International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 5 Issue 10 October 2018

Enhanced Performance of Fingerprint Template Security Using Turtle Encryption Scheme

G. Keerthana[1], Siddharth Nanda[2], Ashoka Rajan R.[3]
SCS, Jain University, Bangalore, Karnataka, India[1]
SOIT, ADYPU, Pune, Maharashtra, India [2]
keerthiguru28@gmail.com[1], nanda.siddharth99@gmail.com[2]

Abstract: *Biometrics refers to the automatic recognition of individuals based on their biological or behavioral characteristics. In fingerprint biometric system, a template security is essential to safeguard the templates from an attacker intruder. In the existing system, alignment free fingerprint cryptosystem performs matching using relative information between minutiae. The existing system uses multi biometric system which leads to high processing time and speed. The focus is to improve speed and performance of the system and to reduce false acceptance and false rejection rate. Hence to overcome this problem, a new fingerprint template security has been proposed using Turtle encryption scheme. In this study, the system generates a feature vector from the fingerprint template and by detecting the core point, minutiae direction is generated. Based on the new extracted features, the matrix form is generated. Then by using the turtle encryption algorithm, a new encrypted feature vector is generated and moreover decimal logic gate encryption scheme enhances more security by encrypting the data in a different manner which is then stored in the database. In the proposed system, the overall error rate is found to be 4.2%. So the attackers find difficult to obtain the original data.*

Keywords: *Turtle Encryption, Minutiae, Decimal Logic Gate Encryption, Template Security, Template Protection.*

1. INTRODUCTION

Naturally human's physiological and behavioral characteristics differs from each. The term "Biometrics" is derived from Greek word bio (life) and metric (to measure). A biological trait that is used for uniquely identifying a human is biometrics. Every individual has unique DNA sequence, no two persons can have the same DNA sequence. Similarly every individual has unique biometrics and it differs from each other. Biometrics play a major role in security related purposes and it replaces the traditional passwords and token cards. Biometrics can be restricted to a particular part of human body. The most employed biometrics are retina, iris, fingerprints, voice and palm-prints.

1.1 BIOMETRIC TECHNOLOGIES

Various fields has been exploiting the biometric technologies in several aspects to increase the security level. Some of the available biometric technologies are summarized as follows:

Fingerprint recognition:

Fingerprint recognition is the live acquisition of a persons fingerprint with an impression of ridges and valleys. It is used to uniquely identify the person by analysing their fingerprints.

Hand geometry:

Hand geometry is an automated measurement of hand or finger dimensions. It records an accurate spatial representation of an individual's hand.

Facial recognition:

Facial recognition identify facial features by extracting length and width of noise, shape of cheekbones and depth of the eye sockets.

Retina scanning:

Retina scanning involves an electronic scan of an individual retina by comparing the blood vessels.

Iris scanning:

Iris scanning automatically measures the iris pattern in a coloured part of an eye.

Voice Recognition:

Voice or speech recognition exploits the vocal characteristics to identify an individual using a pass-phrase.

Signature Verification:

Signature verification is an automated method of measuring an individual's signatures. It determines the direction, speed and pressure that occurs during signing. Hence, from the available biometric technologies fingerprint recognition plays a major role all over the world. Fingerprint uniqueness is high when compared with other technologies and more convenient. So, the system moved in the direction of fingerprint recognition.

1.2 BIOMETRIC RECOGNITION

Every biometric system has four modules such as sensor module, feature extraction module, matcher and database module. In sensor module the biometric system scans each individual's biometric traits which then extracts the details in feature extraction module for extracting the core features to uniquely identify an individual. After extracting features, the information is stored in the database. Simple flow chart is shown in figure 1.1.

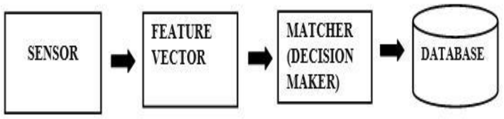

Figure 1.1 Flow diagram of biometric recognition

1.2.1 Authentication

In authentication phase, it verifies the identity of a user. Biometric authentication is a security process that includes unique biological characteristics of an individual to verify. The users provide their biometric as password to grant access. There are two types of biometric authentication namely enrolment followed by verification process.

1.2.1.1 Enrolment

During enrolment phase the system reads a user's biometric image and it automatically creates a template of features extracted from the image. Finally the template of biometric features gets stored in the designated database. Further it is verified for authentication purposes.

1.2.1.2 Verification

In verification phase, the fingerprint in query is again acquired from the user and it is verified with the pre-enrolled ones. If there is a match then the user is considered a genuine user and permitted for access**.**

1.3 VULNERABILITY IN BIOMETRICS

Biometric faces vulnerabilities at various levels such as at input level, processing level,transmitting level and at matching or decision making level. The unauthorized users can act as a genuine user to gain access to the database. All of us must become aware of these facts while using biometrics, it may also lead to failure due to some factors regarding operations. Thus a security mechanism is needed to prevent those vulnerabilities.

1.3.1 Direct attacks

The direct attack deals with hardware part .i.e. attacks on sensors. In biometric authentication system, the initial stage belongs to collection of the raw data from a sensor. Even if the sensor fails or it has been hacked by the attackers then it will fake fingerprint image. Direct attack is a part from digital domain. It does not need technical knowledge. It can be carried out if the fingerprint of the person is obtained directly through other means.

1.3.2 Indirect attacks

In these type of attacks, the attacker needs to understand technical knowledge about the internal working of the system. Attackers should have knowledge about the sample format, feature extraction implementation, template and also about matcher implementation format. The side channel and Trojan horse attacks gain information about the features in the database. So there should be strong security mechanism in a place to avoid deciphering of those feature vectors.

1.4 FINGERPRINT BIOMETRICS

A fingerprint is an impression or mark made on a surface by a person fingertip. Fingerprint is able to identify an individual's unique patterns of lines and whorls on the fingertips. Fingerprints are made up of arrangement of ridges called friction ridges. Each ridge contains pores that is attached to sweat glands under the skin.

A fingerprint biometric system automatically recognizes the individual's fingerprints and makes some pre-processing steps such as binarisation, thinning and extracted the features using feature extraction algorithm and then store it in a database, and again it is checked to verify whether the user is genuine or an impostor. Features involves tiny minutiae points that cannot be viewed through naked eyes. These types of minutiae points are ridge endings, bifurcations and dots. Even if the age is rolled out the fingerprints remains constant without fading. So these features are of great importance for identification of any individual.

1.5 BIOMETRIC SECURITY USING CRYPTOGRAPHY

Use of biometric data to identify individuals creates several security concerns also. The biometric templates are stored in database or servers, the raw image can be generated from the biometric templates when it can also be hacked by an attacker. Unlike traditional password or token card which can be reissued when it is compromised. Here it is not possible when using biometric data which is non-replaceable. Compromising these biometric templates lead to a great loss to owner in all applications that relies on biometric data. There has been a great deal of work on securing the biometric templates.

Biometric protection approaches uses inverted data on behalf of original data. To ensure the secure transmission of data, cryptography is essential. Cryptography key is generated using key generation algorithm which is very difficult to be compromised by attackers. Using those keys, the feature vectors are encrypted and it is stored in a database during enrolment. During verification the same key is used to decrypt the feature vectors. The brute force attack on passwords and that against biometric traits proves that it is very difficult to crack the biometric system than the password system.

Biometric cryptosystem is judged by its performance based on two factors such as security and accuracy. The accuracy is measured by False Acceptance Rate (FAR) and False Rejection Rate (FRR). The security relies on helper data such as key, once it is compromised it should not reveal original biometric data.

1.6 ADVANTAGES OF SINGLE BIOMETRIC SYSTEM

The advantage of choosing a single biometric system are mainly as follows:

ADDS CONVENIENCE:

Since every individual has a unique characteristic in fingerprints, it is very convenient to identify each person without the need to carry ID cards or remember complicated passwords.

DIFFICULT TO FORGE:

In biometric system, factors such as fingerprints are more difficult to forge. As fingerprints are unique in nature, it is hard to find the original template.

INCREASED SECURITY:

While considering several passwords, which has general words and numbers biometric data cannot be guessed or stolen easily. Hence, to increase security biometric systems plays a major role.

1.7 MOTIVATION

The proposed system develops new methods to protect the templates by improving the security and performance. The motivation of the proposed method is to prevent the attackers from hacking the templates. The concept of turtle encryption makes the templates more complicated so as that it could not be compromised by attackers. It also ensures that even in case of a successful attack, no meaningful information is revealed to the attackers.

1.8 PROBLEM STATEMENT

1. Providing efficient methods for encryption of feature vector that enhances the security level.
2. To improve processing time and to have quick access i.e. in a short period of time.
3. To reduce false acceptance rate and false rejection rate of the fingerprint.
4. To improve security and recognition of fingerprint and template should be secured.

2. LITERATURE SURVEY

Koen Simoens et al [10] proposed the vulnerabilities of biometric authentication protocols with respect to user and data privacy. The goal of an attacker is to learn information either on a user or biometric data of the system. The adversary’s aim is not only to bypass the system but also to gather information about the confidential data. The authors made their analysis on a general system model involving four logical entities (server, sensor, database and matcher). They focus mostly on internal adversaries that would be dangerous and malicious to the system. The malicious person may hack the system by using a single entity or combination of entities. For security analysis of biometric authentication protocols, a blackbox framework is exploited. The framework models a internal adversaries against a generic distributed biometric system. The authors defines the roles of the different entities who are involved and their potential attack goals. From these roles and attack goals the authors derived the requirements that are imposed on the data that are exchanged between the entities. First of all the generic attacks that are discussed here can be exploited by developers and reviewers as a first evaluation for new protocol proposals.

In [8], the author uses two fingerprints. From one fingerprint Minutiae points are extracted, whereas from the other fingerprint orientation directions are extracted. From both the fingerprints reference points are extracted. From these obtained points, a combined minutiae template is generated. This provides enhanced security against the hackers to extract original minutiae points. Because of these reference points it is easy to recover minutiae points once the hacker matches the orientation direction.

Juels and Sudan et al. [6] proposed the fuzzy vault scheme. This method conceals the biometric data using a polynomial and the identification is based on polynomial reconstruction using a Reed–Solomon Error Correcting Code. In [5] the author proposed amodel which uses a feature-level fusion to secure many templates of a user as single entity. The implementation is done using the techniques fuzzy vault and fuzzy commitment. But the limitation of this technique is, it is difficult to distinguish chaff points from genuine points and in fuzzy commitment, there is a lack of perfect codes for desired code lengths. Nandakumarand Jain [3] adopt fuzzy vault to conceal a template byfusing fingerprint and iris features among a host of chaff points.

Wencheng Yang et al [16] proposed Delaunay triangle based structure, which has been used in many authentication systems. It yields better and satisfactory results but there may be also some disadvantages such as structure change due to non-linear distortion. The author proposed an innovative structure known as Delaunay quadrangle structure for increased security. Pin sketch and secure sketch techniques were used. Pin sketch technique is nothing but a code to recover biometric template data and in the meantime it provides the secure protection of the template data. Because of this structure enhanced level of security is obtained and this leads to a nonlinear distortion which causes alteration in structure of the images that becomes a drawback of this system.

Vishnu Naresh Boddeti et al [15] proposed a framework to bind information to image patterns and to retrieve this information during authentication by embedding the information in the template designed to discriminate that pattern class from the other pattern classes. The framework is flexible enough to allow spreading the information to be bound over multiple pattern classes which in the context of biometric key-binding, enables multiclass and multimodal biometric key binding. The effectiveness of the proposed scheme via extensive numerical results on multiple biometric databases is demonstrated. The drawbacks of this proposed method is its limited robustness to large appearance variations. The authors believe that by using CFsreduces more distortion which in turn increases the algorithm’s tolerance to larger variations in images.

Kai cao et al. [2] proposed that reconstruction techniques demonstrate the need for securing fingerprint templates. This can be done by improving the template interoperability and improving fingerprint synthesis. In this method, reconstruction algorithm is used which utilizes prior knowledge of fingerprint ridge structure to improve the reconstructed fingerprint image is developed. However investigation must be made to make the reconstructed fingerprints more realistic.

3. PROPOSED SYSTEM

The Fingerprint template has to be made secure by applying a transformation that makes the attacker's possibility of revoking back to the original fingerprint template infeasible.

3.1 PREPROCESSING

Pre-processing is done with the images that is captured by fingerprint sensor. The aim of pre-processing is to suppress the unwanted distortions and to enhance the important features that is needed for further processing.

3.1.1 BINARIZATION

The first step involved in pre-processing fingerprints is binarization. It is the process which converts a pixel image to a binary image. There are two possible values each for white and black.

Two important properties for pixel by pixel operations in algorithms are neighborhoods and connectives. A neighborhood of 4 (N4) considers horizontal and vertical points around the pixel P whereas neighborhood of 8 (N8) considers horizontal and vertical positions as well as diagonal points. The connectivity between pixels is identified by using adjacent points that have the same properties of the central pixel P with a mask of 4 or 8 neighborhood.

3.1.2 THINNING

The thinning is defined by transformation of digital images into simplified equivalent images. The computation is done by using mathematical morphology operators but it belongs to a topological skeleton type. The ‘bimorph’ function is used for thinning the image.

3.1.3 ENHANCEMENT

The image obtained from many other sources is not of good quality. So the enhancement techniques increases the contrast between ridges and valleys and connect the false broken points of ridges. For such purpose Gabor filter is used.

Gabor filter are bandpass filters which are used in image processing for feature extraction. It serves as excellent bandpass filters for unidimensional signals. Gabor filters are orientation-sensitive filters used for texture analysis.

3.2 ARCHITECTURE OF THE PROPOSED SYSTEM

The architecture of the proposed system is described in figure 3.1. The feature vectors has to be extracted from the fingerprint-image.

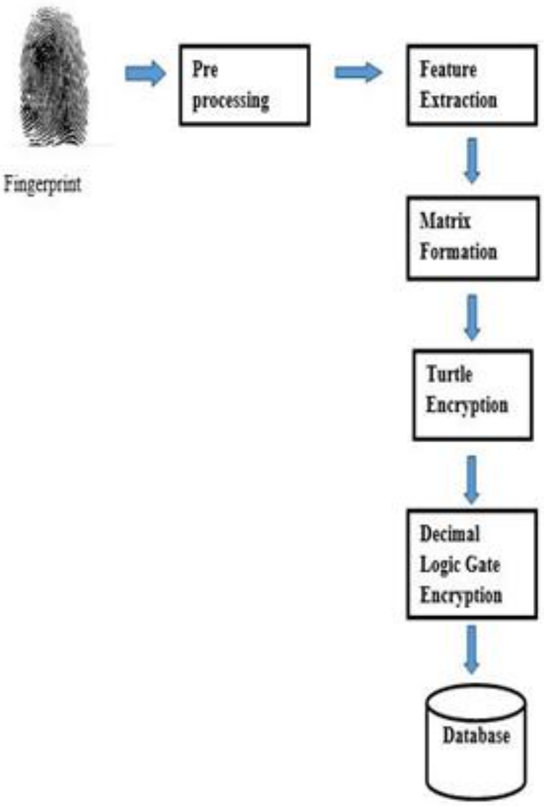

Figure 3.1 Architecture diagram

The x and y coordinates of the minutiae points is considered as feature vectors. Additionally, the angle of the minutia points are determined using core point. The feature vectors are taken as array of sequences of numbers and converted into matrix format. From the matrix format, the turtle based encryption (TBE) algorithm is used and new encrypted feature vector is obtained. Moreover, these encrypted data are embedded with the security key in the decimal logic gate encryption module and finally stored in database.

3.2.1 TURTLE BASED ENCRYPTION SCHEME:

The turtle based encryption scheme explains how the feature vectors are encrypted in the matrix format by applying turtle structure to the given matrix. The matrix is then separated into 4 quadrants namely S1, S2, S3 and S4. Then each quadrant values are taken as per encryption scheme and a sequence of array is formed.

The cell 1 is the first value to be returned followed by 2 and 3 to the left of the matrix and 4 and 5 to the right side of the matrix as specified in figure 3.2. Finally the remaining 6, 7, 8 and 9 values are also returned.

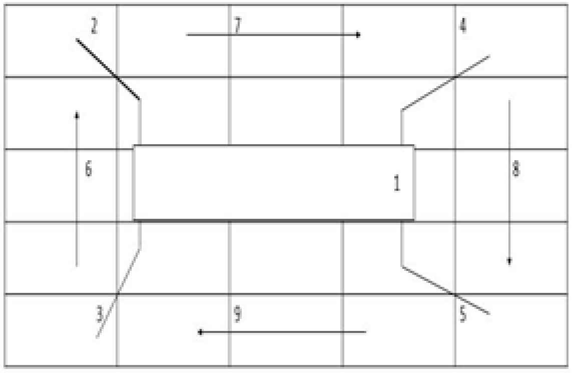

Figure 3.2 Turtle encryption scheme

4. PROPOSED ALGORITHM

4.1 Turtle encryption method:

Matrix Formation:

Considering array values of x, y coordinates, angle, radians and distance of the featured vectors, the matrix is formed.

Input: Feature vector
Output: Encrypted Feature vector
Initialize k;
k-array of elements
Loop:
i-size of row
j-size of column

```
Mat[i][j]=arr[k];
```

Turtle Formation:

```
TurtleDirection(int direction, int i, int j, int n)
{

if(i+j==n-1)
direction++;
if(i==j && j+j>=n)
direction++;
if(i==j+1 && i+j<n)
direction++;
return direction;
}
```

4.2 DECIMAL LOGIC GATE ENCRYPTION:

This module explains about adding security key to the encrypted feature vector. The key is received from the user and embedded in the encrypted feature vector using logical gate operations. The overview of the operations are given in figure 3.3. The Encrypted feature vector is taken as input A and security key to be added is considered as input B.

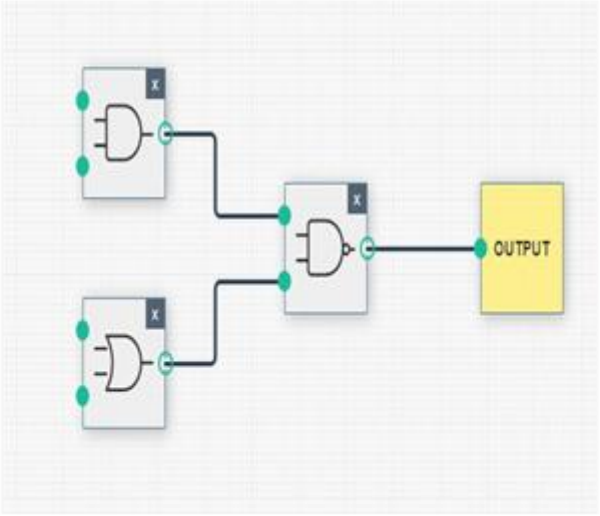

Figure 3.3 Decimal logic gate scheme

The functions applied in the logical gate operations are OR gate, AND gate and NAND gate.

For AND gate, the corresponding equation is
$f(x)=(Ax-k)/(Bx-k)]^2*[(Ax+k)/(Bx+k)]^2$**(4.1)**
where x is the encrypted feature vector

k is the key received from user
A is the (1,1) of the x matrix and
B is the (1,1) of the k matrix.
For OR gate,
$f(x)=(Ax-k)/(Bx-k)]^2+[(Ax+k)/(Bx+k)]^2$**(4.2)**

For NAND gate the equation is,
$f(x)=NOT\{[(Ax-k)/(Bx-k)]^2*[(Ax+k)/(Bx+k)]^2\}$ **(4.3)**

5. RESULTS ANALYSIS

In a biometric system, an equal error rate is a point at which both the FAR and FRR are equal. In a graph with x-axis as threshold any y-axis as error rate, the FRR and FAR are two entities, the interception of the intersection of the two entities along the x-axis gives the threshold and the interception of the intersection of the two entities along y-axis gives the equal error rate. It is also known as Crossover Error Rate (CER). The overall EER of the system should be low for higher accuracy. The False Acceptance Rate (FAR) should be very low and the False Rejection Rate should be very low. If FAR is tried to decrease the FRR might rise. The correct person might be rejected assuming him to be a wrong one. If FRR is tried to decrease the FAR might rise. An optimal value is the equal error rate at which both the FAR and FRR are low. The threshold value must be adjusted to attain this value. Thus by testing and running a large dataset threshold value is determined.

TABLE 5.1 VARIATION OF THRESHOLD WITH RESPECT TO FAR AND FRR

Threshold	FAR	FRR
0.34	25	1
0.45	15	3
0.52	4.2	4.2
0.92	3	7
0.99	1	10

In table 5.1, as the threshold increases, FAR increases. Thus at lower thresholds a faulty person might be allowed. The FRR increases with the threshold. Thus at higher thresholds a correct person might be rejected. When threshold is set at 0.52 both FAR and FRR is in 4.2%. Thus this point is considered to be the optimal point.

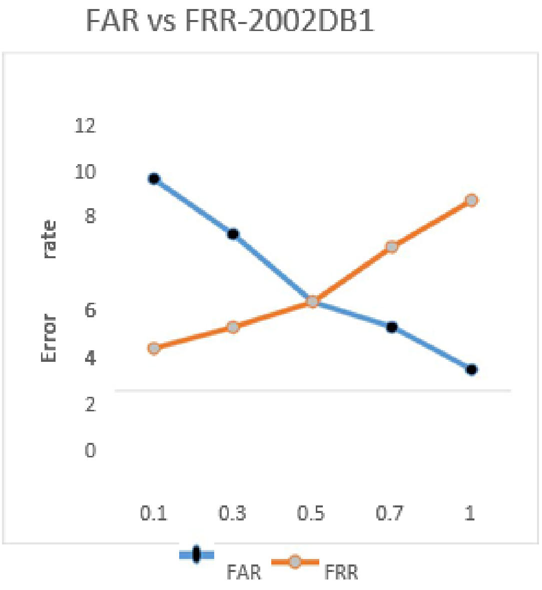

Figure 5.1 FAR vs FRR Analysis for 2002DB1

In the figure 5.1, the proposed system's threshold value was found to be 0.52% with an error rate of 4.2%.

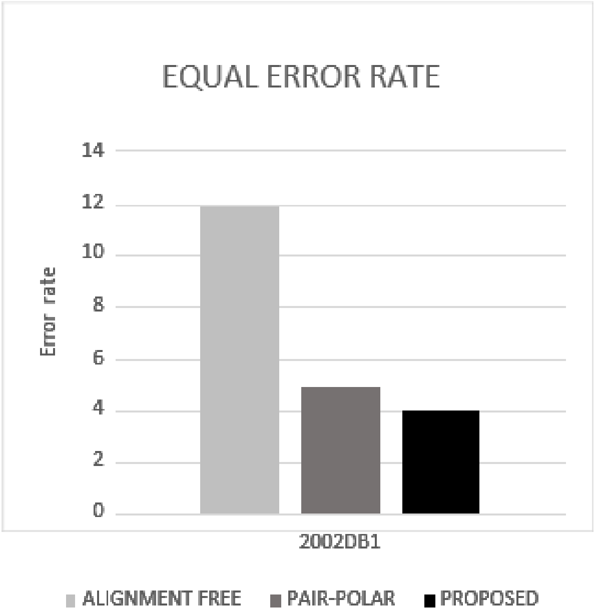

Figure 5.2 Performance of Proposed System against Existing System in 2002DB1

The Equal Error Rate of the proposed system against the Equal Error Rate of the existing systems is given in figure 5.2. The performance is for the database 2002DB1. The EER of the existing methods, Alignment–free minutia structures stands with the error rate of 11.84%, Pair-Polar minutia structures with theerror rate of 5%, Turtle encryption scheme has error rate of 4.2%.Thus the EER of the proposed system is better than the previous system.

Table 5.2 Performance Comparison of matching algorithms

Method	**2002DB1 (FAR/FRR) EER**	**2004DB2 (FAR/FRR) EER**	**2006DB2 (FAR/FRR) EER**
Wang et al(2014)	13.11	9.80	8.63
Yang et al(2014)	11.84	8.65	3.07
Liu et al(2015)	8.6	7.5	2.5
Cai			

Li et al(2016)	5	6.8	1.59

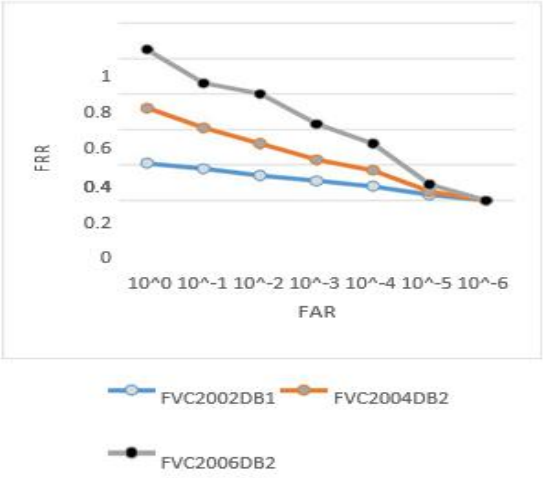

Figure 5.3 Comparison of Performance of proposed and Other Fingerprint cryptosystems using FVC Protocol

5.2 Computational Hardness:

5.2.1 Turtle Encryption algorithm

Turtle encryption algorithm is used for transforming the fingerprint inputs to another form. Based on the security provider, the turtle encryption matrix is varied. According to the number of input feature vectors the matrix size varies. So the attackers find it very difficult to crack the system. Although it provides one way encryption, the process cannot be reversed to produce the original inputs. So there is no possibility of regenerating the inputs. Even if the database is compromised, the hacker cannot get any information regarding the fingerprints. During process, these vectors will be represented in another form.

5.2.2 Decimal logic gate encryption algorithm

Decimal logic gate algorithm is used for transforming the fingerprint input to another form. Here the inputs are separated by using digits logic. Since it provides more encryption, the process cannot be reversed to produce the original input. Here the array of number ranges from 0 to 9, alphabets ranges from 0 to 25 and special characters varies randomly based on individual user. The secret key varies for individual users. Even if the attacker guesses the sequence he could not get any information regarding the digit logic.

Consider Ni as count of numbers, lower and upper case alphabets and special characters.

Numbers - 0 to 9-10 digits
Lowercase letters- 0 to 25-26 letters
Uppercase letters -0 to 25-26 letters
Special characters -33 characters

$$X= \sum_{i=1}^{4} Ni \qquad \textbf{(5.1)}$$

$$Y=N1xN2xN3xN4xX^4 \qquad \textbf{(5.2)}$$

The security analysis of any method is based on the strength of the encryption method. The computational hardness of the proposed system shows how strong our system works. It varies based on total count of minutiae points. The count of minutiae points varies according to an individual. In brute force the attackers' needs to try n! combinations. The probability of finding correct sequence is 1/n!. The total time complexity of the system is O(n^k) , where n and k are input.

6. CONCLUSION

This project underwent encryption of feature vector from the fingerprint after the process of binarisation and thinning. The point considered here is to improve the process time and to access quickly in a short period and also to improve the performance of the template security. The proposed system includes encryption of feature vector using turtle based encryption scheme. Moreover, decimal logic gate encryption algorithm enhances with more security.

By increasing the hardness of the system. The attackers find it really difficult to crack the templates and it provides better security to the templates. The proposed system error rate was found to be 4.2% by enhancing the performance. The future work is to include and redefine various parameters in turtle based encryption scheme and also to increase the size of the matrix with the goal to enhance the security. In decimal logic gate encryption algorithm, using various logical operations like NOR, XOR and XNOR can be included into process which improves the security and to perceive the threat.

REFERENCES

[1] Anil K.Jain and Karthik Nandakumar "Fingerprint-Based FuzzyVault: Implementation and Performance", IEEE Transactions on information forensics andsecurity,vol.2, no.4,2007.

[2] Raja Rao.B, Dr.Krishna Rao.E.V. and S.V.Rama Rao "Finger print parameter based cryptographic key generation" ,pp. 1598-1604,2012.

[3] Bishwa Ranjan Roy,Arun Kumar Yadav,and Amit Kumar Trivedi"An Effictive Approach to Estimate Fingerprint Orientation" IEEE Transactions,2016.

[4] Cai Li, Member, IEEE, and Jiankun Hu "A Security-Enhanced Alignment- Free Fuzzy Vault-BasedFingerprint Cryptosystem Using Pair-Polar Minutiae Structures",, 2016.

[5] Lee.C,Choi.J, Toh K-A, Lee.S and Kim.J, "Alignment-free cancellable fingerprint templates based on local minutiae information," IEEETrans.Syst.,Man,Cybern.B,Cybern.,vol.37,no.4,pp.980 992,Aug.2007.

[6] Chen Kaizhi, Hu Aiqun "An Enhancing Fingerprint Template Protection Method " IEEE,PP.275-279,2013.

[7] Enrique Argones Rua (2012) "Biometric Template Protection Using Universal Background Models: An Application to Online Signature", IEEE Transactions on information forensics and security, Vol. 7, no. 1.

[8] Bahgat.G.A ,Khalil A. H, Mashali.S(2013) "Fast and accurate algorithm for core point detection in fingerprint images" Egyptian Informatics Journal,15-25,2013.

[9] Juels and Sudan.M "A fuzzy vault scheme," Designs,Codes Cryptography., vol. 38, no. 2,2006.

[10] Kai Cao"Learning Fingerprint Reconstruction:From Minutiae to Image", IEEE Transactions on information forensics and security, Vol. 10, no 1.22,2015.

[11] Koen Simoens "A Framework for Analyzing Template Security and Privacy in BiometricAuthentication Systems", IEEE Transactions on information forensics and security,Vol. 7, no. 2,2012.

[12] Li S. and Kot A. C."Privacy protection of fingerprint database", IEEE Signal Process. Lett., vol.18, no. 2, pp. 115–118,2011

[13] Manvjeet Kaur and Taranpreet Kaur "Cryptographic key generation from multimodal template using fuzzy extractor",IC3,pp.1-6,2017.

[14] 14.NGUYEN Thi Hoang Lan "An Approach to protect key using fingerprint biometric encryption key in BioPKI based security system", Intl.Conf.on Control,pp.1595-1599,2018.

[15] 15.Li.p, Yang.X, Cao.K, Shi.P and Tan.J, "Security-enhanced fuzzy fingerprint vault based on minutiae's local ridge information," in Proc.3rd Int.Conf.Biometrics,2009,pp.930-939.

[16] Ratha N. K., Chikkerur S., Connell .J. H, and Bolle R.M(2007) "Generating cancelable fingerprint templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561–72.

[17] Sutcu Y., Li Q., and Memon N. (2007) "Secure Biometric Templates from Fingerprint-Face Features," in Proc. CVPR Workshop on Biometrics, Minneapolis