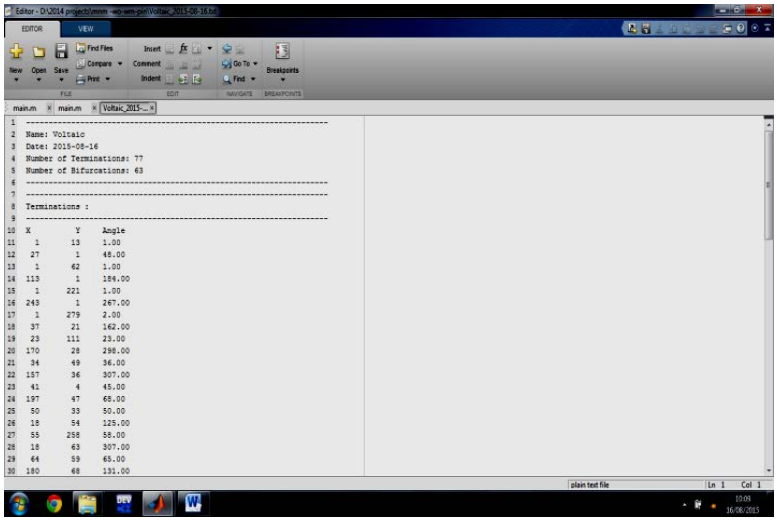


Fig. 15: Bifurification and termination values for the input fingerprint image

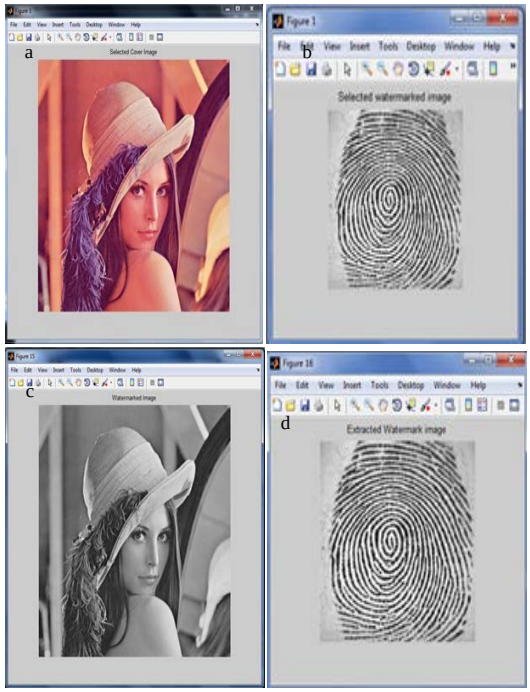


Fig. 16: a) Cover Image; b) Input image; c) Stego image; d) Extracted image

Fig. 17: Gender classification process

CONCLUSION

In this study, we have proposed a secure fingerprint based biometric authentication for M-commerce applications. For fingerprint feature extraction, we have implemented MM algorithm. The bifurcation and termination values are stored in the database during user registration. The matching is performed using fuzzy logic technique. The fingerprint from the user is sent to the biometric server using DWT technique. DWT provides improved MSE and PSNR value. The proposed architecture includes gender classification using neural network. Gender classification from fingerprint is accurate and useful to identify/predict the demand by male/female. Once the user fingerprint matching score is above the threshold value of the system an OTP is sent to the user registered contact number. If the OTP process is success, PIN distribution technique is initiated. PIN distribution technique will be explained in next phase.

REFERENCES

Bartunek, J.S., M. Nilsson, J. Nordberg and I. Claesson, 2006. Neural network based minutiae extraction from skeletonized fingerprints. Proceedings of the IEEE Region 10 Conference on TENCON 2006, November 14-17, 2006, IEEE, Hong Kong, pp: 1-4.

Bhowmik, P., K. Bhowmik, M.N. Azam and M.W. Rony, 2012. Fingerprint image enhancement and it's feature extraction for recognition. Int. J. Sci. Technol. Res., 1: 117-121.

Gornale, S.S., C.D. Geetha and R. Kruthi, 2013. Analysis of fingerprint image for gender classification using spatial and frequency domain analysis. Am. Int. J. Res. Sci. Technol. Eng. Math., 1: 46-50.

Jiang, X., W.Y. Yau and W. Ser, 1999. Minutiae extraction by adaptive tracing the gray level ridge of the fingerprint image. Proceedings of the 1999 International Conference on Image Processing, 1999 ICIP 99, October 24-28, 1999, IEEE, Kobe, Japan, pp: 852-856.

Ponnarasi, S.S. and M. Rajaram, 2012. Impact of algorithms for the extraction of minutiae points in fingerprint biometrics. J. Comput. Sci., 8: 1467-1472.

Shanmugam, K. and B. Vanathi, 2014. A novel secure transaction and identity endorsement in m-commerce. Int. J. Eng. Dev. Res., 2: 186-195.

Tom, R.J., T. Arulkumaran M.E. Scholar, 2013. Fingerprint based gender classification using 2D discrete wavelet transforms and principal component analysis. Int. J. Eng. Trends Technol., 4: 199-203.

Tsai, C.L., C.J. Chen and D.J. Zhuang, 2012. Secure OTP and biometric verification scheme for mobile banking. Proceedings of the 2012 Third FTRA International Conference on Mobile, Ubiquitous and Intelligent Computing (MUSIC), June 26-28, 2012, IEEE, Vancouver, BC, pp: 138-141.

Zebbiche, K., L. Ghouti, F. Khelifi and A. Bouridane, 2006. Protecting fingerprint data using watermarking. Proceeding of the First NASA/ESA Conference on Adaptive Hardware and Systems AHS 2006, June 15-18, 2006, IEEE, Istanbul, Turki, pp: 451-456.