IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified
Vol. 7, Issue 4, April 2018

A Multi-Biometric Cryptosystem Based on Hybrid Fusion

Sreemol R[1]

M. Tech in Computer Science and Engineering, CSE, Rajiv Gandhi Institute of Technology, Kottayam, India[1]

Abstract: For person recognition, we use different physiological and behavioural features such as iris, fingerprint, face, voice etc. Biometric Identification is one of the areas related to this. The biometric data of the user are usually stored in biometric template. So the protection of biometric template is necessary because the biometric features cannot be modified like traditional username and passwords. Biometric cryptosystems can be used to protect the biometric template in an efficient manner. Single Biometric Cryptosystem which uses a single biometric feature suffers the problem of noisy data and spoofs attacks. Multi-Biometric Cryptosystem uses two or more biometric features for the protection of biometric template. Multi-Biometric Cryptosystem are of different types which uses different fusion methods. A Multi-Biometric Cryptosystem based on Hybrid Fusion is implemented with the help of biometric features such as fingerprints and iris. Delaunay Triangulation is used to extract the fingerprint feature vector and Gabor Filter is used to extract the iris feature vector. AES Encryption is used to encrypt the data of the user using the keys generated from the biometric feature. Also, Hash Function is used to further protect each biometric feature. The FAR and FRR curve of this system shows that it provides high security to the user's data

Keywords: Biometric, Cryptosystem, Delaunay Triangulation, Gabor Filter, Hybrid Fusion, Iris, Minutiae

I. INTRODUCTION

With the growth of technology, application of biometric features also faces a lot of security challenges. Earlier days, Entropy-based method was used to protect the biometric template. But, later it is proved that it is proved that it gives only the probabilistic values, not the actual values. Biometric Protection Techniques are usually classified into two: Feature Transformation and Biometric Cryptosystems. In the case of Feature Transformations, the original biometric data are changed by applying certain non-invertible transformations. In Biometric Cryptosystems, the templates are converted into biometric-dependent helper data. It will help in recovering Cryptographic keys. The generated cryptographic keys are used during the matching stage. Single Biometric Cryptosystem protects the biometric template with the help of a single biometric feature. Multi-Biometric Cryptosystems are classified into different types based on fusion mode [1]. Multi-Biometric Cryptosystems Based on Feature Level Fusion (MBCF) [5] combines a number of features into a single template for identification and verification. But, the problem associated with this fusion technique is the curse-of-dimensionality problem. When the volume of data increases, the data become sparse and we will lose some important information. Multi- Biometric Cryptosystem Based on Decision Level Fusion (MBCD) process each features separately and outputs decision based on certain rules. MBCD avoids the problem of unification of different kinds of features. Also, it retains the advantages of each biometric. Score Level Fusion method uses a biometric score which indicates the matching of the extracted feature with that of value of features inside the template. Hybrid Fusion is a combination of Score Level and Decision Level Fusion. So, Hybrid Fusion can be used to protect the biometric template in an efficient way with the help of fingerprints and iris features. Fingerprint features are extracted using a technique called Delaunay Triangulation which helps to avoid authentication errors. Iris Features are extracted using Gabor Filter.

II. FINGERPRINT FEATURE EXTRACTION

Before extracting the features, the fingerprint image has undergone some pre-processing steps to improve the quality. First, the image is converted into gray scale and again con-verted into binary image. Then smoothening is done to remove the noise. After skeletonising the image, the minutiae are calculated using Crossing Number Concept.

A. Smoothening Using Mean Filter: Mean Filter is usually used to remove noise in images. Each pixel value in an image is replaced with average of its neighbors including itself. Mean Filter helps in eliminating pixel values which are unrepresentative of their surroundings Kernels of different squares can be used (3X3, 5X5etc).

1/9	1/9	1/9
1/9	1/9	1/9
1/9	1/9	1/9

Fig. 1 The 3X3 Average Kernel often used in Mean Filtering

DOI 10.17148/IJARCCE.2018.7470

B. Skelotonization: Zhuang Shenn Thinning Algorithm is used for thinning the image. The assumption is black pixel is zero and white pixel is one. The input is an N X M array of ones and zeros.P1 represents the black pixels that have 8 neighbours. This algorithm works on all black pixels like P1.The neighbours are shown in (Fig.2).All calculations are done on the following square which is the representation of the pixels. The pixels are transformed in different ways during each step of the Zhuang Shenn Thinning Algorithm [6]. The boundary pixels of the image cannot have eight neighbours.

P9	P2	P3
P8	P1	P4
P7	P6	P5

Fig.2 Pixel Representation of the image

The steps in the algorithm are as follows:

Let X(P1)=number of transitions from white to black in the order P2,P3,P4,P5,P6,P7,P8,P9,P2.Define Y(P1)= number of black pixel neighbours of P1.
In First Step, all pixels are tested and pixels satisfied the following conditions are identified during this stage.

- The pixel is black and has 8 neighbours.
- 2<=Y(P1)<=6
- Y(P1)=1
- At least one of P2 and P4 and P6 is white
- At least one of P4 and P6 and P8 is white

The above pixels are set to white after iterating over the image.

In the next step, all pixels are again tested and pixels satisfied the following conditions are identified during this stage.

- The pixel is black and has 8 neighbours.
- 2<=Y(P1)<=6
- X(P1)=1
- At least one of P2 and P4 and P8 is white
- At least one of P2 and P6 and P8 is white

The above pixels are set to white after iterating over the image again. When any pixels were set in the above round of either step 1or 2, then all the steps are repeated until no image pixels are changed.

C. Minutiae Identification from the Image: For the above representation of the image, minutiae are identified using Crossing Number (CN) concept [2]. CN value is computed as follows:

$$CN = \sum_{i=1}^{8} |P_i - P_{i+1}| \qquad (1)$$

Here P1=P9.Using the properties of CN from above, we can-identify the minutiae. Ridge endings and bifurcations together forms the Minutiae. If the value of CN is 1, it is ridge ending and if it is 3, it is Bifurcation point. Ridge Endings and Ridge Bifurcations together form the minutiae. Thus minutiae are located in the fingerprint image.

D. Image Feature Vector from Delaunay Triangulation: Dividing the entire regions into smaller triangles is called triangulation. If a fingerprint contains 'n' minutiae, then it is represented as:

$$M = \{m_i\} \qquad (2)$$

Here 'i' varies from 1 to n.

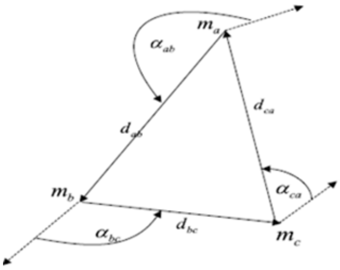

Fig. 3.Delaunay Triangulation and its features

Delaunay Triangulation [1] has 2 steps. First, a Voronoi diagram of the given set is constructed. Secondly, given the Voronoi diagram, we connect the minutiae in the neighboring regions and form the Delaunay Triangulation net. We denote the ith triangle of a Delaunay triangulation net by:

$$T_i = \{m_a, m_b, m_c\}, mk \mid k\text{E}a, b, c = \{x_k, y_k, \theta_k, t_k\} \qquad (3)$$

Here m_a, m_b, m_c are the vertices of the triangle. (x_k, y_k) denotes the co-ordinates of the minutiae. θ_k is the orientation of its associated edge.tk Є{0,1} denotes the minutiae type(0 for ridge endings and 1 for ridge bifurcation).Feature Vector of T_i is represented as:

$$FV_i = \{d_{ab}, d_{bc}, d_{ca}, \propto_{ab}, \propto_{bc}, \propto_{ca}\} \qquad (4)$$

These are the features which are extracted from the fingerprint images for the generation of final key. In this work, three fingerprints of the user are used.

III. IRIS FEATURE EXTRACTION

Iris is an internal human organ that lies inside the eye .It contains many important features that uniquely identify the individuals. Here, Gabor Filter is used to extract the iris feature vector.

A. Gabor Filter

First of all, we found the Region of Interest (RoI) in the iris image of the user around the pupil. The Region of Interest is defined as the collection of all sectors Si. After that Gabor Filter is applied in 8 directions of the iris image. Gabor Filter wavelet is the form of sine wave modulated by Gaussian Co-efficient. It is useful for extracting the global and local infor-mation of the iris. Gabor Filter is based on the frequency, orientation and Gaussian Kernel. Gabor Filter is expressed as follows:

$$Gabor(x, y, \theta, \phi) = X.Y \qquad (5)$$

$$X = \exp\{-\frac{x^2 + y^2}{2\sigma^2}\} \qquad (6)$$

$$Y = \exp\{2\pi\theta(x\cos\theta + y\sin\theta)\} \qquad (7)$$

Here x and y denotes the position of the filter relative to the input signal. θ is the angular representation of the filter and ϕ is the angular orientation.

B. Feature Vector from Gabor Filter

Let $F_{i\theta}$ (x,y) be the θ-directed filtered image. The feature value [3] $V_{i\theta}$ be defined as the average absolute deviation from the mean and represented as:

$$V_{i\theta} = \frac{1}{n_i} \sum | F_{i\theta}(x, y) - P_{i\theta} | \qquad (8)$$

iЄ{0,1….139}, θЄ{0,22.5,45,67.5,90,112.5,135,157.5} in degrees. n_i is the number of pixels in Sector Si. Piθ is the mean of pixel values.

IV. MATCHING

We calculate hamming distance [4] between all bifurcations in the fingerprint image and allother bifurcations. Also hamming distance between the ridge endings and all other ridge endings are calculated.Then take the average of the both. To achieve high precision and accuracy, add the results finally. The process is applied on both images and results are compared to find the percentage match between two images. Similiarly, hamming distance is used for calculate the matching scores between two iris templates.

V. HYBRID FUSION

Hybrid Fusion is a combination of Decision Level Fusion nd Score Level Fusion. Decision Level Fusion performs authentication in each feature separately. Here, 4 fingerprints and a singleiris image of the user are required for the final decisions.That is, the output is depends upon certain rules. Score Level Fusion uses a score value which denotes how close the current feature vector value with that of the stored template's feature vector. The score value is calculated with the help of hamming distance. If the score doesn't matches, the system denies access for that user. Thus, Hybrid Fusion is implemented.

VI. HASH FUNCTION

Hash Functions are used in this work to further protect each biometric trait. After generating the feature vector, Hash Function is applied on that value. Secure Hash Algorithm (SHA-1) is used to generate hash value. SHA-1uses a 160-bit (20 byte) hash value known as message digest. A SHA-1 hash value is usually represented as a hexadecimal, 60 digits long value.

VII. KEY GENERATION AND ENCRYPTION

In this work, the user data is encrypted using the keys which are generated from four fingerprints and iris images. To de-crypt the data, the keys should be the same. Otherwise, the system will identifies it as a faulty user. If both keys are the same, then data can be decrypted to the user. Here, AES Encryption is used for encrypting the data of the user with the help of key generated above. AES is a symmetric block cipher. This means it uses the same key for encryption and decryption. The algorithm can only accept a block size of 128 bits and a choice of 3 keys- 128, 192 and 256.

VIII. PERFORMANCE EVALUATION

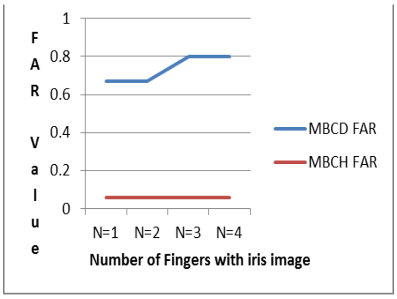

Fig.4. FAR Curve for MBCD and MBCH

The performance of the system is evaluated on the basis of False Acceptance Rate (FAR) and False Rejection Rate (FRR). False Acceptance Rate of the system can be defined as the ratio of the number of false acceptances divided by the total number of attempts. It is the probability of an attacker being accepted as an authorized user. FRR is the probability of a real user being rejected as an attacker. A good system should have a low FAR and FRR. In this work, four fingerprints image along with a single iris image are used for experiments. The FAR of MBCD and MBCH are compared here. Here, number of trials M=15.

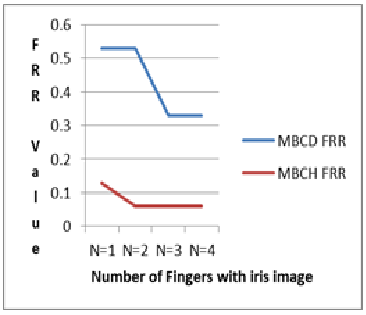

Fig. 5 FRR Curve for MBCD and MBCH

From FRR Curve (Fig.5), we can understand that the FRR value of the system based on MBCH is lower than that of MBCD. So, we can conclude that MBCH provides better protection to the user data. Also, when the number of biometric feature increases, it is very difficult for the attacker to generate the keys for decrypting the data.

CONCULSION

Multi- Biometric Cryptosystem based on Hybrid Fusion (MBCH) performs better than existing systems. It provides better security to the user data. The FAR and FRR value of the system is very less. Also, Delaunay Triangulation helps to extract the fingerprint features in an efficient way. Delaunay Triangulation has very good local stability. Also, the set of points obtained from a Delaunay Triangulation net is unique. Gabor Filter is applied on the iris for feature extraction. The use of Hash Function (SHA-1) further protects each biometric feature separately.

DOI 10.17148/IJARCCE.2018.7470

REFERENCES

[1] Cai Li, Jiankun Hu, Joseph Pieprzyk and Willy Suzilo, “A New Bio cryptosystem-Oriented Security Analysis Framework and Implementation of Multi Biometric Cryptosystem Based on Decision Level Fusion, ”IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1193-1206, June 2016

[2] Roli Bansal, Priti Sehgal and Punam Bedi, “Minutiae Extraction from Fingerprint images- A Review”, Journal of Computer Science Is-sues, vol. 8,no. 3, September 2011

[3] Ali Abdul Mun’im Ibrahim, “Iris Recognition using Gabor Filters”, Academic Scientific Journals, vol. 21, no. 7, 2008

[4] Subhash V.Thul, Anurag Rishishwar and Neetesh Raghuwanshi, “Sum Rule based Matching Score Level Fusion of Fingerprint and Iris images for Multimodal Biometric Identification”, International Research Journal of Engineering and Technology, vol.3, pp.1371-1376, 2016

[5] Abhishek Nagar, Karthik Nandakumar and Anil K Jain , “Multi Biometric Cryptosystem based on Feature Level Fusion”, IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, pp. 255-268, 2012

[6] N P Khanyile, J R Tapamo and E Dude, “A Comparitive Study of Fingerprint Thinning Algorithms”, Proc. Information Security, January 2011

[7] Thi Hanh Nguyen, Yi Wang, Trung Nhan Nguyen and Renfa Li, “A Fingerprint Fuzzy Vault Scheme using a Fast Chaff Point Generation Algorithm“, IEEE International Conference on Signal Processing, Communication and Computing, 2013

DOI 10.17148/IJARCCE.2018.7470