VOL. 11, NO. 13, JULY2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

AN EFFICIENT CLUSTERING FORMULATION FROM RESEMBLANCE IN EXTANT ALGORITHMS

Mohana Prasad K.[1], R. Sabitha[2] and Oviya[1]
[1]Department of Computer Science Engineering, Sathyabama University, Chennai, India
[2]Department of IT, Jeppiaar Engineering College, Chennai, India
E-Mail:mohanaprasad1983@gmail.com

ABSTRACT

Mobile commerce is an emerging trend. Mobile commerce provides exciting opportunities for users to perform shopping, order food, m-payments etc. This increasing trend leads to security threats. This paper is focused on user authentication, service provider authentication and security. User authentication is performed by using finger vein based biometric methodology. Existing system used for mobile payment services in handheld devices doesn't involve biometric authentication. Hence leading to misuse and confusion among m-commerce users. Our proposed system is focused on finger vein authentication system (FVAS) for user authentication. The finger vein obtained is matched with the database using fuzzy logic system to obtain the matching score. If the matching score is above the threshold value PIN distribution process is initiated. Thus this paper looks to provide time efficient, high secure solution for m-commerce users and bring new m-commerce users to this vertical.

Keywords: M-Commerce, clustering, gabor filter, PIN distribution.

INTRODUCTION

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" (R. Arunprakash *et al*., 2014).

M-commerce is subjected to several security vulnerabilities such as Theft/Loss of device and information, Clone, Hijacking, Malicious software (Malware), Phishing, and Wireless connection vulnerabilities (R. Arunprakash *et al*., 2014).

Mobile access is an important factor. Our system should ensure only authorized person are allowed to access the device and enable security for m-commerce applications.

Enabling high security 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.

In this paper, we propose an effective finger vein authentication system for permitting only the authorized individual to access the m-commerce applications. Finger vein is considered to be very secure and reliable when compared with other biometric systems.

Face recognition big threat is illumination change. This might allow unauthorized user to authenticate sometimes. Fingerprint authentication is the user friendly and feasible authentication. But this is vulnerable to forgery because they are easily exposed to others. Also in sweat and dryness condition it is difficult to obtain a clear pattern for feature extraction and matching (Uday Rajanna, 2010).

Finger vein authentication uses pattern recognition. All handheld devices are provided with vein authentication sensor for obtaining the user finger vein for recognizing the pattern. Finger vein is unique and difficult to forge and copy. This user authentication can be used during login and session management (session is expired).

Thus designing and implementing secure m-commerce architecture with finger vein authentication system and PIN distribution technique is considered one of the best solution for increasing the confidentiality among m-commerce users.

RELATED WORKS

Recent study states by the year 2017, 3 billion smartphones and 1 billion tablets will be used by the users globally. Also the online retail sales through mobile devices will grow from 11% to 25% by the year 2017 (Seth Earley, 2014).

Mobile commerce has emerged and acquired many users in the last five years. In fact, Bank of America estimates US $67.1 billion transactions will be done using mobile devices by the year 2015. Now, even banks and trading firms developed mobile apps to support online banking and trading. The main driver for online commerce is to provide strong security practices (J.Morris Chang *et al*., 2014)

Examining finger vein can be found in this paper details the working principle of finger vein authentication. Also it defines finger vein is a new biometric method obtaining vein patterns. Vein patterns are different and unique among each person.

Several biometric methodologies are vulnerable to spoof attacks. This involves fake fingerprint, static face images can be employed in the database to duplicate the individual. [1] To prevent few methods like electrical

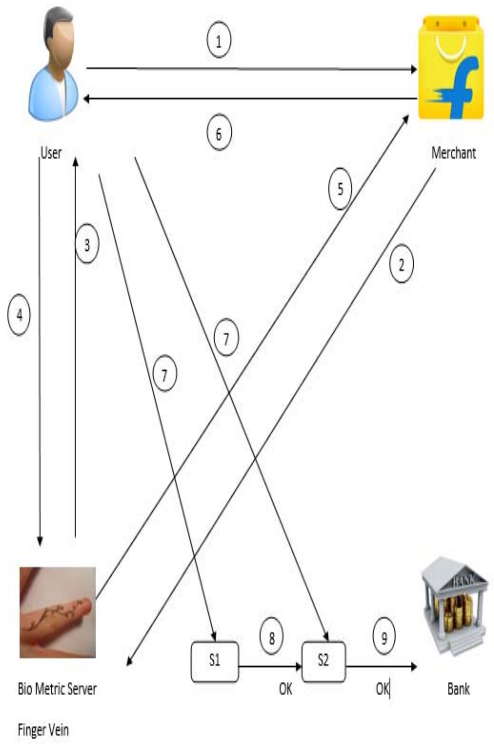
impulse, percentage of oxygen-saturated hemoglobin in the blood can be proposed.

The finger vein can be obtained from near-infrared or thermal-infrared based techniques. Thermal infrared based technique is not economically feasible. Hence near-infrared technique is feasible. Also ultrasonic scanning, X-ray imaging could provide valuable finger image data to identify each personal.

The finger vein pattern can be recognized using normalized cross correlation [3].

The secure pin distribution is discussed in Improved Pin Distribution Techniques in m-commerce System (R. Arunprakash*et al*., 2011). This paper states high security in m-commerce application is achieved by using a more secure WAP gateway by framing double encryption model. The pin will be split into two half's and encrypted send to two servers. In the server side the pin will be decrypted and checked for matching score. If the matching score is good an acknowledgement message stating OK will be passed to the other server and finally the transaction is initiated.

PROPOSED SYSTEM



Finger vein

Feature extraction techniques

We use Gabor filter, for finger vein extraction, since it is found to be the most appropriate technique. Gabor filter helps in providing the highest response at edges and also points the texture change when applied to an image.

Gabor filter's general format is

$$R(a,b,f,\varphi) = \frac{1}{2\pi\sigma_a\sigma_b}\exp\left[\frac{-1}{2}\left(\frac{a\varphi^2}{\sigma_{a^2}}+\frac{b\varphi^2}{\sigma_{b^2}}\right)\right]\cos(2\pi f a_\varphi)$$

Here $\begin{bmatrix} a & \varphi \\ b & \varphi \end{bmatrix} = \begin{bmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix}$

Where φ is the orientation of the Gabor filter, f is the frequency of the sinusoidal wave (Fengling Han*et al*, 2012)

To trace the line along the vein pattern we use repeated line tracking method. Until the vein pattern is obtained, the process is repeated. While tracking the vein pattern, a starting point is noticed for every iteration; from that starting point the vein pattern is obtained.

The labeling of the pixels in the image is done using local binary pattern (LBP). LBP provides a discriminative power and computational simplicity hence it is used in finger vein extraction.

A high-dimensional data is reduced to fewer dimensions by using dimensionality reduction method. The variance in the lower dimensional data is kept maximized using principal component analysis.

The contrast in the finger vein is enhanced by spreading frequent intensity values which is performed through histogram equalization.

The fuzzy sets are used to represent uncertainty and imperfection in the finger vein. The final process is the matching of the finger vein, which helps in identifying the genuine vein of the user. For effective classification, Fuzzy technique has been proposed to identify the respective user finger vein.

Once the authentication is passed, PIN distribution technique is initiated. If the authentication is failed, the user will be automatically logged out [Sudha*et al*, 2012].

Data hiding

In the reversible watermarking process, the dataset are hidden into images by using Discrete Wavelet Transform(DWT) algorithm. The DWT algorithm undergoes three level process where the given data is completely hidden behind the image and even the shadow of the image is not visible. The extraction process is done by IDWT (Inverse Discrete Wavelet Transform) algorithm. The DWT algorithm produces PSNR (peak signal to noise ratio) and MSE(the mean square error) values, which helps to identify that data hiding process is done and to also find the accurate ratio values of the hidden data. The DWT algorithm helps to perform faster hiding and extraction process. The watermarked image changes into a grey scale image after the hiding process. Reversible watermarking process produces high security while transferring the data from the customer to the merchant.

PIN distribution

The pin distribution process is done after user authentication. RC4 algorithm is used in this process. RC4

algorithm is a stream cipher. RC4 algorithm is faster than AES, DES, 3DES, SHA algorithms. AES algorithm is a block cipher in which the data are been transmitted block by block. Since our domain is m-commerce, time plays an important role. Hence RC4 algorithm has been implemented.

In the pin distribution process, the given 4 digit pin is split into pairs. The first 2 digits are sent to server1 and after the authentication process is completed, server 1 generates a message "ok" or "not ok". If the generated message is "ok", the message is sent to server 2, where it verifies the message from server 1 and also the other 2 digits. Then server 2 passes an acknowledgement message "ok" to the bank initiating for transaction.

EXPERIMENTAL RESULTS

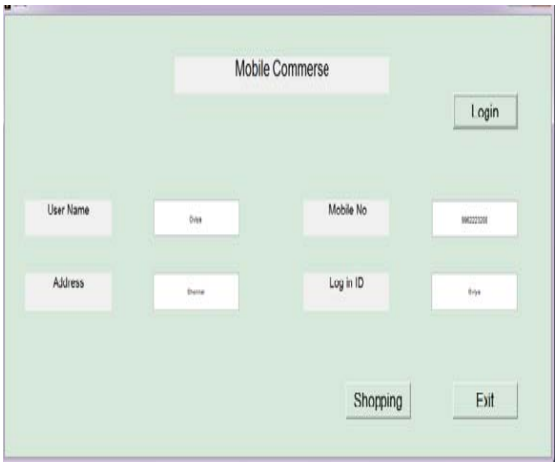


Figure-1. User authentication.

Figure-2. Vein input image.

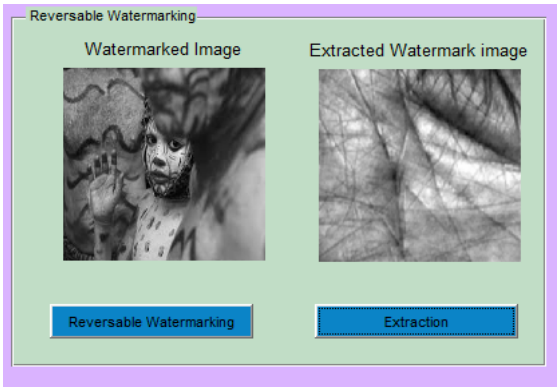


Figure-3. Reversible data hiding and embedding using DWT.

The image is hidden using reversible data hiding and this process uses DWT algorithm. This generates the PSNR and MSE value which confirms the performance of embedding. The extraction process is done using IDWT algorithm.

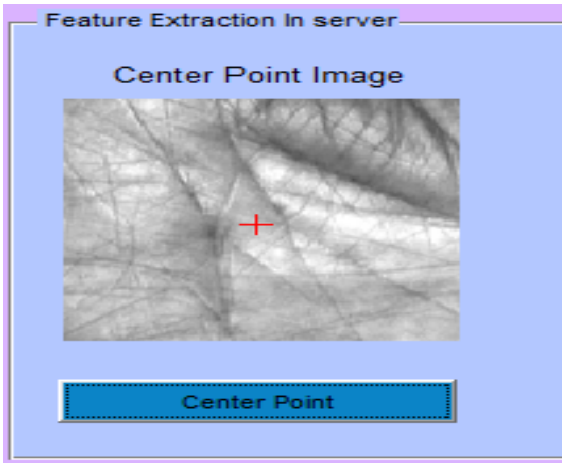


Figure-4.ROI detection.

This process is used to detect the center part of the vein, so extraction of the center point is obtained.

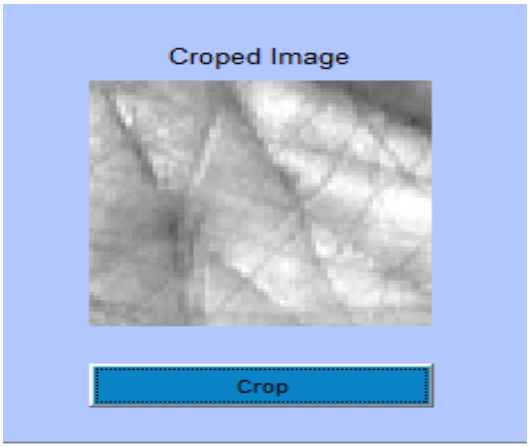


Figure-5. Cropped image.

The cropped image helps to detect the ROI (Region of Interest). Even if the finger is placed at any position,this helps to detect the user vein.

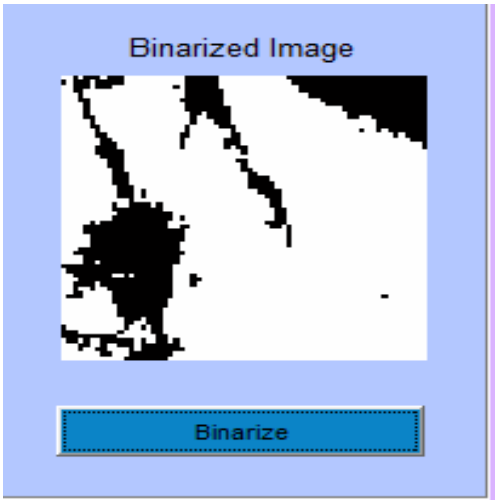


Figure-6. Binarization.

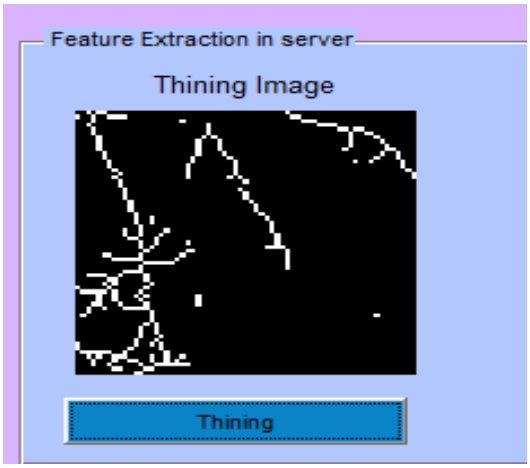


Figure-7. Thinning.

After the binarization process the output is converted into a skeleton image, which helps in the easy detection of ridges.

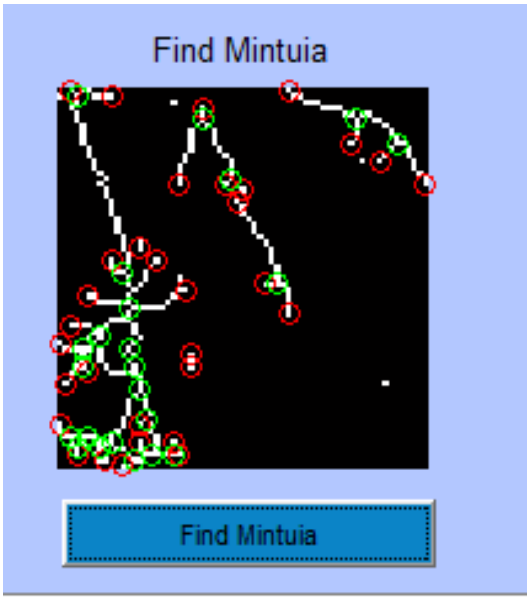


Figure-8. Minutiae detection.

The minutia value generates two values:

i) Bifurcation- identifies the joining of ridges.
ii) Termination- identifies the start and end point of the ridges.

This helps in easier process of recognition.

Figure-9. False minutiae detection.

This process removes the additional data which are not required for the process.

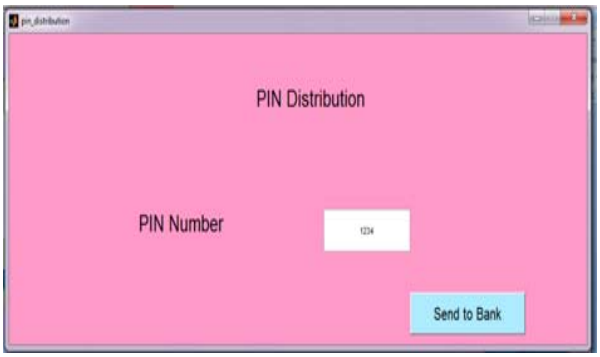


Figure-10. User PIN initiation.

The pin is sent to the bank for verification.

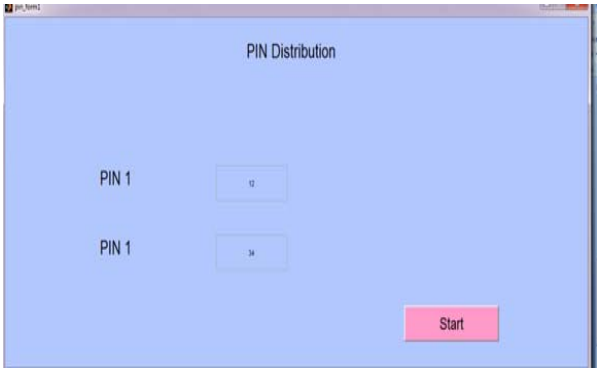


Figure-11. PIN distribution.

The pin is divided into two and the first half is sent to server1 and the second half is sent to server2.

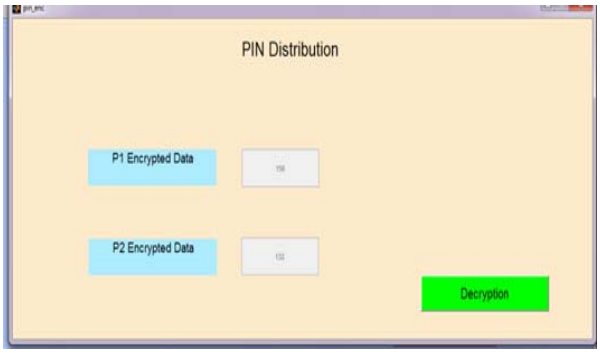


Figure-12. PIN encryption using RC4 algorithm.

The divided pin is encrypted using RC4 algorithm. This process is done for the secure transaction of the pin.

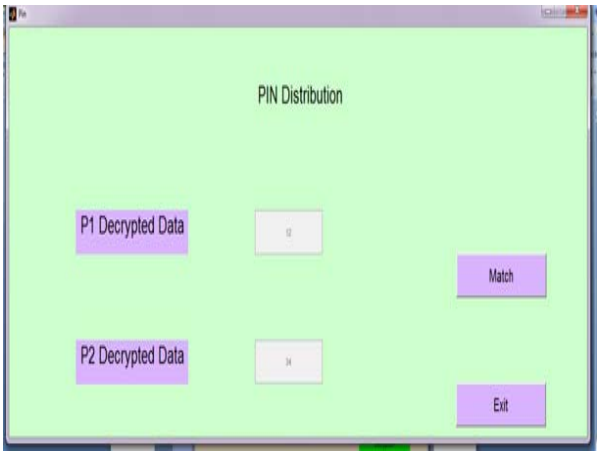


Figure-13. PIN decryption using RC4 algorithm.

Figure-14. PIN verification.

The decrypted pin is verified by the bank and if the pin number matches,it executes a message "Pin number perfectly matched".

CONCLUSIONS

User authentication is important in M-commerce applications to ensure the communicating entity is the exact user and our proposed architecture ensures using finger vein analysis. The finger vein analysis is effectively performed by fusion of two algorithms namely Gabor filter and orientation maps (OM). By fusing and implementing both algorithms the finger vein process is more accurate and effective. Also the finger vein is sent to the biometric server through WAP gateway in a secure way using DWT data hiding technique. The extraction is implemented using IDWT. PSNR and MSE values are been analyzed. To add more security we introduce secure PIN distribution process using our proposed PIN distribution architecture, OK message concept and RC4 encryption algorithm for message authentication.Thus the proposed architecture ensures complete reliable and secure transaction for m-commerce users.

REFERENCES

[1] R.Arunprakash, K.M.Mehata and C.Chellappan. 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. 7672: 1-10.

[3] Seth Earley. 2014. Earley and Associates, Mobile Commerce: A Broader Perspective, IEEE computer society.

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

[5] UdayRajanna 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. 13(3): 263-72.

[6] Sudha S. Ponnarasi and M. Rajaram. 2012. Impact of Algorithms for the Extraction of Minutiae Points in Fingerprint Biometrics.Journal of Computer Science. 8(9): 1467-72.

[7] K. Mohana Prasad, Dr. R. Sabitha. Meta Physical Algorithmic Representation for Flawless Clustering. Journal of Theoretical and Applied Information Technology (JATIT), ISSN: 1992-8645, 76(1): 82-87.

[8] k.mohanaprasad, Dr. R. Sabitha. Evolution ofan Algorithm for Formulating Efficient Clusters to Eliminate Limitations. International Journal of Applied Engineering Research (IJAER), ISSN 0973 - 4562, 9(23): 20111-20118.

[9] Ø K. Mohana Prasad, Dr. R. Sabitha. 2015. Yoking of Algorithms for Effective Clustering. Indian Journal of Science and Technology, ISSN: 0974-6846, Vol. 8(22), IPL0269. pp. 1-4.