

To Increase The Recognition Accuracy of Biometric System Using Fusion Technique In Mobile Transactions

Chavi Ralhan¹, Aseem Kumar², Rohit Saini³

School of Computer Science & Engineering

Lovely Professional University, Phagwara, Punjab, India

Abstract— in our study related to the mobile commerce we analyses that mobile commerce proves to be an efficient technique for buy or selling the products online by using mobile devices. One can perform any activities related to the transactions very easily by using mobile devices at any time. On the other side mobile commerce also have certain drawbacks. The main drawback concerned with the mobile commerce is related to the security. As the whole transactions data transfers between the two parties in an open air. We are trying to overcome this issue with the help of the biometric systems. There are few challenges related to the biometric systems like security of the biometric features that are extracted by the system and the recognition accuracy of the biometric systems. We are learning some techniques which can improvise the privacy and accuracy of the biometric systems. We analyses certain types of errors in the recognition accuracy of the biometric system like FAR and FRR that is Fault Acceptance Rate and Fault Rejection Rate. The Fault Acceptance Rate is the incorrectly accepting the unauthorized user. And the Fault Rejection Rate is rejecting the authorized user. In order to improve the recognition accuracy of the biometric systems these above two factors must be low. The overall accuracy of the biometric system depends upon the GAR that is Genuine Acceptance Rate[12]. The system having maximum GAR rate is considered to be the most accurate system. We are trying to overcome these errors with the help of the Multimodal Biometric system that fuses the features from more than one biometric trait that is fusion of fingerprint and face and this technique is commonly known as fusion technique. With the help of this modal we can increase the visibility of the input images and make the recognition process efficient.

Keywords—Mobile commerce, multimodal biometric system, fuzzy vault, fusion, template security.

1. INTRODUCTION

1.1 Mobile Commerce

Mobile commerce or m-commerce is an e-commerce model, except that all the activities are being performed across the wireless network using mobile device PDA and palm hand held devices. The various activities performed by the m-commerce are as follows on line banking transactions, online shopping, online reservation, online reservation of air tickets etc. Mobile Commerce is basically the purchasing and selling of the various products with the help of wireless hand held device like laptops and mobile phones [1]. The various payments methods used in the m-commerce are as follows first is with the help of credit cards, micro payments system and store value cards.

1.2 Difference between the M-Commerce and E-Commerce

The main difference between the m-commerce and E-commerce is that m-commerce is the process of purchasing and selling the different product over the wireless network with the help of hand held devices such as laptop, palm held devices or the mobile phones while e-commerce is the process of purchasing and selling services and products over the wired network like telephone and e-mail. Whereas If we compare m-commerce with the e-commerce the basic difference comes out e-commerce is limited as to conduct the various inline transaction on e-commerce requires the computer and internet connections while if the same activities are performed with the help of m-commerce require only the mobile phones, because the mobile commerce is same what faster than the e-commerce. M-commerce is the process in which the users perform the various transactions comfortably without the hassle of wires and electricity. Whereas e-commerce is the process, in which the user has to worry about the wires and the electricity.

1.3 Advantages of M-commerce

The advantages of the M-commerce are as follows:

- (i) M-Commerce is highly convenient that is the size and weight of the mobile devices are quite less

- (ii) M-Commerce is highly accessible one can perform, the activities anywhere at any time.
- (iii) M-Commerce is highly personalized the mobile devices can not shared among another.
- (iv) M-Commerce permute mobility that is mobile phones are easily portable that is one can take the mobile phone where and perform the activities.
- (v) M-Commerce avoid the hassle of the wires and electricity.

1.4 Disadvantages of M-commerce

- (i) The size of screen of the mobile devices are very small
- (ii) Computational power of the mobile device is less as compare to the computers.
- (iii) Battery of the mobile devices does not lasts for large period
- (iv) Mobile devices can be easily lost
- (v) Data stored in the mobile devices, can be easily interpreted by the other third person.

1.5 Security issues related to the M-commerce are as follows [2]

- a.** *Authentication:* - Authentication is an operation of verifying the identity of user. Authentication plays an important role in the m-commerce process. If the application is not strongly authenticated then any hacker, can steal the important data
- b.** *Authorization:-* Authorization is the process of assigning the access right to the user. Authorization is important, so that, any unauthorized person cannot access the application
- c.** *Integrity :-* It involves that the message sent by the sender and received by the receivers is same that is there is no change in the message before reaching to the receiver

- d. *Confidentiality* :- It involves that the important information, should not be disclosed to the authorized user, so that the information cannot be misused
- e. *Non-Repudiation* :- It involves that of the transaction has take place then it is proud that's , transaction take place
- f. *Denial of service* :- It involves that if any person can send the mail to anyone, then he/she cannot say that Particular e-mail is not sent by that sender

1.6 M-Commerce Payments Transaction

Mobile payments transaction plays a vital role in the whole process of the mobile commerce, as we know that in the mobile commerce, the user buy and sell the product online, so it require online fund transfers or amount paid to the merchant for the purchasing of the product. [3] The payments may be big or small depending upon the needs of customer. Mobile payments is the inline banking requirement is very sensitive as it require, a strong security, while accessing the different transaction, so that the confidential user name or password, can't be disclosed the third unauthorized person . in the process of the banking transaction, the customer access the banking application installed in the mobile phone it asks for the authentication to check or you can say that it verify that whether the right person is accessing the application and send the username and password entered by the customer. In the banking application portal the bank server. Bank server, matches or you can say that checks whether , the user name is right or wrong if the username or password is right then the bank server grant the OTP(one time password) and send to the user by short message services. After receiving the message the user enter the OTP password and send again to the bank server. Bank server verify, OTP sent by the user and with the same sent by the server to user. It matches then, user have successfully authenticated

1.7 Transaction Authentication [3]

- (i) The user send the data amount or account no. to the bank server, by filling the amount of data detail in the banking application
- (ii) Banking application sends the information to the bank server

- (iii) After that the bank server create an signature and send back to the user with the amount of data entered by the user
- (iv) After receiving the message , the user verifies that whether the data is same that user send to the bank server if it matches then user provide the internet banking application with signature transaction data
- (v) The banking application sends the signature to the banking server.
- (vi) Then the banking server verify, signature sent by the user, whether it matches or not, if it matches then it is true and transaction take place successfully

1.8 Biometric Techniques

Biometric techniques play a crucial role in the mobile payment, as it provides the strong authentication [4]. Biometric technique is the process, which uses the physiological behavior of the persons.

It includes the followings:-

- a. Finger prints
- b. Face recognition
- c. Iris recognition

The main challenge of the biometric technique is:-

Recognition accuracy: - it is mainly concerned with comparing biometric features of the person with data base reserved that is how accurately it recognize biometric template. Two basic indicators used to measure the recognition accuracy of biometric templates are FRR and FAR i.e. Fault rejection rate and Fault acceptance rate. FRR is number of false rejections to the total number of attempts. FAR is the number of false acceptance to the total number of attempts[13].

1.9 Increased Recognition accuracy

To enhance the recognition accuracy of system multibiometric system plays a crucial role. Multibiometric system is a system that joins the result derived from all the biometric features for authentication. These systems are in great demand in many of the applications now days, because of the several advantages of these systems. The first advantage of this

system is that it has lower error rate and the second advantage is large population coverage. Biometric cryptosystem effectiveness depends on the two factors first one is matching performance and second is template security. The matching performance of the biometric system depends on the FAR and FRR that is false acceptance rate and false rejection rate. The recognition accuracy of the biometric system gets increased by using the multimodal biometric system which means using more than one biometric feature. It includes two stages first is enrolment and second is verification. The enrolment process includes scanning of the biometric traits that is finger print and face or fingerprint and iris. The verification process includes verifying whether the authorized person is accessing the application or not. In this process biometric template created is matched with the template stored in the data base. Multibiometric system increases the accuracy and reliability of the biometric system as compare to the unibiometric system that rely on the single biometric trait

.

The unibiometric system has the following limitations

1. Noise in the sensor data
- 2 Lacking operational points of interest relating to performance and precision.
- 3 Lack of universalities
- 4 Inter class similarities
- 5 Intra class variation
- 6 Interoperability issues.
- 7 Spoof attacks

1.10 Multimodal biometric systems [5]

The multibiometric model consists of four above modules.

1. Sensor module: It is used to record raw biometric details of the user.
2. Feature extraction module; extracted biometric data is assessed for further processing.
3. Matching module: In this the extracted figures are compared with the template saved in data base.
4. Decision making module: It decides whether user is authorized or not

1.11 Techniques for finger print recognition are:

1. Minutiae based: In this the Fingerprints are being represented by their local features such as bifurcation or termination.
2. Ridge feature based: feature extraction and template generation are based on series of ridges as opposed to discrete points, which forms the basis of pattern based techniques

Finger print recognition includes the following: Fingerprint enrolment, Fingerprint verification, Fingerprint identification.

Fingerprint identification which is also called dactyloscopy. It is process of collating two cases of friction ridge skin impressions (minutiae) from the human hand.

Finger print minutia's are:

1. Termination
2. Bifurcation
3. Short ridge

A. Bifurcation: Bifurcation defines point of splitting of single ridge into two, which is comparatively of shorter length than average ridge length available on the finger print [6] Minutiae plays a significant role in analysis of the finger. Minutiae based technique is better because of easy storage and less space occupancy.

Steps involved in the process

Step1: In finger print every individual have distinct termination and bifurcation points.

Step2: By combining these two factors that is termination and bifurcation collectively we get minutiae points.

Step3: After that extract the minutiae with the help of minutiae extraction techniques.

Step4: It will give a metrics in coordinates are in the form of (x, y), named as A1.

Step5: In the case of facial feature we use principle component analysis algorithm to extract the feature which gives Eigen values in the terms of x and y and we get another metric named as A2.

Steps: at last by combining both the metrics A1 and A2 we get new template = (A1 + A2).

1.12 Security of template

In order to secure the template we use fuzzy vault scheme [7]. In this scheme minutiae extracted from fingerprint are merged with a key (K) to form a vault. In this process we use 128 bits and with the help of Galois field we create a polynomial of degree $n-1$. A Galois field is the function in mat lab that is used to create the polynomial. After that we plot the values of the coefficient of the polynomial obtained and we get a graph. The drawback of this graph is that by plotting the values any one can identify the graph. so to increase the randomness of the minutiae points we add chaff points .chaff points are the points that increases the randomness so that no one can easily identifies the path of the graph hence increases the security. This whole above process is called fuzzy vault encoding.

1.13 Benefits of the fuzzy vault

1. Fuzzy vault is safe as it does not reveal the data about minutiae as it practises the one way hash function for encryption.
2. It handles the intra class variations in biometric data[14].
3. It saves only transformed or updated version of the template which make it usable for various modalities along with fingerprints.

In the fingerprint there are present terminations and bifurcations which are collectively called as minutiae points. Every individual have different fingerprint features. These minutiae points are extracted with the help of different minutiae extraction techniques and create the secure template. Galois field is the mat lab function used to create the polynomial.in the finger print the minutiae points that are extracted are stored in the database, which can be easily attacked means to say any un authorized person can identifies the pattern of the minutia, so in order to secure the minutiae points. These points are merged with the key to create the vault which is known as the fuzzy vault.

1.14 Fingerprint recognition:

Fingerprint recognition is divisible into two parts. The first being fingerprint verification and second being fingerprint identification. Fingerprint verification is to verify whether the person is authorized or not. While fingerprint identification helps the user to recognize identity of a person through impressions of their fingerprint. [8] Two set of approaches are used for fingerprint recognition i.e. minutia based and image based. Finger print

recognition process can be shown diagrammatically in the given figure below. In the finger print recognition the minutiae are extracted from the finger with the help of the minutiae extraction technique are matched with the data of user stored in the system data base. Both data are matched with each other if the data matched with each other than verification successful else not matched.

1.15 Face recognition:

In the face recognition PCA algorithm is used. PCA stands for principle component analysis. PCA gives the Eigen values and Eigen vectors [10]

Implementation of the PCA

1. Face image of size $p \times q$ pixels is defined by using vectors in $p \times q$ dimensional space.
2. PCA implementation includes identifying faces of 50 peoples to recognize that include girls and boys.
3. First step is by using the training set to train the PCA and every face in this training set is changed into face shape. Their components are also stored in the memory.
4. Two dimensional pictures are considered as vector, by joining each row or column of the picture.
5. Each classifier has their own presentation of basis vector of high dimensional face vector space.

2. PROPOSED METHODOLOGY

Research Methodology

With a purpose to enhance the recognition accuracy of biometric system two main factors should be considered.

1. FAR(Fault Acceptance Rate)
2. FRR(Fault Rejection Rate)

The Fault Acceptance Rate is the incorrectly accepting the unauthorized user. The Fault Rejection Rate is the rejecting the authorized user.

These following above two factors must be low to enhance the recognition accuracy of the biometric system. GAR (Genuine Acceptance Rate) is a sum total of all the measurement of the biometric system. It can be measured by using formula: $GAR = 1 -$

FRR. We can directly compare separate biometric systems by setting their threshold, so that FRR is at specific value. The system with maximum GAR rate is considered most accurate. We are trying to increase GAR by using the multimodal biometrics system (Fusion of finger print and face) [9]. This approach extract biometric features more accurately than unimodal biometric.

Research methodology comprises of two basic modules:

(i) Fusion module

(ii) Biometric cryptosystem:

A. Fusion module: In the fusion module fusion of two biometric traits take place. In this module first of all the feature from the different biometric modalities is extracted with the help of the different extraction techniques like embedded algorithm for fingerprint and PCA for the facial feature. After extraction the different features are fused to create the one new template which is more accurate and secure.

B. Biometric Cryptosystem Implementation

Biometric cryptosystem is very essential in order to secure the minutiae point extracted from the fingerprint [11]. It includes the fuzzy vault scheme. Fuzzy vault scheme consists of two steps.

The first step is fuzzy vault encoding and the second one is fuzzy vault decoding. In the fuzzy vault encoding the minutiae extracted from the fingerprint are merged with the security key and create the secure vault.

Biometric cryptosystem: The implementation of the biometric cryptosystem is divided into two parts. First part is fuzzy vault encoding and second part is fuzzy vault decoding that is enrolment stage and verification stage. It is very essential to secure the minutiae point that is extracted from the fingerprint. In order to create the secure sketch we use fuzzy vault scheme. Fuzzy vault scheme consists of two steps the first one is encoding and second one is decoding. In the fuzzy vault encoding the feature extracted from the fingerprint and face are merged [15] with the 128 bit security key and with the help of the Galois field we get an polynomial of degree $n-1$ and we plot the coefficients of the polynomial to get an secure sketch. This sketch can be easily identified by the attacker so in order to make it more complex we add chaff points which increases the randomness and sketch cannot be easily identified.

In the fuzzy vault decoding, this stage is also known as the verification stage. We take query image of both the templates. These images may not be properly aligned so we use helper data for the proper alignment. After that we get a transformed minutiae points and transformed facial features and then match with original template stored and key is retrieved. If the key matched then successful otherwise not successful. In contrast to fingerprints, the extracted features are minutiae points. In the finger there are present termination and bifurcation collectively which are known as minutiae points. While in the case of face the extracted features are in the terms of Eigen points. These two different features are combined together to create new template.

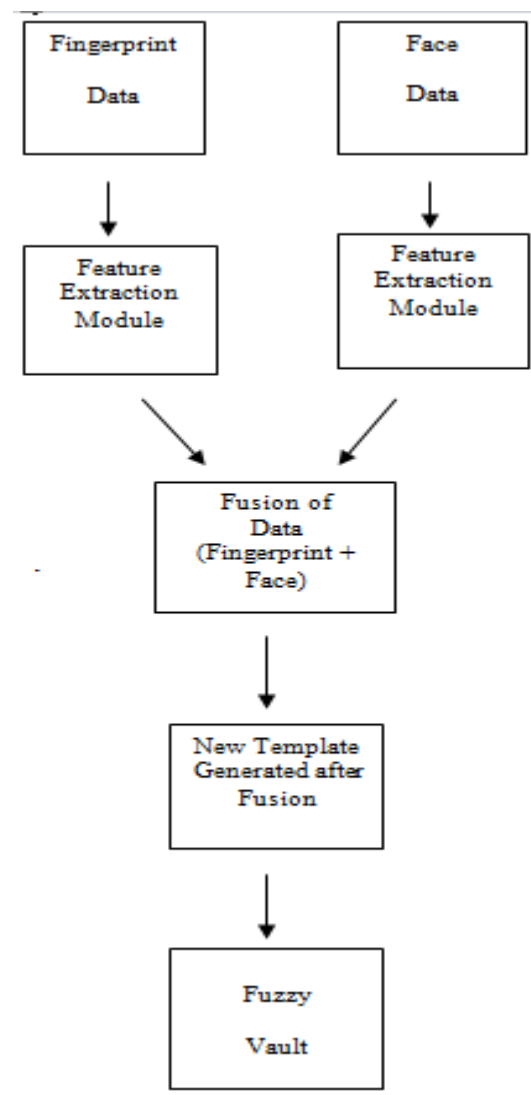


Figure.1 Flow chart of research methodology

3. RESULTS

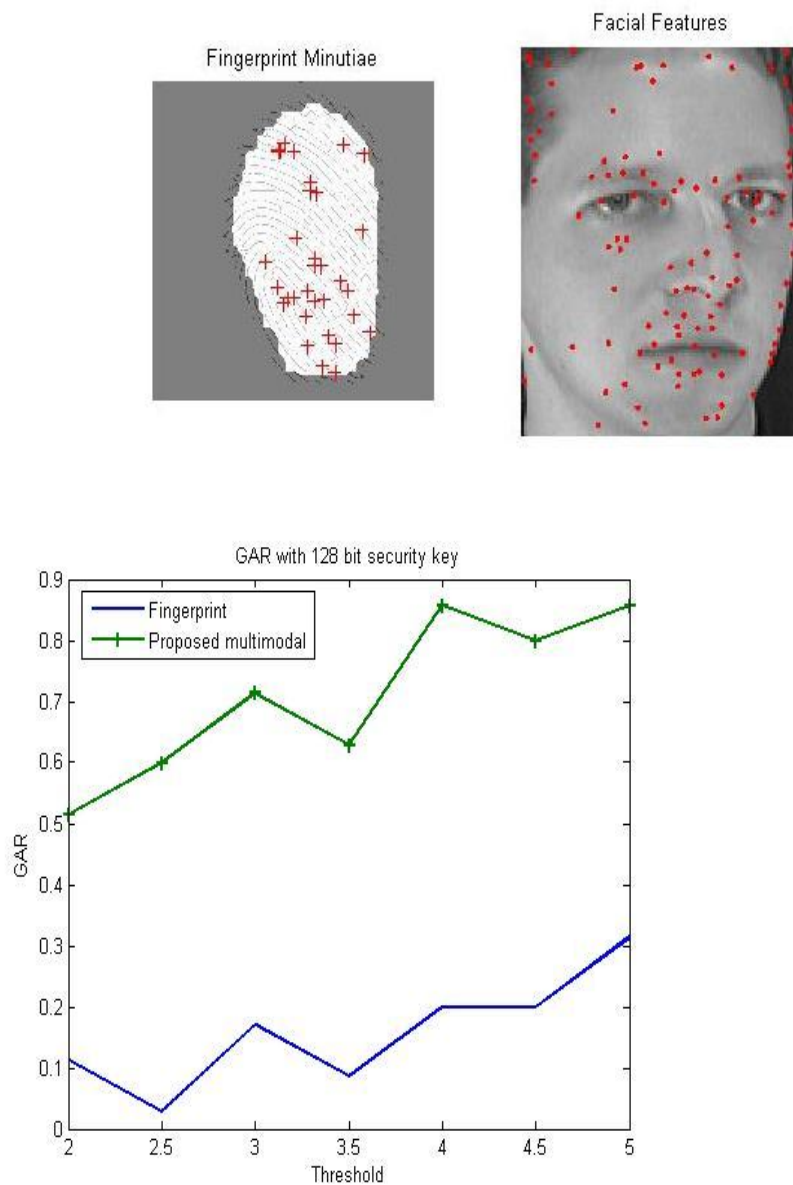


Figure.2 GAR comparison for fingerprint and proposed multimodal

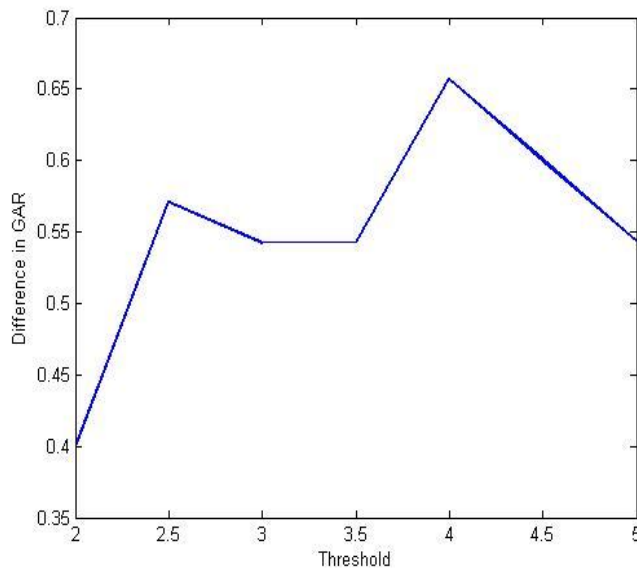


Figure 3. Difference in GAR (GAR_multimodal and GAR_fingerprint)

- 1.Security and reliability of Mobile payment transactions will be enhanced.
- 2.Fault Rejection Rate of the biometric authentication system is decreased.
- 3.Fault Acceptance Rate of biometric authentication system is decreased.
4. The probability of attack during mobile commerce transactions is decreased

With the decrease of these two factors FRR and FAR the recognition accuracy of the biometric system increases. Multimodal biometric is used to decrease the fault acceptance rate and fault rejection rate. Multimodal biometric uses the fusion of the finger print and face. It extracts the biometric feature more accurately than the unimodal biometrics

4.CONCLUSION

In our examination we break down the difficulties in the recognition accuracy of the biometric extracted information. The diverse issues that we discovered during the recognition of biometric template is unmatching of the finger prints, facial elements derived from the database stored of that person. There are two fundamental angle to

access the recognition accuracy of the biometric identification system namely FRR (fault rejection rate) and FAR (fault acceptance rate).

1. $FRR = \text{Number of fault rejection} / \text{total no of genuine attempts}$
2. $FAR = \text{Number of fault acceptance} / \text{total no of imposter attempts}$

We can persuade this issue of error in biometric feature derived information by using multi model biometric system (fusion of finger print and face) and it enhances the recognition accuracy of biometric template. This technique helps in increasing the overall genuine acceptance rate of the system and makes the mobile payment transactions profoundly secure and dependable.

5. FUTURE WORK

According to the recent survey there is continuously a rapid increase in the users that uses the smart mobile phones and most of the users divert toward the use of the mobile applications for the online transaction purposes. We will develop an integrated module that can be used in the mobile transaction applications (paytm, flip cart etc.), in order to provide the highest security in the terms of authentication by using biometric systems, because these Systems uses the biometric features of human beings for the authentication purposes and biometric traits are different for every individual and difficult to be compromised. Thus making the mobile transactions reliable and secure.

6. REFERENCES

- [1] Rajesh kumar, Rahul Rishi (2012), "Impact of mobile commerce & its application with security in india context".
- [2] Krishna Dharavath, F .A Taludkar (2013) "study on biometric authentication systems, challenges and future trends"

- [3] Dai Wei, Tang Yangling (2010) “Research on security payment technology based on mobile e commerce
- [4] Ravi subban and Dattatreya P.Mankame (2013), “A study of Biometric approach using finger print recognition”.
- [5] Vipul Awasthi, Vanchha Awasthi (2012), “Sheena S, Sheena Mathew (2014) “A study of multimodal biometric system”
- [6] L.Ravi kumar, S.Sai Kumar (2012), “Finger print Minutia match using bifurcation technique”
- [7] Ismeet Kaur, Ajay Mittal (2014), “Security enhancement techniques of the fuzzy vault”
- [8] Santosh Sharma (2013), “Fingerprint recognition based on ridges, bifurcations and 3 branch position”.
- [9] Houda Benaliouche, Mohamed Touahria(2014) “Comparitive study of Multimodal biometric recognition by fusion of iris and fingerprint”
- [10] Snehlata Barde, GR Sinha (2014), “PCA based multimodal biometrics using ear and face modalities”.
- [11] Abhishek Nagar, Anil K Jain (2012) “Multimodal cryptosystems based on feature level fusion”
- [12] Khokher R, Singh RC. Footprint-Based Personal Recognition Using Dactyloscopy Technique. InIndustrial Mathematics and Complex Systems 2017 (pp. 207-219). Springer, Singapore.
- [13] Sathiya T, Sathiyabhama B. Fuzzy relevance vector machine based classification of lung nodules in computed tomography images. International Journal of Imaging Systems and Technology.

[14] Chitra D, Sujitha V. Security analysis of prealigned fingerprint template using fuzzy vault scheme. Cluster Computing. 2018:1-9.

[15] Sree SS, Radha N. Cancellable multimodal biometric user authentication system with fuzzy vault. In 2016 International Conference on Computer Communication and Informatics (ICCCI) 2016 Jan 7 (pp. 1-6). IEEE.