Volume 6, Issue 1, January 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Multi Biometric Cryptosystem Based on Decision Level Fusion

Aneesha P A
M.Tech Student, KMEA, CSE Department,
MG University, Kerala, India

Abstract— Biometric cryptosystem that provide an innovative solution for encryption, cryptographic key generation and biometric template protection. Security and authentication are the two major factors in biometric cryptosystem. In biometric cryptosystem original templates are replaced by a helper data, which assist in recovering the cryptographic keys. There are two major criteria for judging the performance the biometric cryptosystem, they are accuracy and security. The accuracy of biometric cryptosystem is similar to that of biometric authentication system and the security of biometric cryptosystem that requires helper data, that is once compromised by an attacker that should not reveal significant information about the original template. The proposed method can be classified in to two types: feature transformation and biometric cryptosystems. Here we construct a Multibiometric Cryptosystem (MBC) using decision level fusion. Here multiple fingers are used for protecting the data. Accuracy and security of single biometric cryptosystem (SBC) are limited compare to multibiometric cryptosystem. MBC offer higher authentication accuracy and flexibility.

Keywords— Biometric cryptosystem, authentication, accuracy, security, template protection

I. INTRODUCTION

Now a days there are several authentication techniques , such as passwords ,PIN, smart card ,token keys, biometrics etc. Compared with traditional authentication techniques biometric is more universal. It is used to identify an individual based on his/her behavioral characteristics .Two main characteristics of biometric are physiological (face, fingerprint, Retina, iris) and Behavioral (Signature, Voice) . [1] Authentication based on biometric is divided into two process is shown in fig. 1: Enrollment process and Authentication process .In Enrollment process , the system scans a biometric image , extract features from that image and then create a biometric template. For Authentication process , system again scans the biometric image , extract features from that image and compare with the user's template . Then the system will check a comparison and find if it is match or not.

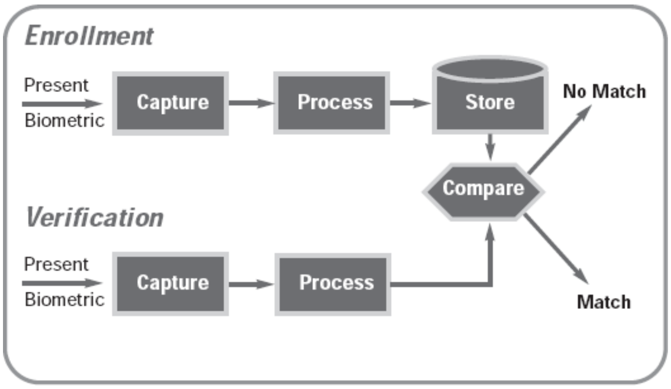

Fig. 1 Biometric Authentication System

However ,a biometric template is repeatedly used on different applications. The application is lead to risk and more loss due to compromise of biometric template. Traditional authentication system such as passwords , smart cards , token keys etc they can be reset or reissued . In biometric based authentication system, a permanent loss of biometric features will lead to a great loss. Different biometric applications would lead to new security challenges.

Here we proposed a fingerprint based cryptosystems. In fingerprint , on the surface of fingertip there contain a pattern of ridges and valleys shown in fig. 2. [2] Fingerprint representations are of different types, They are : gray scale image , skeleton image and minutiae. For authentication of user's ,transformed data is used instead of original data for protecting the biometric templates. For biometric template protection they contain, encryption, cryptographic key generation ,and a biometric cryptosystems . In biometric cryptosystems , use biometric dependant information (Helper data) instead of using original templates , for recovering the cryptographic keys .

Accuracy and Security are the criterion for evaluating the performance of biometric cryptosystem . Accuracy is similar to the typical biometric authentication system and security of biometric cryptosystems , consider the helper data . That is it does not reveal the information about original biometric templates . Biometric cryptosystem are applying both Single

Biometric Cryptosystems (SBC) and Multi Biometric Cryptosystems (MBC) . Accuracy and Security is limited in Single Biometric Cryptosystems , but in Multi Biometric Cryptosystem has higher authentication and security. Based on different fusion methods , MBC can classified as two types: fusion at feature level and fusion at decision level .

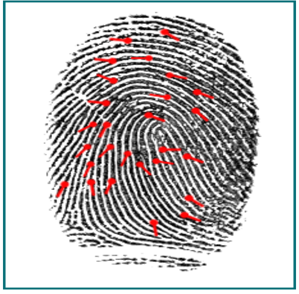

Fig. 2 Fingerprint image + minutiae

II. RELATED WORK

In this section contains various fingerprint template protection techniques . For protecting the template various schemes are used . A biometric system is used for protecting the template security .

Y. Sutcu , Q . Li and N .Memon [3] proposed that a fusion of minutiae based fingerprint and SVD based face authentication scheme .A geometric based transformation is applied for fingerprint authentication scheme and a secure sketch is used for face authentication . Authentication based on biometric is composed of two process : Enrollment and Authentication. For geometric transformations they contain a minutiae based fingerprint features, here they transform the minutiae to points on a circle shown in fig. 3.

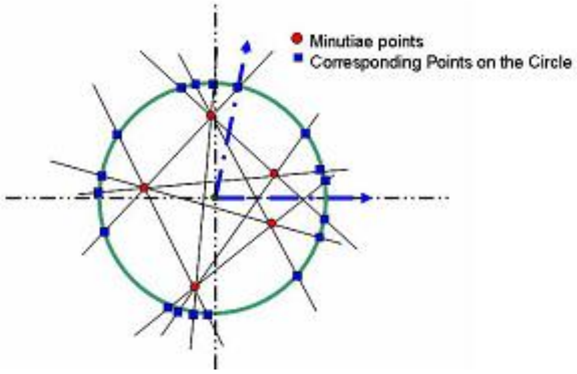

Fig. 3 Geometric transformation of minutiae

N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle [4] introduces several methods to generate cancelable fingerprints. A biometric cannot be changed it fully associated with user. It lost everything if a biometric identifier is compromised . The entire application will lost. A transformation key is issued many biometric identifiers . When the biometric will compromised identifier can be cancelled or replaced. It contain different transformations they are cartesian , polar and functional. In cartesian tra

nsformation, the minutiae space is tessellated into a rectangular grid and corresponding to the translation set by the key each cell is shifted to a new position into the grid. The polar transformation is similar to the cartesian transformation, here image is now tessellated into a number of shells and each shell is divided into sectors. By use of transformation functions the biometric templates are protected.

A. Juels and M. Sudan [5] introduces a method called fuzzy vault . It's a cryptographic construct. Which is securely encrypted and decrypted the secret information they uses a fuzzy unordered set of genuine points and chaff points . Fuzzy vault protecting the private keys and releases when the legal users enter their biometric data . Here they extracted biometric data and securely binding random generated key. Fuzzy vault scheme based on the location of minutiae points in a fingerprint.

Limitation of fuzzy vault schemes are, after stastically analysing points in vault it is easy for an attacker to stage attacks.

A. Juels and M. Wattenberg [6] proposes another method called fuzzy commitment . It's a biometric cryptosystem used to secure biometric traits are binary vectors . Binary vectors are alienated into number of segments and secured separately .

The main difference between fuzzy vault and fuzzy commit are , in fuzzy commitment scheme the biometric traits are represented by binary vectors. In fuzzy vault scheme biometric traits are represented as point set. The binary vectors are divided into number of segments and segment is secured separately. Point set in fuzzy vault are secured by hiding them with chaff points.

A. Nagar, K. Nandakumar, and A. K. Jain [7] proposed that feature level multibiometric cryptosystem . Here multiple templates of a user secured. using a feature level fusion generate a single biometric template . Using the fuzzy vault construct they secure the multibiometric template . Different features are fused into multibiometric template.

III. FINGERPRINT BASED MBCD

Compared with MBCD , Multibiometric cryptosystem based on Fusion Level (MBCF) protecting single biometric templates very strongly. In feature level fusion leads to some practical issues, from different biometric traits incompatibility of features, entropy loss for fusion, and the curse-of-dimensionality problem. Biometric feature unification difficulty will avoid MBCD and can maintain the advantages of each biometric and its related cryptosystem construction. Here we construct MBCD based on MN-split model, to secure cryptographic keys we use fingerprints from multiple fingers. There are several steps are used for protecting a finger print template. A preprocessing of fingerprint should done for protecting the fingerprint template.

A. Preprocessing of Fingerprint

Based on the local ridge characteristics ,the uniqueness of fingerprint is determined. The two important characteristics of local ridge are:

1) Ridge Ending
2) Ridge Bifurcation

Ridge Ending means the point at which ridges are end and the point where the ridges are diverge is called ridge bifurcation. The below fig. 4 shows the ridge ending and ridge bifurcation.

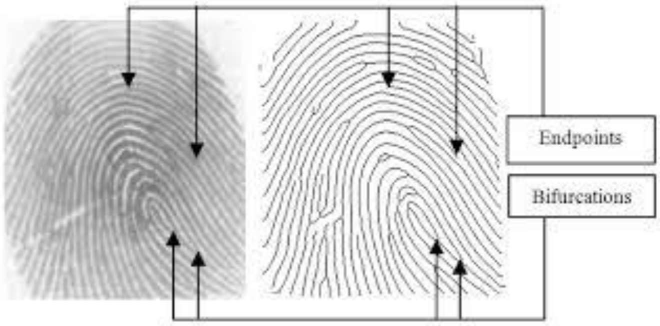

Fig. 4 Ridge ending and ridge bifurcation

Ridge endings and ridge bifurcation types of minutiae has three attributes:

1) the x-coordinate
2) the y-coordinate
3) the local ridge direction(θ)

There are different methods for minutiae extraction, they are:

1) Binarization
2) Thinning
3) Minutiae detection

Binarization is the process for converting the grayscale image into binary image. The intensity of the image has contain two value, Black represents the ridges and white represents the valleys and the background. Thinning that eliminate the redundant pixels and find the ridges of one pixel width. The minutiae's are detected from the binary thinned image.

B. Triangulation

Triangulation is a process of dividing a region of space into multiple smaller triangular regions. A fingerprint image consist of number of minutiae's n which are denoted by $M = \{m_i\}_{i=1}^{n}$. Triangulation of fingerprint M consist of two steps shown in figure 5,

1) a minutiae set is constructed that is the image is partitioned into n regions.
2) given minutiae points we connect the neighboring minutiae's and form a triangulation.

C. Feature Extraction

In triangulation process we consider ith triangle $T_i = \{m_a, m_b, m_c\}, m_{k|k\in\{a,b,c\}} = \{x_k, y_k, \theta_k, t_k\}$, where minutiae m_a, m_b, m_c are vertexes of triangle, (x_k, y_k) is the coordinates of the minutiae m_k, orientation of associated edge is θ_k , and t_k ϵ {0, 1}is the minutia type where ridge ending which represents 0 and ridge bifurcation represents 1. Feature vector of T_i is expressed by the following equations below.

Below figure shows that a triangle T_i and its features are illustrated in figure 6.

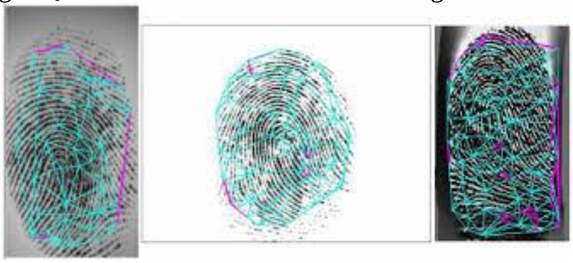

Fig. 5 Triangulation

In the triangulation net there consist of s triangles, then the fingerprint image can be expressed by a set of s local features a $SV = \{FV_i\}_{i=1}^{s}$

$$FV_i = \{d_{ab}, d_{bc}, d_{ca}, \alpha_{ab}, \alpha_{bc}, \alpha_{ca}\}$$

$$d_{ab} = \sqrt{(x_a - x_b)^2 + (y_a - y_b)^2}$$

$$d_{bc} = \sqrt{(x_b - x_c)^2 + (y_b - y_c)^2}$$

$$d_{ca} = \sqrt{(x_c - x_a)^2 + (y_c - y_a)^2}$$

$$\alpha_{ab} = \tan^{-1}\left(\frac{y_a - y_b}{x_a - x_b}\right) - \theta_a$$

$$\alpha_{bc} = \tan^{-1}\left(\frac{y_b - y_c}{x_b - x_c}\right) - \theta_b$$

$$\alpha_{ca} = \tan^{-1}\left(\frac{y_c - y_a}{x_c - x_a}\right) - \theta_c$$

D. Encryption

Suppose the multibiometric template in our MBCD consists of templates from $2 \le m \le 10$ different fingers. From the different fingers we extract the features and then form the finger template as $SV_{T,j} = \{FV_{T,j,i}\}_{i=1}^{s}$ and we apply a hash function $H_1(.)$ to each $FV_{T,j,i}$, then form a transformed template $Trans(SV_{T,j}) = \{H_1(FV_{T,j,i})\}_{i=1}^{s}$Then we generate a key and based on that key encrypt the data.

E. Decryption

In decryption extract features from multiple fingers and form the template as $SV_{T,j} = \{FV_{T,j,i}\}_{i=1}^{s}$and we apply the hash function H(.) and form the transformed template$Trans(SV_{T,j}) = \{H_1(FV_{T,J,i})\}_{i=1}^{s}$ Hence generate the same key as encryption. with the decrypted key we decrypt the file.

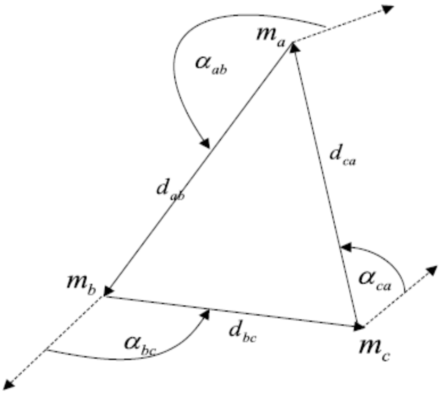

Fig. 6 Triangle and corresponding local features

IV. CONCLUSIONS

A fingerprint based MBCD is used for protecting the multibiometric cryptosystem. Multiple fingers are used for protecting the biometric cryptosystem. Accuracy and security are the two important factors that influencing biometric cryptosystem. Accuracy in biometric cryptosystem is similar to the authentication techniques and security in biometric cryptosystem that requires the helper data. From the multiple fingerprints we generate a key. Based on that key we encrypt and decrypt the data.

The biometric cryptosystem that provide an innovative solution for cryptographic key generation, Encryption, and biometric template protection. In biometric cryptosystem original templates are replaced by helper data which assist in recovering the cryptographic keys.

ACKNOWLEDGMENT

The authors would like to sincerely thank the editors and anonymous reviewers for their valuable comments.

REFERENCES

[1] Cai Li; Jiankun Hu; Pieprzyk, J.; Susilo, W " A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion", *IEEE Trans. on information forensics and security* ,vol. 10,no. 6,June. 2015.

[2] A. Ross, J. Shah, and A. K. Jain, "From template to image: Reconstructing fingerprints from minutiae points," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 544–560, Apr. 2007.

[3] Y. Sutcu, Q. Li, and N. Memon, "Secure biometric templates from fingerprint-face features," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Minneapolis, MN, USA, Jun. 2007, pp. 1–6.

[4] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[5] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes Cryptograph.*, vol. 38, no. 2, pp. 237–257, Feb. 2006.

[6] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. Comput. Commun. Secur.*, Singapore, 1999, pp. 28–36.

[7] A. Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric cryptosystems based on feature-level fusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 255–268, Feb. 2012.