An Altered Fingerprint and Multi-Biometric System to Enhanced Security Using Delaunay Triangulation

Ms.V.Mathavi[1], Ms.T.Bavithra Devi[2]
PG Scholar[1], Research Scholar[2]
[1]M.Tech., Dept. of Computer Science & Engineering, PRIST University,Vallam ,Thanjavur.
[2]Assistant Professor, Dept. of Computer Science & Engineering,PRIST University,Vallam ,Thanjavur.

Abstract— Biometrics are used in authentication process because biometrics are distinctive recognition of human being. Multi-biometric systems need storage of multiple biometric templates (e.g., fingerprint, iris, Palm and face) for each user, which results in increased risk to user privacy and system security. One method to keep individual templates is to store only the secure sketch generated from the corresponding template using a biometric cryptosystem using minutiae method. In addition we construct finger print based biometric concept of Delaunay Triangulation. We propose the Novel Algorithm altered finger print based Authentication to avoid the authentication problem due the scratches in our finger. This method provides better security with time efficient compared to the cryptosystem based on multi bio-metric.

Index Terms— Multi biometric cryptosystems, Delaunay triangulation, Altered fingerprint based authentication, authentication accuracy, security.

I. INTRODUCTION

Multi-biometric systems accumulate evidence from more than one biometric trait (e.g., face, fingerprint, and iris) in order to recognize a person. Compared to multi-biometric systems that rely on a Multi biometric trait, multi-biometric systems can provide higher recognition accuracy and larger population coverage and large time consuming.

Consequently, multi-biometric systems are being widely adopted in many large-scale identification systems, number of software and hardware multi-biometric products have also been introduced by biometric vendors. The system will output a match if

Associated edge, and t k ∈ {0, 1} is the minutia type (0 corresponds to ridge ending while 1 corresponds to ridge bifurcation).biometric-based techniques offer a non-repudiable, more universal and reliable option for individuals' authentication.

A typical according to a pre-defined similarity measure, a query is sufficiently similar to the template or a mismatch if it is not. As biometric template sare physically stored in databases or servers, raw images are able to be reconstructed once the templates are compromised by attackers. Compromised biometric data is unlikely to be replaced due to the scarcity of biometric traits an individual possesses, which means a permanent loss of the chosen biometric features for authentication purposes. More seriously, since a biometric template is likely to be used repeatedly on different applications, a compromise of the template will put all these applications at risk and may lead to a great loss to the owner. Practical implementation of the proposed feature level fusion framework[5] using familiar biometric cryptosystems for between matching accuracy and security in the proposed multi-biometric cryptosystems based on two different databases (one real and one virtual multimodal database), each containing the three most popular biometric modalities, namely, fingerprint, iris, and face. Experimental results show that both the multi-biometric cryptosystems proposed here have higher security and matching performance compared to their Multi-biometric counterparts. These components are synchronized in the Multi biometric concepts altered finger print technique. This technique performs the Delaunay Triangulation with dots minutiae. The finger prints image, the dots are selected from the scanned image. The dots are formed into triangle and process can synchronize from multi- biometric to uni – biometric process. In an existing system, multi-biometric systems require storage of multiple biometric templates (e.g., fingerprint,) for each user, which results in increased time delay.

II RELATED WORK

A. DELAUNAY TRIANGULATION

Triangulation is a process of dividing a region of space into multiple minor triangular regions. Suppose a fingerprint image consists of n minutiae, which are denoted by M = {mi} n i=1. [5] A Voronoi diagram of the minutiae set M is constructed, which partitions the complete image into n regions such that all the points in the ith region are closer to mi than to any other minutia .we connect the minutiae in neighboring Voronoi regions and form the Delaunay triangulation net.

B.FEATURES EXTRACTION

The features of images extracted using Delaunay triangulation. In our construction, to reduce matching processing time, we choose the first 80 Delaunay triangles from the whole set in ascending order of the distance between them and the singular point or the center of the fingerprint image[1][5]. It can be represented by a 24-bit binary string.

C. ENCRYPTION

The encryption process having two level of process. In the first level the images are encrypted using hash function .This encrypted templates are transformed into second level encryption process with sub key K[5][3].This sub keys will be used as input of the second level. The hash value also computed.

D. DECRYPTION

The decryption process also handled in two level of process .The sub keys are recovered and then add to an unlocked set [5] .This set having more than n or n sub keys then it can be decrypted.

III PROPOSED METHOD

A. COLLECT USER FINGER PRINT FROM BIOMETRIC IMAGES

A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. Human fingerprints are detailed, unique, difficult to alter, and durable over the life of an individual, making them suitable as long-term markers of human identity such as (e.g., fingerprint, iris, Palm and face). For a biometric process the finger print data are collected and stored in the database from the biometric devices. During authentication process the database provide the matching results of the particular process.

B.BIOMETRIC MINUTIAE

Bio metric devices (e.g., fingerprint, iris, Palm and face) Fingerprint minutiae are extracted obtain the binary string representation from the minutiae set. First the user has to upload and select the biometric images from the sample database. Then the Finger print features are loaded into the system. Then this module, extracts the biometric image features. We further assume that the adversary has knowledge about the biometric system.

C.DELAUNAY TRIANGULATION

Delaunay triangle is used to form the dots triangle from the minutiae. Delaunay triangulations maximize the minimum angle of all the angles of the triangles in the triangulation. For a set of points on the similar line there is no Delaunay triangulation for four or more points on the same circle the Delaunay triangulation is not unique, each of the two possible triangulations that split the quadrangle into two triangles satisfies the Delaunay condition. In this process the Delaunay triangle formation from the dots minutiae.

D.ALTERED FINGER PRINT BASED AUTHENTICATION

In this module, constrained Multibiometric cryptosystem, we implemented a system consisting of biometric (face, iris, palm, fingerprint) modalities, where minimum matching constraints are imposed for the fingerprint modality of 70% matching. In this experiment a Multibiometric fuzzy commitment is implemented and a secondary representation of fingerprints is obtained using altered fingerprint aggregates.Fig.1show system implementations. This may avoid the authentication problem of scratches in a finger prints. And similarly the process for other biometric devices.

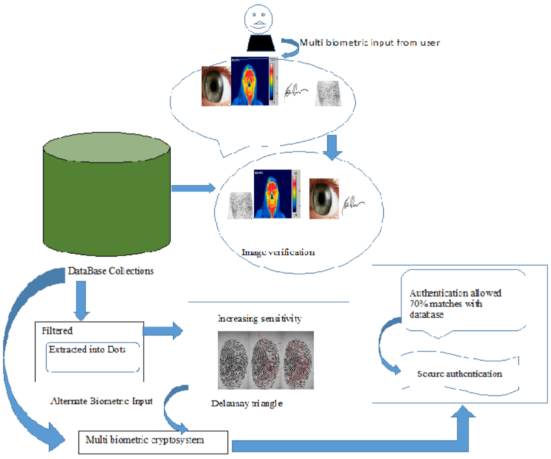

Multi biometric input from user
Image verification
DataBase Collections
Filtered
Extracted into Dots
Increasing sensitivity
Authentication allowed 70% matches with database
Secure authentication
Alternate Biometric Input
Delaunay triangle
Multi biometric cryptosystem

Fig.1 Proposed System

E.ALGORITHMS

1. LEGAL TRIANGULATION (T) ALGORITHM

Observe that the criterion is symmetric in pk and Pl: pllies inside the circle through pi, pj, pk if and only if pklies inside the circle through pi, pj, Pl. When all four points lie on a circle, both pipj and pk Pl are legal. Note that the two triangles incident to an illegal edge must form a convex quadrilateral, so that it is always possible to flip an illegal edge.

We define a legal triangulation to be a triangulation that does not contain any illegal edge. From the observation above it popular because at about the same time a new way to compute the decomposition was proposed using follows that any angle-optimal triangulation is legal. Computing a legal triangulation is quite simple, once we are given an initial triangulation. We simply flip illegal edges until all edges are legal.

Algorithm LEGALTRIANGULATION (T)

```
Input. Some triangulation T of a point set P.
Output. A legal triangulation of P.
1. While T contains an illegal edge pipj
2. do (∗ Flip pipj ∗)
3. Let pipjpk and pipjpl be the two triangles adjacent to pi pj
4. Remove pi pj from T, and add pk pl instead.
5. Return T
```

2.DISCRETE WAVELET TRANSFORM ALGORITHM

This algorithm used to take the required images and image separations. If we want images in black and white then we can use this algorithm.

Input: Data D, Signal length L;

Output: An array of the same length as the input one;

1. Take the data D =2^N and the length of the signal is L

2. To compute the first D/2 data at scale L/2^ (N-1)

3. To compute the data up to obtaining 2 data at scale L/2

4. To return the result

The result is an array of the same length as input one, the data is sorted from largest scale to small scale.

3. QR DECOMPOSITION ALGORITHM

This algorithm is used to decompose the images. This image separates the foreground and background images. If you want the images in color then we can use this algorithm.

Input: Image I;

Output: The matrix value is numerically closer to input image I;

1. To take the input image I, considered the I is an (m×n) real matrix

2. To decomposed the input image I into QR where the Q is (m×n) orthogonal and R is (n×n) upper triangular

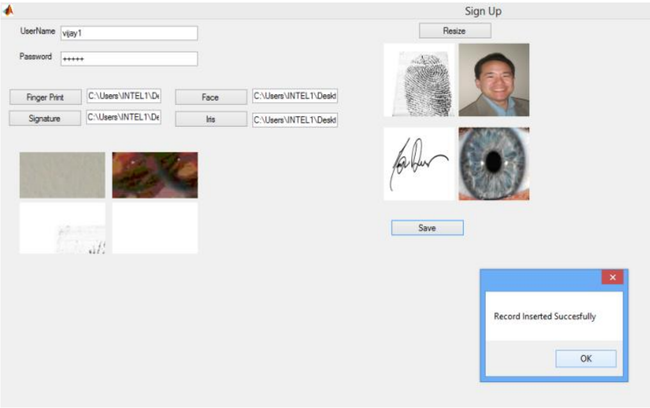
3. To compute the Q (the all informations are stored in Q) and update the matrix R

4. Return result

The result of the matrix QR value is numerically closer to input image I

IV RESULTS

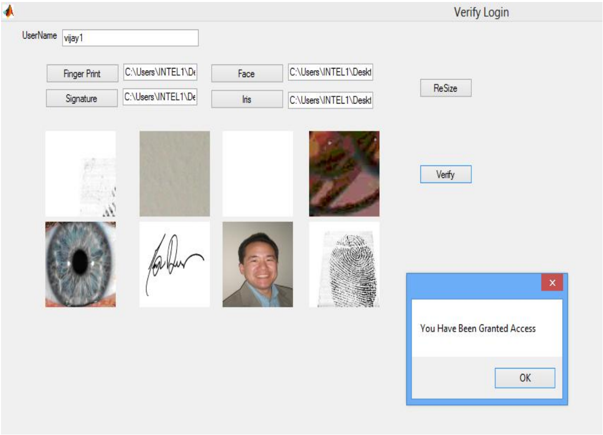
In this experiment, a Multibiometric fuzzy commitment is implemented and a secondary representation of fingerprints is obtained using altered fingerprint aggregates. This may avoid the authentication problem of scratches in a finger prints. And similarly the process for other biometric devices. Experimental results show that both the biometric cryptosystems proposed here have higher security and matching performance compared to their multi-biometric counterparts.



UserName vijay1
Password *****
Finger Print C:\Users\INTEL1\De
Face C:\Users\INTEL1\Deskt
Signature C:\Users\INTEL1\De
Iris C:\Users\INTEL1\Deskt

Record Inserted Succesfully

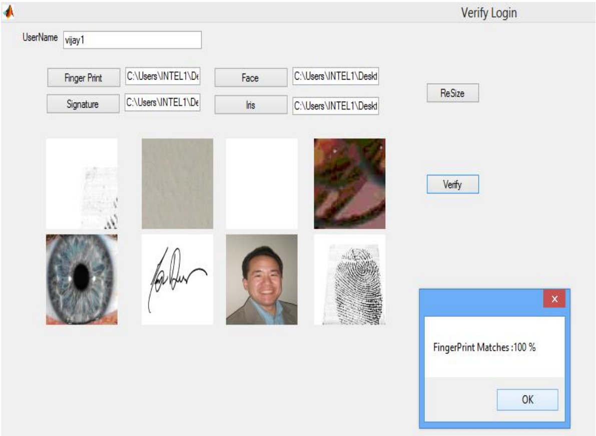
Fig.2.Database collection process



UserName vijay1
Finger Print C:\Users\INTEL1\De
Face C:\Users\INTEL1\Deskt
Signature C:\Users\INTEL1\De
Iris C:\Users\INTEL1\Deskt

You Have Been Granted Access

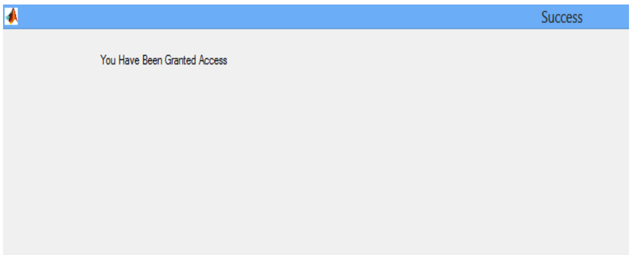
Fig.3.Compare input images into Database images



UserName vijay1
Finger Print C:\Users\INTEL1\De
Face C:\Users\INTEL1\Deskt
Signature C:\Users\INTEL1\De
Iris C:\Users\INTEL1\Deskt

FingerPrint Matches :100 %

Fig.4.Matching value show in percentage



You Have Been Granted Access

Fig.5.Authentication process

V CONCLUSION

Biometrics is not only a fascinating pattern recognition research problem. The proposed methodology presented here provides security to the distributed system and feature level fusion framework is provided. Likewise, it cannot be guessed it out how many biometrics is used and what type of biometrics are used. As secure sketch is generated from the minutiae template and stored in the database, the hackers cannot be able to use the template.

REFERENCES

[1] Y. Sutcu, Q. Li and N. Memon,“Secure biometric templates from fingerprint-face features,” in *Proc.IEEEConf.Comput.Vis.PatternRecognit.(CVPR),*Minneapolis,MN,USA,Jun.2007,pp.1–6.

[2] A.Ross, J.Shah and A.K.Jain, “From template to image: Recon-structing fingerprints from minutiae points,”*IEEETrans.PatternAnal. Mach.Intell*. vol.

[3] T.Ahmad,J.Hu,andS.Wang,“Pairpolarcoordinate-based cance- lable fingerprint templates,” *Pattern Recognit*., vol. 44, nos. 10–11, pp.2555–2564,Oct./Nov.2011.

[4]C.Le, J.Y.Choi, K.A.Toh, and S.Lee, “Alignment-free cancelable fingerprint templates based on local minutiae information,”*IEEETrans. Syst., Man, Cybern.B, Cybern.*, vol.37, no.4, pp.980–992, Aug.2007.

[5]CaiLi, Student Member, IEEE, JiankunHu, JosefPieprzyk, and WillySusilo, SeniorMember, IEEE “A new biocryptosystem_oriented security analysis framework and implementation of multibiometric cryptosystems based on decision level fusion”.IEEE Trans. *Inf. Forensics Security*, vol.10, no.6, JUNE 2015.