IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 13, Issue 2 Ver. II (Mar. – Apr. 2018), PP 52-62
www.iosrjournals.org

Secure Authentication System Using Biometric Cryptosystem

Manjari Benhar Peethala
Lecturer, Electronics and Telecommunication Department, St. John College Of Engineering And Management Mumbai, Maharashtra, India
Corresponding Author: Manjari Benhar Peethala

Abstract : *Online digital information security is gaining drastic significance with the boost and progression of internet communication. With the advent of ecommerce and ebanking and its further evolution, the traditional methods of personal identification like token based methods and knowledge-based methods like PINs, passwords are no longer sufficient for secure transfer of critical data online. Though Biometric Authentication systems are comparatively a better option, they can be vulnerable to several attacks when it comes to Authentication online. Hence, Biometric Cryptosystems are proposed to enhance the security of biometric authentication systems and to create revocable representations of individuals. Alternatively, Steganography techniques play a crucial role in encapsulating encoded biometric data behind an unpredicted carrier. The proposed system employs CASIA-FingerprintV5 database of fifty fingerprint samples and emphasizes on providing improved security to the critical biometric data in two stages (i.e. Biometric Cryptosystem followed by Steganography) before it is transferred online to the Authenticator. At the Authenticator side, the verification and identification process are carried out using Euclidean distance and Hausdorff distance. On analyzing the experimental results, it can be concluded that the proposed system performs better matching when Euclidean distance is used.*

Keywords – *Authentication, Biometric Cryptosystem, Minutiae, Open Networks, Steganography.*

Date of Submission: 15-03-2018 Date of acceptance: 30-03-2018

I. Introduction

Security is one of the prime concerns in the present world scenario. Safeguarding critical digital information and privacy of the client's personal information is of priority of any online system. Nowadays most of the valuable data and documents are being stored in an organization server system and many individuals share personal information over the World Wide Web. Hence, the need for providing security and approving only the authorized client to access the system is becoming crucial as well as challenging. Biometric Authentication is thereby employed in several applications and it is gradually gaining attention in the field of research. Several biometrics like iris, face, fingerprint, retina, etc., are used in providing security to the digital information in addition to the use of secret keys [2].

1.1 Biometric based Authentication

The process of approving the uniqueness of individuals according to their physiological (i.e. face, retina, fingerprint, iris) or behavioral traits like signature is called Biometric Authentication. During the process of biometric authentication, biometric features of an individual are compared with the various biometric samples in the database. Permission to access a system or data is approved only when there is adequate match. Biometric systems are gaining more attention as trustable replacements to password-dependent security systems, as it eliminates the need to remember passwords. Also, biometric samples are very difficult to steal and reproduce. Moreover, it also offers non-repudiation [2].

1.2 Biometric Cryptosystem

Sending out critical biometric data over open networks or internet without any protection or encapsulation is risky. Thereby, to overcome this risky scenario, the concept of Biometric Cryptosystem which involves integrating biometric features with cryptography came into existence. The fundamental idea behind the concept of Biometric Cryptosystems is that the biometric trait ensures client authentication, whereas a standard key generation scheme looks after the other components of control (i.e. secure communication of biometric data over open network). Hence, Biometric Cryptosystems are gaining more popularity in the research domain. Biometric Cryptosystems have been developed to offer strong security mechanisms and to create revocable representations of individuals by combining biometrics with cryptography [9].

1.3 Steganography (critical data hiding)

The use of Steganography further elevates the security of a given Biometric Cryptosystem. Steganography term is derived from the Greek language which means secret communication that involves hiding critical information in an unpredicted carrier. This unsuspected carrier can be a text document, audio, image or a video. While Cryptography concentrates on methods to make critical information meaningless (Encryption) to unauthorized parties or imposters, Steganography looks after concealing the information itself. In other words, Steganography hides the very existence of the presence of a secret information [9].

II. Related Works

Manjari Benhar Peethala and Sujata Kulkari in [1] have used RC4 Key generation Biometric Cryptosystem and DCT based Steganography for unimodal prototype authentication system.

Vincenzo Conti, Salvatore Vitabile, Filippo Sorbello in [2] have fused RSA algorithm with Fingerprint template. Asymmetric key generation is used to generate public key for enrolment phase and private key for authentication phase.

Mr.P.Balakumar, Dr.R.Venkatesan in [3] performed experiments comparing the multimodal biometric system and unimodal biometric system. The multimodal system shows better performance than unimodal system.

Hisham Al-Assam, Rasber Rashid and Sabah Jassim in [4] have integrated Biometric Cryptosystems along with Steganography for secure mutual authentication along with a key exchange algorithm. However, the authors have used primitive techniques like Biometric Key Binding for Biometric Cryptosystem, RLSB for Steganography respectively and obtained lower FAR and FRR.

On further research it was found that Biometric Key Binding technique had certain limitations which can be overcome by Biometric Key Generation Technique for Biometric Cryptosystems. Y.J. Chin, T.S. Ong, A.B.J. Teoh, K.O.M. Goh in [5] has performed Biometric template fusion using hybrid template protection method. This paper also enlightens with Biometric Key Generation advantages over Biometric Key Binding.

The biometric features are transformed into suitable form before generation of Cryptography key in [6] by the authors Yao-Jen Chang, Wende Zhang, and Tsuhan Chen. The distinguishable feature generation is done by techniques like cascaded LDA, GSMMS followed by stable key generation using one-bit approach and multi M bit approach.

Due to the growing use of Internet, information security over open networks becomes a topic of major concern. Conventional Cryptographic techniques (i.e. knowledge- based methods) involves the user to keep the keys in mind, but in general it is impractical. For this very reason, Lifang Wu et al. in [7] proposed and developed a biometric cryptosystem depending on the face biometrics.

Neha Agrawal, Marios Savvides in [8] have implemented various Steganography techniques for hiding the biometric data with varied results based on BER parameter. Out of the different techniques, Single Bit hiding using Multiple DCT Coefficients has the lowest BER of 0.8% with highest accuracy. This technique thereby helps to develop a robust Biometric Authentication System.

Storage of the biometric templates and Cryptography keys can be a matter of concern for biometric authentication applications, since the negotiation or any deterioration of templates or keys inevitably compromises the information protected by those keys. Weiguo Sheng et al in [9] developed a new technique, which needs neither the storage of biometric templates nor the Cryptography keys, by openly producing the keys from statistical characteristics of biometric data.

Anil K J, Mut Uludag in [10] discussed about the methods for secure transmission of biometric templates over open networks which included Steganography and Watermarking. However, in their project, the biometric template undergoes Steganography without Encryption which threatens the security and integrity of data. The comparison between multimodal system and Biometric based cryptography key generated system is showed by David Marius Daniel, Borda Monica in [11]. The fingerprint data and iris data are transformed into their respective feature vectors. The final feature vector is converted into 256-bit cryptography key. Biometric based cryptography key generated system has lower FAR and FRR as compared to simple multimodal system.

Sujata Kulkarni, Dr.R.D. Raut and Dr.P.K.Dakhole in [12] have used Kekre's wavelet transform for global feature extraction of finger-vein framework. The proposed algorithm is examined on self-database of 128 x 128 size of 500 samples over 50 users from teenagers to senior citizen for better recognition.

Allam Mousa and Ahmad Hamad in [13] have examined the effect of different parameters of the RC4 algorithm for data encryption. The execution time of the RC4 algorithm for wide range of encryption key lengths and file sizes were evaluated. Various datatypes were also analyzed.

Due to the advantage of directly producing cryptographic key from biometric template, A. Jagadeesan and K. Duraiswamy in [14] proposed and implemented a 256-bit Biometric cryptography key generation algorithm. The 256-bit key was generated from the multi-biometric template which was formed by fusing the extracted fingerprint features and iris features at feature level.

Roli Bansal, Priti Sehgal and Punam Bedi in [15] have put forth in-depth literature over fingerprint feature Minutiae. The Minutiae points are broadly classified as ridge endings and bifurcations. The authors have given detailed explanation of a variety of techniques for extracting the fingerprint Minutiae. These techniques are broadly classified as those working on binarized images and those that work on gray scale images.

III. Proposed System Design

The proposed system is executed in the following two phases:

3.1 Registration Phase

In the Registration phase, the fingerprint biometric sample of the client is given as an input to a Biometric Key Generation Algorithm to generate 256-bit unique Key. This 256-bit unique Key is then stored in Authenticator Database as shown in Fig. 3-1. Instead of storing biometric template (Minutiae) directly, we generate 256-bit keys from biometric feature vectors and store these keys in the Authenticator database. Each client registers three samples of his or her fingerprint at different instances of time with varied pressures and orientations.

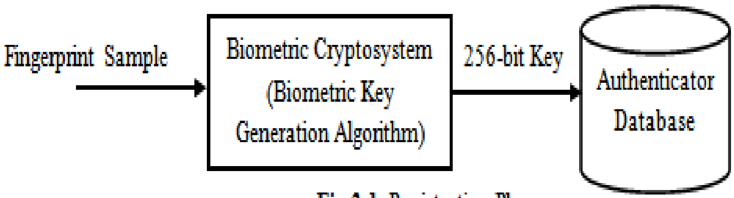

Fig 3-1. Registration Phase

3.2 Verification and Identification Phase

After the client's samples are registered in the Authenticator database, he needs to undergo the Verification and Identification Phase as shown in Fig. 3-2. In this phase, the client is required to once again input the fingerprint which is applied to the Biometric Cryptosystem algorithm to produce the 256-bit unique Key. This unique key is further encoded to form a Biometric Lock. The Biometric Lock is concealed behind an unsuspected cover image (carrier) using Steganography encoder to produce the Stego image. The Stego image is next communicated over the open network or internet. At the Authenticator's side, the Steganography decoder receives the Stego image and produces back the encapsulated Biometric Lock. Now, the 256-bit Key generated from the received Biometric Lock and the 256-bit Key registered in the Authenticator database during the Registration process are applied to the reverse algorithm of Biometric Cryptosystem to produce their respective Biometric samples. If the fresh fingerprint sample matches with the registered fingerprint sample retrieved from the database, the client will be accepted as a genuine one. On the other hand, if the matching fails, then the system will reject him as an imposter. In the proposed system, the matching process is carried out using either the Euclidean or Hausdorff distance.

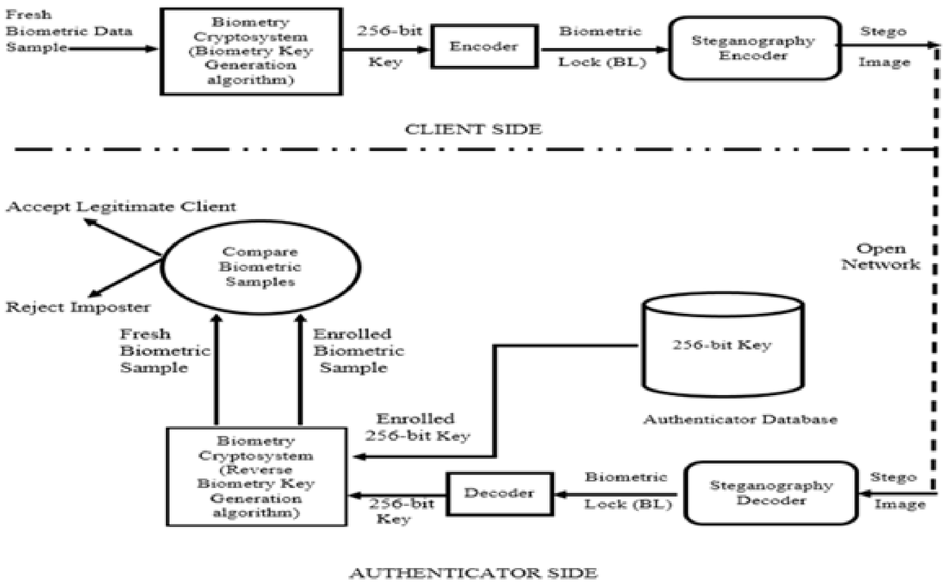

Fig 3-2. Verification and Identification Phase

Fig 3-2. Verification and Identification Phase

During Verification, the client's fingerprint sample is compared with his own remaining two fingerprint samples in the database. During Identification, the client's fingerprint sample is matched with the fingerprint samples of all the other clients in the database.

IV. Research Methodology

The combination of Steganography with Biometric Cryptosystem is the prime focus of the proposed system for enhanced authentication, encapsulation from online network attacks and security.

4.1 Tools

Software: Matlab R2013b
Biometric trait: Fingerprint
Database: CASIA Fingerprint Image Database (v 5.0)
Biometric feature: Minutiae (Ridge, bifurcations)

4.2 Biometric Cryptosystem

Biometric Cryptosystems are intended to securely bind a secret key to the biometric data of a client or generate a secret key from a biometric trait. They are classified as Biometric Key Binding Technique and Biometric Key Generation Technique. The Biometric Key Binding Technique comprises of binding a secret key with the original biometric sample to form a biometric lock. However, this technique can be easily reversed by the attacker once he gets any information regarding secret key using brute force methods. Conversely, Biometric Key Generation Technique creates a secret key from the original biometric sample itself to form a biometric lock. As a result, the attacker is denied access to the secret key since it is produced from biometric sample only which is unique for every client. Due to this benefit, the Biometric Key Generation Technique is employed in the proposed system.

4.2.1 Minutiae Extraction

Fingerprint image is utilized as the biometric sample in this system. This sample image undergoes binarization followed by the thinning process. This thinned image is applied to morphological Hit or Miss transform to obtain true minutiae.

A. Bifurcation Extraction

The pixels of an image having only three neighbours in a 3x3 neighbourhood and these neighbours are not adjacent to each other are called as the Bifurcations.

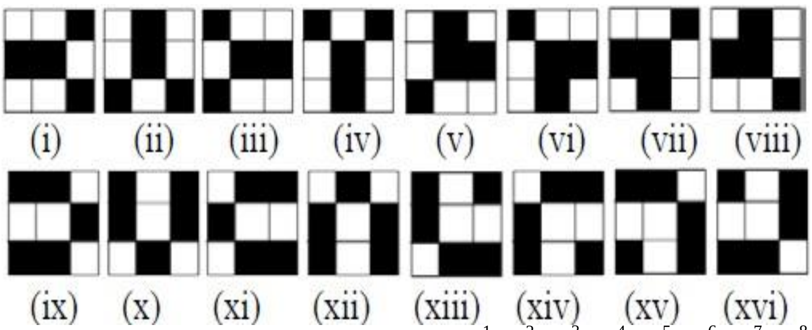

Fig. 4-1. (i) to (viii) Structuring sequence $S_1 = (S_1^1, S_1^2, S_1^3, S_1^4, S_1^5, S_1^6, S_1^7, S_1^8)$ and (ix) to (xvi) Structuring sequence $S_2 = (S_2^1, S_2^2, S_2^3, S_2^4, S_2^5, S_2^6, S_2^7, S_2^8)$

Hence, by applying Hit or Miss transform on X by S, the minutiae image N1 containing bifurcations is obtained as follows [14].

$$N1 = X \otimes S \qquad (1)$$

Where, X is the thinned image and S is the sequence of structuring element pairs (S1, S2) as shown in Fig. 4-1.

B. Ridge Extraction

The pixels of image having only one neighbour in a 3x3 neighbourhood is called as the Ridge endings.

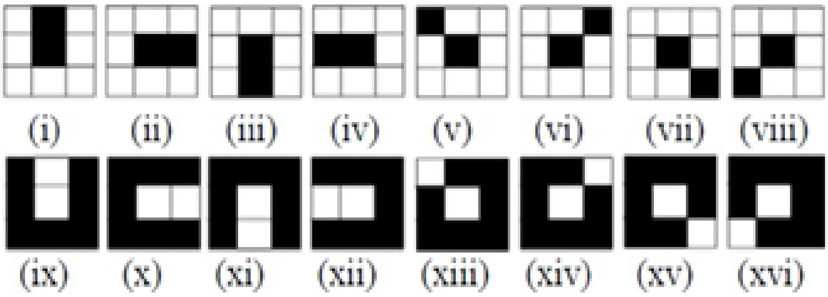

Fig. 4-2. (i) to (viii) Structuring sequence $S_1 = (S_1^1, S_1^2, S_1^3, S_1^4, S_1^5, S_1^6, S_1^7, S_1^8)$ and (ix) to (xvi) Structuring sequence $S_2 = (S_2^1, S_2^2, S_2^3, S_2^4, S_2^5, S_2^6, S_2^7, S_2^8)$

By applying Hit or Miss transform on X by S, the minutiae image N2 containing ridge endings is obtained as follows [14].

$$N2 = X \otimes S \qquad (2)$$

Where, S is Structuring sequence (S1, S2) for ridge extraction as shown in Fig. 4-2.

4.2.2 RC4 Algorithm for Biometric Key Generation

The proposed system uses only a particular initial section of the RC4 algorithm to generate pseudo random sequence or a 256-bit Key directly from Minutiae feature vectors [12].

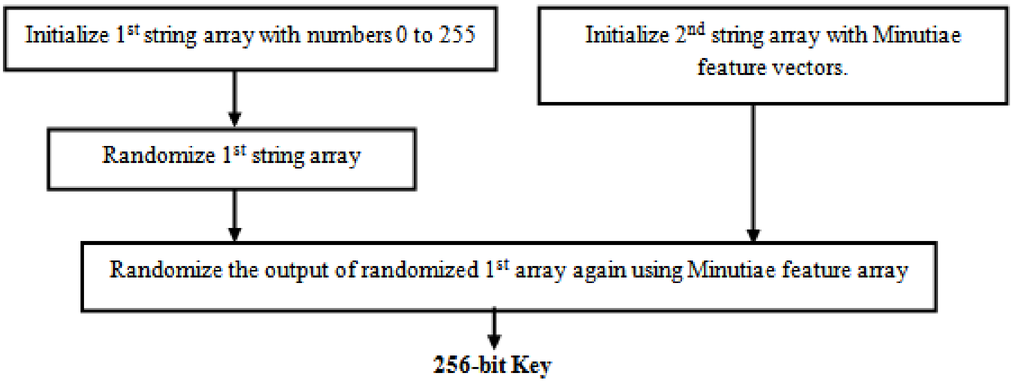

Fig. 4-3. Flowchart of the RC4 Algorithm used in Proposed System

4.3 DCT Steganography

Hiding of the critical data can be achieved using various Steganography techniques. Out of all these techniques, the proposed system uses Single Bit hiding using Multiple DCT Coefficients is considered to be more robust to image noise and compression artifacts in [7]. In this technique, the signs of multiple DCT coefficients are changed to embed one bit of biometric lock in contrast to using only one DCT coefficient for hiding the biometric data.

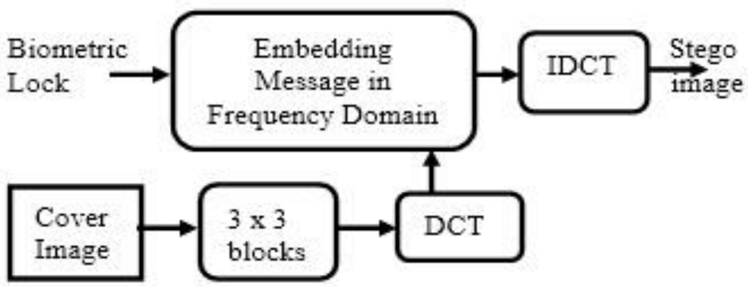

Fig. 4-4. Steganography Encoder

Stego image is formed by embedding the Biometric Lock to the Cover image in frequency domain as shown in Fig. 4-4. The resulting Stego image is transferred over the network.

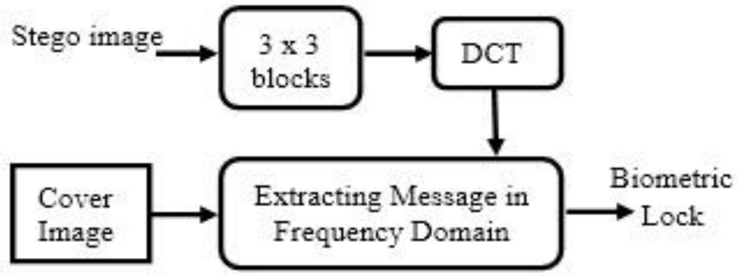

Fig. 4-5. Steganography Decoder

This Stego image reaching the Authenticator's side is given to the Steganography decoder to retrieve the Biometric Lock.

4.4 Matching

Let P be 256- bit Key corresponding to a client which has just entered for identification in the system and Q be one of 256-bit Keys already registered in the Authenticator database.

4.4.1 Euclidean distance

Euclidean distance E between P-key and Q-key is given as:

$$E = \sqrt[2]{\left\{\sum_{i=1}^{256}(|P_i - Q_i|)\right\}^2} \qquad (3)$$

is computed between the P-key and all the other keys stored in the database. The minimum Euclidean distance E, corresponds to the Authentic Client during identification. During verification, calculation of minimum E is between the P-key and the remaining two Keys corresponding to the client with P Key only.

4.4.2 Hausdorff distance

Hausdorff distance H between P-key and Q-key is given as:

$$H(P, Q) = \max\{h(P, Q), h(Q, P)\} \qquad (4)$$

$$h(P, Q) = \max_{p \in P}\{\min_{q \in Q}\{d(P, Q)\}\} \qquad (5)$$

Where h (P, Q) and h (Q, P) is directed Hausdorff distance from P to Q and Q to P respectively and min {d (P, Q)} is the minimum distance between P and Q. Here H is computed between the P-key and all the other keys stored in the database and the maximum Hausdorff Distance corresponds to the Authentic Client.

V. Performance evaluation

The proposed system performs experiments in following two broad categories as:

1. The Memory Storage space for Final Keys in comparison to Minutiae features storage size.
2. TAR and FAR of the Proposed System during the verification and the identification process each.

5.1 Memory Storage

This system comprises registered fingerprints of 50 users. Each user has given his or her 3 fingerprints at different orientations and pressures. All together there 150 (i.e. 50 x 3) fingerprint samples to be registered in the Authenticator database. The following table distinguishes the memory space required for storing 256-bit Final Keys and for storing the minutiae feature vectors for 150 fingerprint samples of 50 Clients.

Table 5-1. Memory Storage Size

No.	Case	Memory Storage Size
1	When Minutiae feature vectors are stored in Authenticator database	2.46 Mb
2	When 256-bit Final Keys are stored in Authenticator database	50 Kb

From Table 5-1, it is clear that space required for storing the 256-bit Final Keys is much small as compared to that of Minutiae feature storage. Due to this compact storage size, the proposed system stores 256-bit Final Keys for 150 fingerprint samples of 50 clients in the Authenticator database instead of the minutiae features.

5.2 Proposed System Analysis (i.e. TAR and FAR)

The proposed system was tested on all these 150 fingerprint image samples belonging to 50 clients. Each client has a unique Client ID. For example, Client 4 (i.e. User 4) has the ID=103, Client 5 (i.e. User 5) has the ID=104 and so on to Client 50 (User 50) which has the ID=149. On the other hand, each client has registered 3 fingerprint samples which is represented as _0, _1, _2. For example, the 3 samples belonging to Client 4 (i.e. User 4) have been given Client IDs as 103_0, 103_1, 103_2 as shown in Table 5-2.

Table 5-2. Proposed System results for 50 Legitimate Clients undergoing Verification, Identification process.

Client ID	Result using Euclidean distance	Result using Hausdorff distance	Client ID	Result using Euclidean distance	Result using Hausdorff distance	Client ID	Result using Euclidean distance	Result using Hausdorff distance
100_0	User 1	User 1	117_0	User 18	User 18	134_0	User 35	User 35
100_1	User 1	User 1	117_1	User 18	User 18	134_1	User 35	User 35
100_2	User 1	User 1	117_2	User 18	User 18	134_2	User 35	User 35
101_0	User 2	User 2	118_0	User 19	User 19	135_0	User 36	User 36
101_1	User 2	User 2	118_1	User 19	User 19	135_1	User 29	User 36
101_2	User 2	User 2	118_2	User 19	User 19	135_2	User 36	User 36
102_0	User 3	User 3	119_0	User 20	User 20	136_0	User 37	User 37
102_1	User 22	User 3	119_1	User 20	User 32	136_1	User 37	User 42
102_2	User 3	User 3	119_2	User 20	User 20	136_2	User 37	User 37
103_0	User 4	User 4	120_0	User 21	User 21	137_0	User 38	User 38
103_1	User 4	User 4	120_1	User 21	User 21	137_1	User 38	User 38
103_2	User 4	User 4	120_2	User 21	User 21	137_2	User 38	User 38
104_0	User 5	User 5	121_0	User 22	User 22	138_0	User 39	User 39
104_1	User 5	User 5	121_1	User 22	User 22	138_1	User 39	User 39
104_2	User 5	User 5	121_2	User 22	User 22	138_2	User 39	User 39
105_0	User 6	User 6	122_0	User 23	User 23	139_0	User 40	User 40
105_1	User 6	User 6	122_1	User 23	User 23	139_1	User 40	User 40
105_2	User 6	User 6	122_2	User 23	User 23	139_2	User 40	User 40
106_0	User 7	User 7	123_0	User 24	User 24	140_0	User 41	User 41
106_1	User 7	User 7	123_1	User 24	User 24	140_1	User 35	User 41
106_2	User 7	User 7	123_2	User 24	User 24	140_2	User 41	User 41
107_0	User 8	User 8	124_0	User 25	User 25	141_0	User 42	User 42
107_1	User 8	User 8	124_1	User 25	User 25	141_1	User 42	User 42
107_2	User 8	User 8	124_2	User 25	User 25	141_2	User 42	User 42
108_0	User 9	User 9	125_0	User 26	User 26	142_0	User 43	User 43
108_1	User 9	User 9	125_1	User 26	User 26	142_1	User 43	User 21
108_2	User 9	User 9	125_2	User 26	User 26	142_2	User 43	User 43
109_0	User 10	User 10	126_0	User 27	User 27	143_0	User 44	User 44
109_1	User 10	User 45	126_1	User 27	User 27	143_1	User 44	User 44
109_2	User 10	User 10	126_2	User 27	User 27	143_2	User 44	User 44
110_0	User 11	User 11	127_0	User 28	User 28	144_0	User 45	User 45
110_1	User 11	User 11	127_1	User 28	User 28	144_1	User 45	User 45
110_2	User 11	User 11	127_2	User 28	User 28	144_2	User 45	User 45
111_0	User 12	User 12	128_0	User 29	User 29	145_0	User 46	User 46
111_1	User 12	User 12	128_1	User 29	User 29	145_1	User 46	User 34
111_2	User 12	User 12	128_2	User 29	User 29	145_2	User 46	User 46
112_0	User 13	User 13	129_0	User 30	User 30	146_0	User 47	User 47
112_1	User 13	User 13	129_1	User 30	User 30	146_1	User 47	User 47
112_2	User 13	User 13	129_2	User 30	User 30	146_2	User 47	User 47
113_0	User 14	User 14	130_0	User 31	User 31	147_0	User 48	User 48
113_1	User 14	User 14	130_1	User 31	User 31	147_1	User 48	User 48
113_2	User 14	User 14	130_2	User 31	User 31	147_2	User 48	User 48
114_0	User 15	User 15	131_0	User 32	User 32	148_0	User 49	User 49
114_1	User 15	User 15	131_1	User 32	User 32	148_1	User 49	User 49
114_2	User 15	User 15	131_2	User 32	User 32	148_2	User 49	User 49
115_0	User 16	User 16	132_0	User 33	User 33	149_0	User 50	User 50
115_1	User 16	User 16	132_1	User 33	User 33	149_1	User 50	User 50
115_2	User 16	User 16	132_2	User 33	User 33	149_2	User 50	User 50
116_0	User 17	User 17	133_0	User 34	User 34			
116_1	User 16	User 17	133_1	User 34	User 34			
116_2	User 17	User 17	133_2	User 34	User 34			

5.3 Verification using Euclidean Distance

It is evident from Table 2 that when User 3 gives the fingerprint sample corresponding to client ID 102_1 to the system, his sample is recognized as User 22 which is an error. On the other hand, when User 3 gives the fingerprint sample corresponding to client ID 102_0 and ID 102_2 to the system, his sample is recognized as correctly as User 3 with no error. As a result, when 102_0 sample is compared with 102_1(error), there is no matching (i.e. 0% recognition) and when 102_0 sample is compared with 102_2, there is correct matching (i.e. 100% recognition). Therefore, the average TAR for user 3 using Euclidean distance is 50% and FAR also is 50%. The same scenario repeats when Euclidean distance is used for verification of User 36 and User 41. The remaining Clients (i.e. Users) have 100% TAR and 0% FAR.

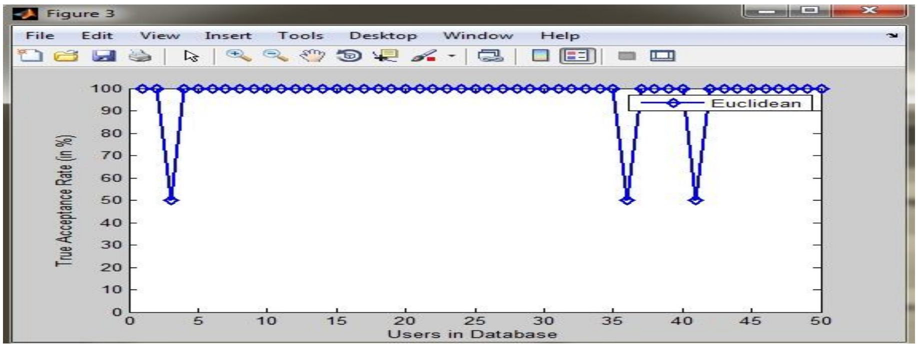

Fig. 5-1. Verification using Euclidean distance (TAR)

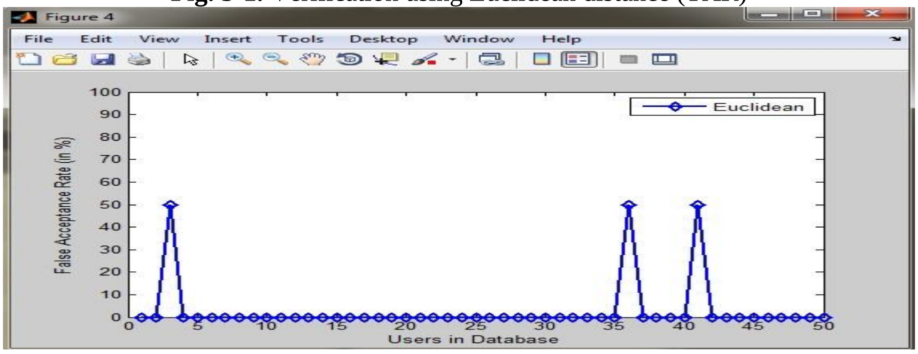

Fig. 5-2. Verification using Euclidean distance (FAR)

5.4 Verification using Hausdorff Distance

Just as Euclidean distance, the same scenario occurs when Hausdorff distance is employed for matching during Verification process. However, the Verification process using Hausdorff distance gives an average TAR of 50% and FAR of 50% for User 10, User 20, User 37, User 43 and User 46.

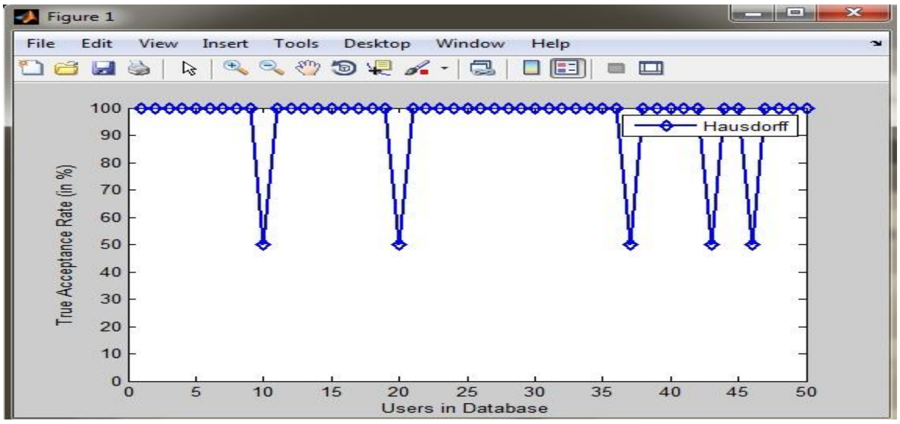

Fig. 5-3. Verification using Hausdorff distance (TAR)

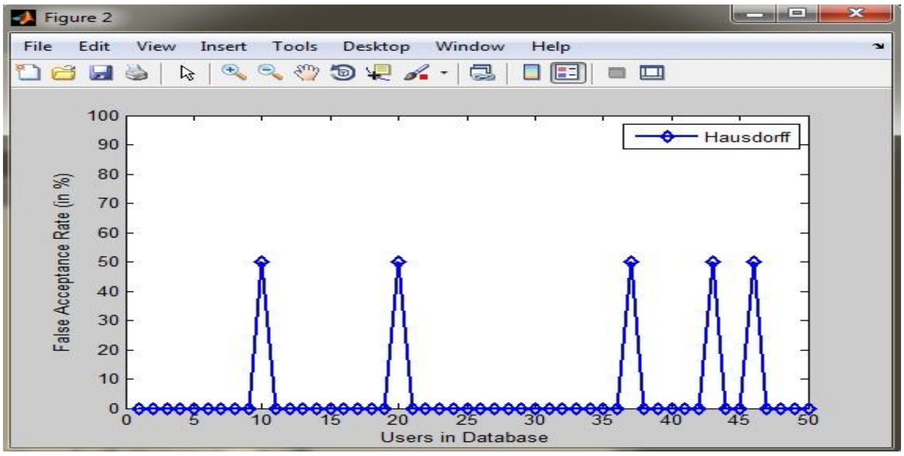

Fig. 5-4. Verification using Hausdorff distance (FAR)

5.5 Identification using Euclidean distance

When User 3 inputs the fingerprint sample corresponding to client ID 102_1 into the system, his sample is matched with samples of all other clients in Authenticator's database (i.e. 100_1, 101_1…..149_1). The best matching is given as the output. However, in the proposed system, User 3 is recognized as User 22 which is an error. Hence, the average TAR for User 3 using Euclidean distance is 0% and FAR is 100%. The same scenario repeats when Euclidean distance is used for Identification of User 36 and User 41. The remaining Clients (i.e. Users) have 100% TAR and 0% FAR.

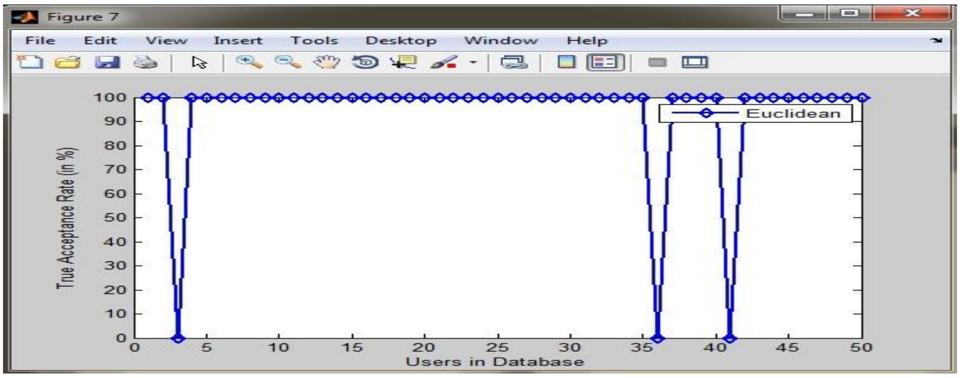

Fig. 5-5. Identification using Euclidean distance (TAR)

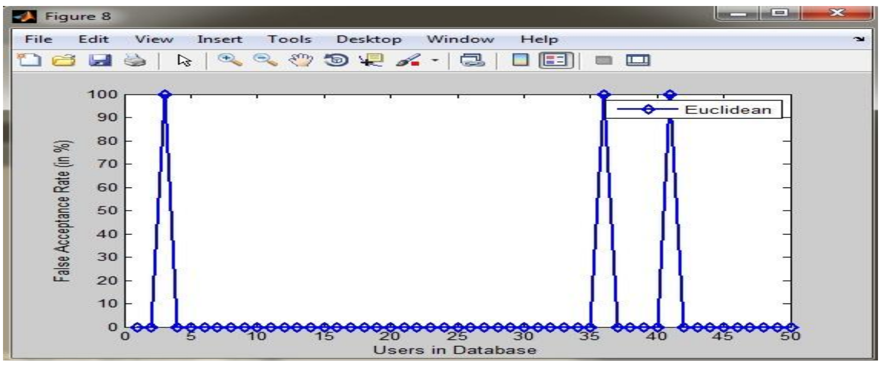

Fig. 5-6. Identification using Euclidean distance (FAR)

5.6 Identification using Hausdorff distance

Just as Euclidean distance, the same scenario occurs when Hausdorff distance is employed for matching during Identification process.

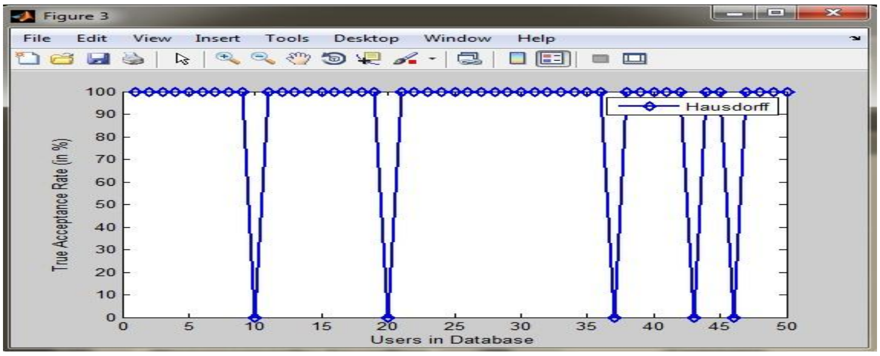

Fig. 5-7. Identification using Hausdorff distance (TAR)

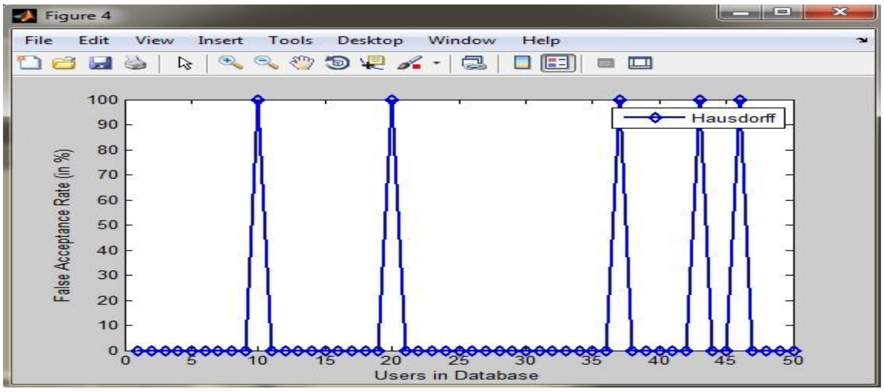

Fig. 5-7. Identification using Hausdorff distance (TAR)

However, the Identification process using Hausdorff distance gives an average TAR of 0% and FAR of 100% for User 10, User 20, User 37, User 43 and User 46.

5.7 System Performance Analysis

From Table 5-3, we can conclude that the proposed system shows better performance when Euclidean distance is employed for matching.

Table 5-3. Proposed system Overall Performance

Modules	TAR	FAR
Verification using Euclidean distance	97%	3%
Identification using Euclidean distance	94%	6%
Verification using Hausdorff distance	95%	5%
Identification using Hausdorff distance	90%	10%

VI. Conclusion

Security of online ecommerce or ebanking transactions is the need of present world. Providing the online authentication system access only to the authorized users is getting more challenging day after day as the number of impostors and security attacks are growing. Biometric systems can be employed for securing ecommerce or ebanking transactions. However, there is always a threat of these critical biometric data to be stolen or altered over the open networks. The proposed system has an increased two-level protection which includes Biometric Cryptosystem followed by Steganography for secure transmission of unimodal fingerprint trait. Hence we can conclude that the proposed system is a secure and robust Biometric Authentication system.

Acknowledgements

Portions of the research in this paper use the CASIA FingerprintV5 collected by the Chinese Academy of Sciences' Institute of Automation (CASIA).

References

[1] Manjari Benhar Peethala, Sujata Kulkarni, “ Integrating Biometric Cryptosystem with steganography for authentication”, IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE), pp. 28-31, 2016.

[2] Vincenzo Conti, Salvatore Vitabile, Filippo Sorbello, “Fingerprint Traits and RSA Algorithm Fusion Technique”, IEEE Complex, Intelligent and Software Intensive Systems(CISIS), pp.351-356, 2012.

[3] Mr.P.Balakumar, Dr.R.Venkatesan, “A Survey on Biometrics based Cryptographic Key Generation Schemes”, International Journal of Computer Science and Information Technology & Security , vol. 2, 2012.

[4] Hisham Al-Assam, Rasber Rashid and Sabah Jassim, “Combining Steganography and Biometric Cryptosystems for Secure Mutual Authentication and Key Exchange”, The 8th International Conference on Internet Technology and Secured Transactions, pp.369-374, 2013.

[5] Y.J. Chin, T.S. Ong, A.B.J. Teoh, K.O.M.Goh, “Integrated biometrics template protection technique based on fingerprint and palm print feature-level fusion”, Elseiver Journal- “Information Fusion 18”, pp.161-174 , 2013.

[6] Yao-Jen Chang, Wende Zhang and Tsuhan Chen, “Biometrics-based cryptographic key generation”, IEEE International Conference on Multimedia and Expo (ICME), vol. 3, pp.2203–2206, 2004.

[7] Lifang Wu, Xingsheng Liu, Songlong Yuan and Peng Xiao, “A novel key generation cryptosystem based on face features”, IEEE 10th International Conference on Signal Processing (ICSP), pp.1675–1678, 2010.

[8] Neha Agrawal, Marios Savvides, “Biometric Data Hiding: A 3 Factor Authentication Approach to Verify Identity with a Single Image Using Steganography, Encryption and Matching”, Computer Vision and Pattern Recognition Workshop in IEEE Computer Society Conference, pp. 85 – 92, 2009.

[9] Weiguo Sheng, G. Howells, M. Fairhurst and F.Deravi, “Template-Free Biometric-Key Generation by Means of Fuzzy Genetic Clustering”, IEEE Transactions on Information Forensics and Security, vol. 3, no. 2, pp.183–191, 2008.

[10] Anil K J, Umut Uludag, “Hiding biometric data”, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 11, pp.1494-1498, 2003.

[11] David Marius Daniel, Borda Monica, “Unconventional methods used in order to generate Cryptographic keys”, Acta Electrotehnica, vol. 56, pp.126-130, 2015.

[12] Sujata Kulkarni, Dr. R.D. Raut, Dr.P.K. Dakhole, “Vein Pattern for Personal Authentication”, International Journal of Electronics, Communication & Soft Computing Science and Engineering, IETE, 2015.

[13] Allam Mousa and Ahmad Hamad, “Evaluation of the RC4 Algorithm for Data Encryption”, International Journal of Computer Science & Applications, vol. 3, 2006.

[14] A. Jagadeesan, K. Duraiswamy, “Secured Cryptographic Key Generation from Multimodal Biometrics”, International Journal of Computer Science and Information Security (IJCSIS), vol. 7, 2010.

[15] Roli Bansal, Priti Sehgal and Punam Bedi, “Minutiae Extraction from Fingerprint Images - a Review”, International Journal of Computer Science Issues (IJCSI), vol. 8, no 3,2011.

[16] CASIA-FingerprintV5, http://biometrics.idealtest.org/”

IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) is UGC approved Journal with Sl. No. 4198, Journal no. 45125.

Manjari Benhar Peethala "Secure Authentication System Using Biometric Cryptosystem." IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) 13.2 (2018): 52-62.