ISSN: 0976-9102(ONLINE)
DOI: 10.21917/ijivp.2012.0052

MULTIMODAL BIOMETRIC AUTHENTICATION USING PARTICLE SWARM OPTIMIZATION ALGORITHM WITH FINGERPRINT AND IRIS

A. Muthukumar[1], C. Kasthuri[2] and S. Kannan[3]

[1]*Department of Electronics and Communication Engineering, Kalasalingam University, India*
E-mail: muthuece.eng@gmail.com
[2]*Department of Electronics and Communication Engineering, Madurai Institute of Engineering and Technology, India*
E-mail: kkas@in.com
[3]*Department of Electrical and Electronics Engineering, Kalasalingam University, India*
E-mail: kannaneeeps@gmail.com

Abstract

In general, the identification and verification are done by passwords, pin number, etc., which is easily cracked by others. In order to overcome this issue biometrics is a unique tool for authenticate an individual person. Nevertheless, unimodal biometric is suffered due to noise, intra class variations, spoof attacks, non-universality and some other attacks. In order to avoid these attacks, the multimodal biometrics i.e. combining of more modalities is adapted. In a biometric authentication system, the acceptance or rejection of an entity is dependent on the similarity score falling above or below the threshold. Hence this paper has focused on the security of the biometric system, because compromised biometric templates cannot be revoked or reissued and also this paper has proposed a multimodal system based on an evolutionary algorithm, Particle Swarm Optimization that adapts for varying security environments. With these two concerns, this paper had developed a design incorporating adaptability, authenticity and security.

Key words:

Multibiometric, Cryptosystem, Score Level Fusion, PSO Algorithm, Feature Extraction

1. INTRODUCTION

Most biometric systems that are presently used in real time applications, typically uses a single biometric characteristic to authenticate a user. The challenges encountered by the unimodal biometric systems are: 1) Noise in the sensed data: At the time of authentication, the feature presented to the system may be contaminated by noise due to imperfect acquisition conditions or slight variations like Scar in the fingerprint.2) Non-universality: The biometric system may not be able to acquire required biometric data. 3) Spoofing by which imposters overcome the system through an introduction of a fake sample, behavioral traits such as voice, signature and the physical characteristic fingerprint (fake fingers can be molded from plastic, or gelatin) are all vulnerable to spoof attacks. 4) Intra-class variations: caused by a user who is improperly interacting, with the sensor (e.g., incorrect facial pose), or when the characteristics of a sensor are modified during authentication phase (e.g., ultrasonic versus solid-state fingerprint sensors). The key generation from the single biometric data consists of three modes: key release mode, key binding mode, and key generation mode [4]. In that paper fuzzy vault based key generation is used with fingerprint as a biometric data [4]. Some of the limitations of a unibiometric system can be addressed by designing a system that integrates multiple sources of biometric information. Such systems, known as Multimodal Biometric Systems, are more reliable due to the presence of multiple, independent pieces of data. Most of the multimodal biometric systems proposed in the literature use a fixed combination rule and a fixed decision threshold level to achieve the desired performance. These systems will only provide a fixed level of security and often have to contend either with high or else with low false acceptance rate based on the security level of the application. In an access controlled system, security concerns are related to the perceived threats to the application. Therefore, reliable multimodal biometrics algorithms should be adaptable to the desired level of security. The design and development of such multimodal biometrics systems that can automatically select the decision threshold to achieve the desired performance is one of the issues investigated in this paper. This paper also considers about the template protection mechanism, since secure storage of biometric templates has become an increasingly important issue in the biometric authentication systems. Once revealed, user's template would potentially allow an attacker to obtain sufficient information to mimic the person. Hence it is important to prevent attackers from learning the biometric templates of the users. Attacks on the template can lead to the vulnerabilities such as; a template can be replaced by an impostor's template to gain unauthorized access into the protected resources. A physical spoof can be created from the template to gain unauthorized access to the resource. This is a very challenging issue because it is extremely difficult to build a server or a device that can never be compromised, and once compromised, the biometric templates cannot be revoked like passwords. This problem is more difficult compared to traditional authentication systems based on passwords or certificates, where compromised user identities can be easily revoked. Hence Biometric is combined with cryptography, Biometric cryptosystems were originally developed for the purpose of either securing a cryptographic key using biometric features. Unimodal Biometric systems are vulnerable to many problems such as noisy data, non-universality and spoofing. This leads to a high false acceptance rate and false rejection rate, limited discrimination capability, and lack of performance. The limitations of unimodal biometric systems can be overcome by using multimodal biometrics where two or more sources have been used to validate identity. In [1] high security is been achieved by means of verifying the user's presence continuously. Their system (fingerprint and face biometric data) requires the presence of the user at all the time, for continuous monitoring, hence it is not suitable for access control applications. In [2], their system requires the user to satisfy all the three modalities if it is intended for a high security application, for a low security application it is enough to satisfy two or one out of three modalities. In their approach, the system administrator provides the decision rules in accordance with the security level. Hence this is not an automatic way of providing decision strategies. In [3], they have developed a system that adapts itself for different security environments. Their approach involves fusion at the score level, in which the similarity scores have been generated by matching the templates in a plaintext form. In the proposed system authors have adapted the fuzzy vault technique [4], [5] to secure the fingerprint and iris template; the matching will be performed at the transformed template domain, achieving template security. In [3], the adaptability framework, was not implemented for the combination of iris and fingerprint, because these two modalities will be used for large scale identification, in the proposed system authors have verified the adaptability for the combination.

In multimodal biometrics, the next step is the fusion of various biometrics. The fusion methods are basically classified into three types. They are sensor level fusion, and decision level fusion and score level fusion. In that fusion classifier after the matching process, it can be classified as rank level, abstract level and measurement level fusion [9]. This proposes a scenario of integrating the biometrics of fingerprint and Iris combined with fuzzy vault to form a multimodal biometric crypto system and also examines the system using the score level fusion. The rest of this paper is arranged as follows. Section 2 describes about structure of the proposed work. Section 3 and 4 gives the details of the encoding and decoding phase of fingerprint as well as Iris. Section 5 discuss about the optimization process. The experimental results and the analysis are given in Section 6. Finally Section 7 provides the conclusion.

2. PROPOSED SYSTEM

The multibiometric cryptosystem is a new tool to give the solution for security of templates as well as authentication of the individual users. In this paper, fingerprint and Iris are acting as biometric keys for the fuzzy vault systems. The overview of the proposed work is shown in Fig.1 and 2. This work consists of two phases; the first one is an enrollment phase, and the second one is a verification phase.

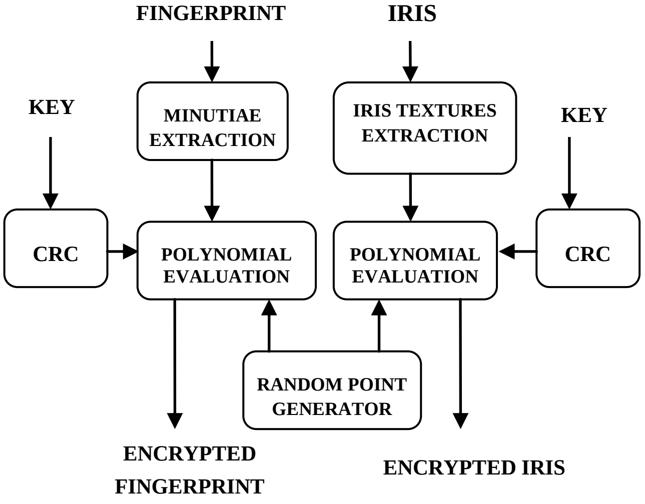

Fig.1. Proposed Architecture for Enrollment Phase

The enrollment phases shown in Fig.1, in this the biometric templates are undergone random transformation using the polynomial construction. This enhances the privacy because it enables the creation of revocable templates and prevents cross matching of templates across different applications.

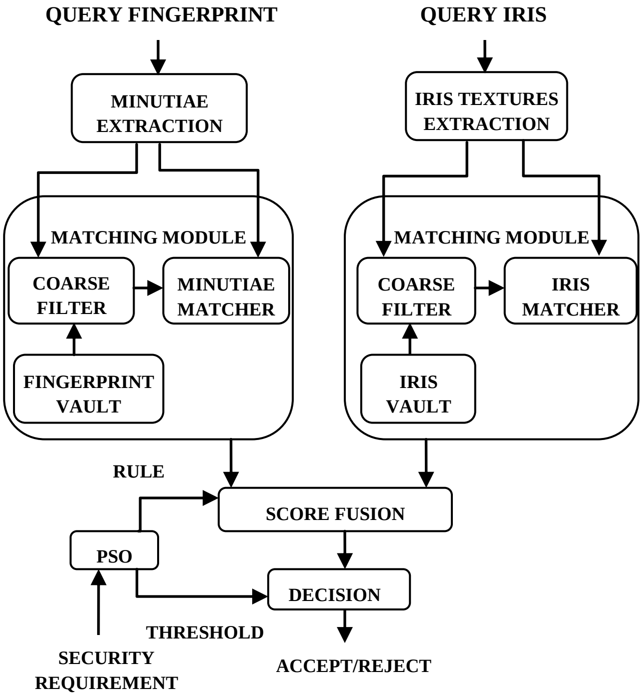

Fig.2. Proposed Architecture for Identification Phase

In the second phase, Identification stage as shown in Fig.2, scores have been combined optimally by means of Particle swarm optimization algorithm to achieve the desired security level.

3. FINGERPRINT ENCODING AND DECODING

3.1 FINGERPRINT VAULT ENCODING

The three main parameters in the vault scheme are r, s, and n. The parameter r denotes the number of points in the vault that lie on the polynomial and s represents the number of imposter points that are added and n denotes the degree of the encoding polynomial. For Minutiae Extraction the proposed system follows the algorithm described in [6], which is depicted in the Fig.3. Each valid minutia point is been characterized by three parameters: x-coordinate, y-coordinate, orientation, and ridge associated with it. The minutiae points are represented as a set M^T. Fig.4, shows the result of minutiae extraction algorithm. We applied a Minutiae selection algorithm to sort the minutiae based on their quality and sequentially selected the minutiae starting with the highest quality minutia. The local quality index proposed in [6] is used to estimate the quality of each minutia in M^T. Moreover, the algorithm selects only well-separated minutiae (i.e., the minimum distance between any two selected minutia points is greater than a threshold $\delta_1 = 25$). The distance D_M between two minutia points' m_i and m_j is defined as,

$$D_M(m_i,m_j) = \sqrt{(u_i - u_j)^2 + (v_i - v_j)^2} \; + \; \beta_M \Delta(\theta_i.\theta_j) \quad (1)$$

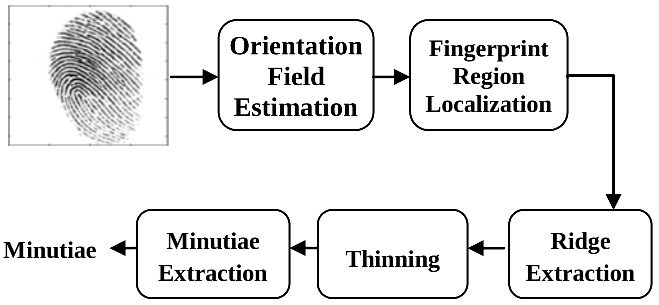

Fig.3. Minutiae Extraction Process Flow

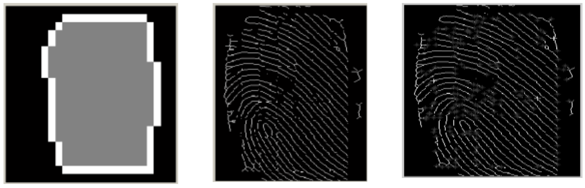

Fig.4(a) Region of Interest (b) Thinning (c) Minutiae

where, and u and v indicate the row and column indices in the image, and θ represents the orientation of the minutia with respect to the horizontal axis. β_M and $\Delta(\theta_i.\theta_j)$ are the weights associated with the orientation attribute. Let $SM^T = (m^T{}_j)j = 1$ to T denotes the selected minutiae set.

An imposter point m = (u, v, θ) is randomly chosen such that, $u \in \{1, 2 \ldots U\}$, $v \in \{1, 2 \ldots V\}$, $\theta \in \{1,2 \ldots 360\}$. The point m is added to a imposter point set IM if the minimum distance between m and all points in the set SM^T Ụ IM is greater than δ1.A 16-b CRC code is appended to key K to obtain a new key K' containing 16(n+1) bits. The generator polynomial (IBM CRC-16) G (w) $=w^{16}+w^{15}+w^2+1$, is used for generating the CRC bits. Then K' is encoded into a polynomial P of degree n in Galois field F by partitioning it into n(n+1) 16-b values $c_o, c_1, .., c_n$ and considering them as coefficients of P, n=8.

The selected template minutiae(genuine points) and the randomly selected points(imposter points)are quantized and encoded into the Galois field F as $X=\{x_j\}_{j=1 \text{ to } r}$ and $Y=\{y_k\}_{k=1 \text{ to } s}$. The polynomial P is then evaluated at all of the points in the selected minutiae set X to obtain the set $P(X) = \{P\ (x_j)\}_{j=1 \text{ to } r}$. The genuine minutiae points X and the genuine points that are lying on the polynomial P(X) form as a Genuine set G= $\{(X_j, P\ (X_j)\}_{j=1 \text{ to } r}$.

A set $Z = \{z_k\}_{k=1 \text{ to } s}$ is obtained by randomly selecting values P. The imposter set is defined as $IM = \{(y_k, z_k)\}_{k=1 \text{ to } s.}$ The union of genuine and imposter set is denoted as E and it is been stored in the system as an encrypted entity (Vault). The Vault encoding pocess is shown in Fig.5.

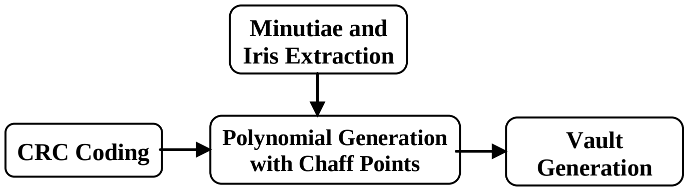
Minutiae and Iris Extraction
CRC Coding
Polynomial Generation with Chaff Points
Vault Generation

Fig.5. Vault Encoding for fingerprint and Iris

3.2 FINGERPRINT VAULT DECODING

Minutiae points are obtained from the Query Fingerprint image, based on the local quality Index. As explained in the encoding stage, only well separated minutiae points having a distance greater than $\delta_1 = 25$ is taken into account. The selected Query minutiae set $SM^Q = (m_j^Q)_{j=1}^r$ are used to filter the imposter points from the Vault.

The 16-b strings in the vault are partitioned into three strings of length B_u=6, B_v=6 and B_θ=5 and are quantized to obtain the set $M^V = m_i^V = (u_i, v_i, \theta_i)_{i=1}^s$. The process of coarse filtering is, the i^th element of set M^V is marked as an imposter point if the minimum distance between the point $m^V{}_i \in M^V$ and all of the selected minutiae $m_j^Q \in SM^Q$ in the query is greater than a threshold $\delta_2 = 30$,obtained the set $SM^V = (m_k^v) N_{k=1}^V$, contains only those elements that are not marked as Imposter point. $N^V$is the number of points in M^V that are not marked as imposter, N^V<< s. A minutiae matcher [6] is applied to determine the corresponding pairs of minutiae from the sets SM^Q andSM^V.

4. IRIS VAULT ENCODING AND DECODING

4.1 IRIS VAULT ENCODING

The iris image normalization, enhancement, Feature extraction, were same as detailed in [7], Fig.7, shows the result of iris normalization. The x and y coordinates of nodes and endpoints (8 bits each) in the iris Textures are taken as a feature set u. The 128 bit key is used to find the coefficients of the polynomial p with degree 8. 16 bit CRC is used to generate the polynomial bits. A total of 144 bits are used to generate a polynomial of 9(144/16) coefficients with degree D=8. Hence $p(u) = c^8u_8 + c^7u_7 + ... + c^0$.

The 144 bit code is divided into non overlapping 16 bit segments and each segment is declared as a specific coefficient. Iris circular rim containing node points is divided into 4 quadrants and for each quadrant one 16 bit segment is assigned.

Genuine set G is found by projecting the polynomial p using N iris template features $u_1, u_2, \ldots u_n$ Thus G ={ [u_1, p(u_1)], [u_2, p(u_2)],….}. Imposter set I is found by randomly assuming M points $c_1, c_2 \ldots c_m$ which do not overlap with feature set u. Another set of random points d1, d2, .d_m are generated, with a constraint that pairs (c_j,dj) j=1,2,…M do not fall onto the polynomial p(u).

Fig.8 shows the selected template minutiae set that will form as a Genuine Set. Imposter set I is then I= {(c_1, d1), (c_2, d2)….}. Union of these two sets, G ∪ I, will form as an encrypted Iris entity (vault V). Fig.9 shows the Vault in which the selected template minutiae are hidden among imposter points.

4.2 IRIS VAULT DECODING

Let SM^Q = {u*1, u*2, .u*N} be the points from query Iris.

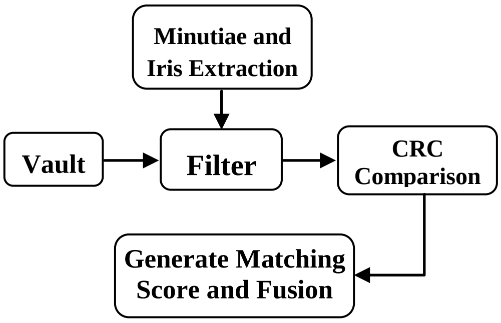
Minutiae and Iris Extraction
Vault
Filter
CRC Comparison
Generate Matching Score and Fusion

Fig.6. Vault Decoding for fingerprint and Iris

If u*i , i=1,2,…N is equal to values of vault V, then vi , i=1,2,…(M+N), the corresponding vault point is added to the list SM^V.

A iris matcher is applied to determine the corresponding pairs of nodes and end points from the sets SM^Q andSM^V.The matching scores obtained is normalized before fusion. The Vault decoding pocess is shown in Fig.6.

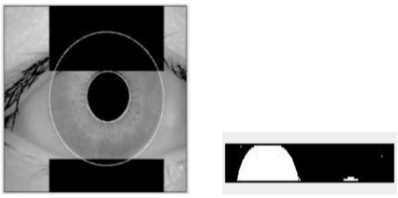

Fig.7(a). Localized Iris, (b) Normalization

5. OPTIMAL MULTIMODAL SYSTEM

PSO is an evolutionary search algorithm [8] that optimizes a problem by iteratively trying to improve a particle solution corresponds to a given measure of quality. In the proposed approach, PSO is employed for the adaptive selection of fusion rule and decision threshold corresponding to the desire security level, the required security level is the external parameter given to the system in terms of cost of falsely accepting an imposter C_{FA}. The Bayesian cost, which is the error measure, is expressed as,

$$E=C_{FA}\,F_{AR}\,(ŋ)+C_{FR}\,F_{RR}\,(ŋ) \qquad (2)$$

$$C_{FA}+C_{FR}=2.$$

where C_{FA} is the cost of falsely accepting an imposter, C_{FR} is the cost of falsely rejecting the genuine individual , F_{AR}(ŋ) is the global or the combined false acceptance rate and F_{RR}(ŋ) is the combined false rejection rate at decision threshold from the multimodal biometric system.

The PSO algorithm, for the given error cost ($C_{FA)}$, it searches for all the possible fusion rules and operating point (threshold) that will minimize the cost E. If Security is heightened, cost of authenticating an imposter C_{FA} will have a higher value; in accordance the optimization algorithm gives the fusion parameters.

In the search space, each particle is characterized by three continuous variables; w_1 and w_2 parameters of score-level fusion rule and, decision threshold ŋ, and a two bit discrete binary variable representing four different score-level fusion rules. The Scores obtained from the minutiae and iris matcher as shown in the Fig.2 is combined dynamically by any one of the below fusion rules as follows,

$$\text{Sum} = \sum_{j=1}^{n} S_j W_j \qquad (3)$$

$$\text{Product} = \prod_{j=1}^{n} S_j^{\;w_j} \qquad (4)$$

$$\text{Exponential sum} = \sum_{j=1}^{n} \exp(S_j) W_j \qquad (5)$$

$$\text{Tan hyperbolic sum} = \sum_{j=1}^{n} \tanh(S_j) W_j \qquad (6)$$

The initial positions of the particle are randomly selected in the search space. After each iteration, the particle in the PSO moves to a new position in the solution space depending upon the particle's best p_{ak} and global best position p_{gk}. The particle updates its velocity whenever the particle obtains a lower fitness value (Bayesian Cost E) in the search space by

$$\begin{aligned} V_{ak}\ \ t+1\ &= wv_{ak}\ \ t\ \ +c1r1\ \ pak\ \ t\ - x_{ak}\ \ t \\ &\quad + c2r2\ \ p_{gk}\ \ t\ \ - x_{ak}\ \ t \end{aligned} \qquad (7)$$

where, *w* is the inertia weight between 0 and 1 and provides a balance between global and local search abilities of the algorithm. The accelerator coefficients c_1 and c_2 are positive constants and r_1 and r_2 are two random numbers in the 0–1 range. The corresponding position vector is updated by

$$x_{ak}\,(t+1) = x_{ak}(t)+v_{ak}(t+1) \qquad (8)$$

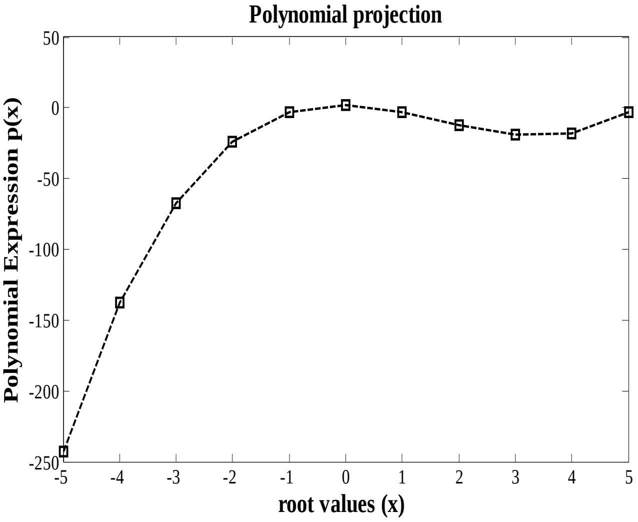

Fig.8. Polynomial Projection

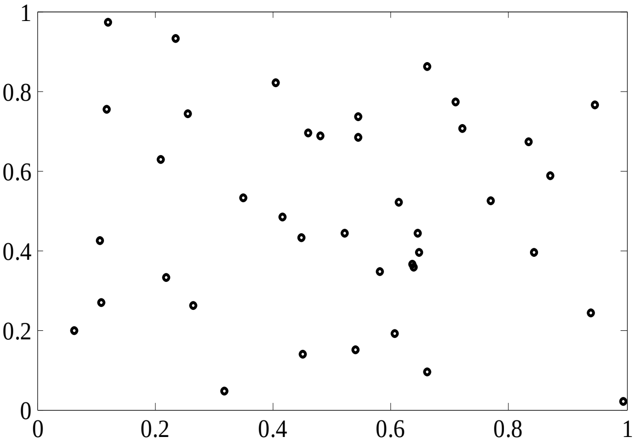

Fig.9. Overlap of polynomial projection with chaff points for the formation of Vault

6. EXPERIMENTAL RESULTS

The fingerprint images from the FVC2004 DB^2 (560 x 290 pixel) database, and iris images from IITD iris database (consists of low-resolution 320 x 240 pixel iris images) were used for our simulation. Here two databases, one for fingerprint and another one for iris was utilized. Two unibiometrics fuzzy vaults are constructed using the features extracted from fingerprint and iris separately; hence we have constructed 10 vaults for each modality. In our implementation, the number of genuine points in the vault ‘r’ ranges from 18-20; the total number of points in the vault ranges from 200-220. The fingerprint and iris matching score employed min–max normalization. The distribution of the normalized matching scores from the two biometric modalities is shown in Fig.10 and 11.The PSO parameters c_1, c_2, w were fixed at 1, 1, 0.8, respectively. Fig.12 shows the adaptive selection of the score-level rules, with the variation of security level, where security levels essentially the sum of cost of false acceptance and cost of false rejection.

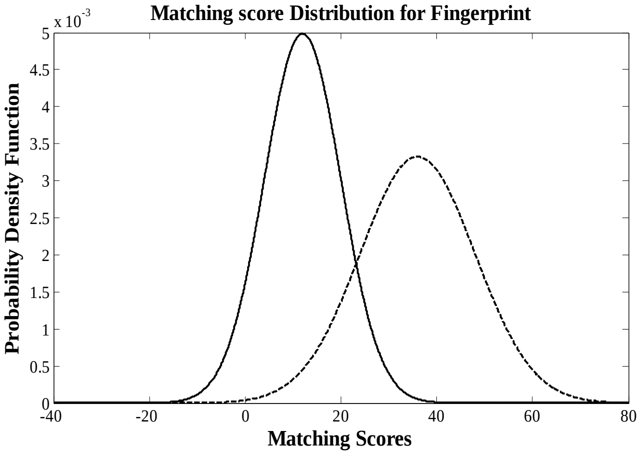

Fig.10. Matching score Distribution for Fingerprint

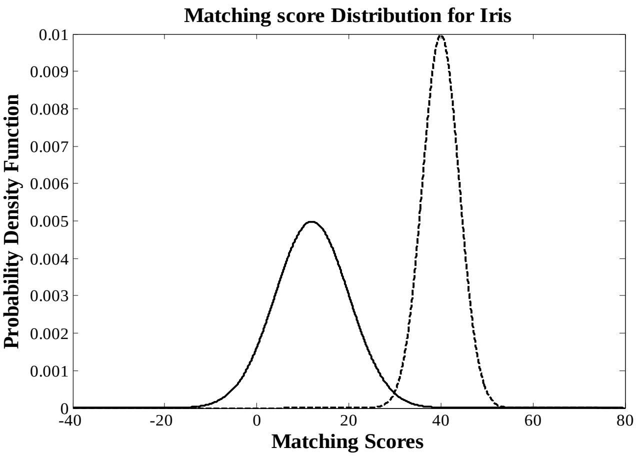

Fig.11. Matching score Distribution for Iris

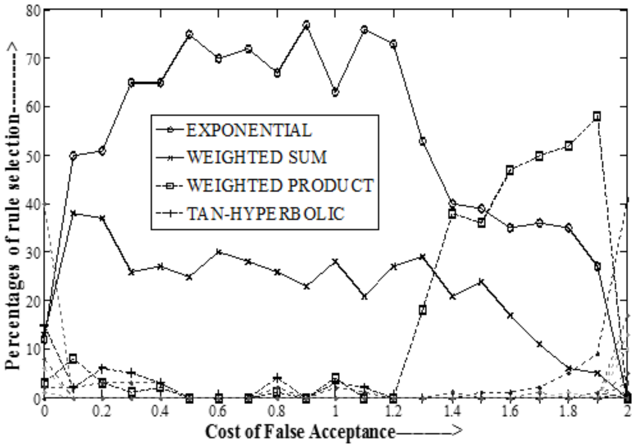

Fig.12. Adaptive Rule selection

The parameters for optimal combination such as fusion rules, weights, and decision threshold have computed offline in our process, for every possible security level in the range 0–2 and have stored in a look-up table. Depending on the security requirement, the parameters can be taken from the look-up table and used for performing authentication/verification tasks. Therefore, the verification time from the proposed methodology is quite equivalent to any other non-adaptive multimodal biometric system. The experimental results presented in this paper suggested that our proposed framework consistently performs well for different security environments, while ensuring the security of biometric system. The number of imposter points is very low; the False Acceptance rate (FAR) is high with the high degree of polynomial. According to this, higher the FAR, Genuine Acceptance rate (GAR) is also high but False Rejection rate is low. If this is not happened, FRR is high, and then system will not be valid one. This system gives high FAR with increase in degree of polynomial and genuine points of finger print and iris which is shown in Fig.13. The FAR and FRR is calculated by Eq.(9) and Eq.(10).

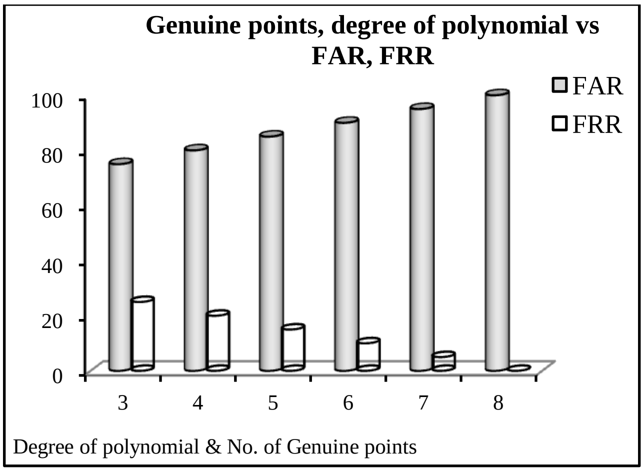

Fig.13. Graph of degree of polynomial vs. FAR, FRR

$$\text{FAR} = \frac{\text{No. of imposter attempts accepted}}{\text{Total No. of imposter attempts}} \qquad (9)$$

$$\text{FRR} = \frac{\text{No. of Genuine attempts rejected}}{\text{Total No. of Genuine attempts}} \qquad (10)$$

Finally this paper was utilized two databases, so here for simulation, a set of fingerprint and iris was enrolled and for verification also the same set fingerprint and iris has been involved. In real time applications, we can create a database with fingerprint and iris of a same person and that database can also be utilized in this system also. This paper provides the template security and authentication for a particular user.

7. CONCLUSION

In this paper, the idea of combining the fuzzy vaults combined with two individual biometrics to form the cryptosystem by generating the polynomial construction using chaff points were generated. After that verification phase, the secret key is decoded with comparing the biometric with vault, and from that matching scores are generated and next that are undergone various adaptive rules of PSO algorithm, the optimized result was generated, so that genuine acceptance rate was increased for this multimodal cryptosystem in order to provide authentication and security.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the management of Kalasalingam University, Krishnankoil, Tamil Nadu, India, for the facilities provided to carry out this research work.

REFERENCES

[1] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, “Continuous verification using multimodal biometrics”, *IEEE Transaction on Pattern Analysis and Machine Intelligence*, Vol. 29, No. 4, pp. 687–700, 2007.

[2] R. W. Frischholz and U. Deickmann, “BioID: A multimodal biometric identification system”, *Computer*, Vol. 33, No. 2, pp. 64–68, 2000.

[3] D. Zhang, V. Kanhangad, and A. Kumar, “A New Framework for Adaptive Multimodal Biometrics Management”, *IEEE Transactions on Systems, Man, Cybernetics-Part C: Applications and Reviews,* Vol. 38, No. 5, pp. 92–102, 2010.

[4] Anil K. Jain *and* Sharath Pankanti, “Fingerprint-Based Fuzzy Vault: Implementation and Performance”, *IEEE Transaction on Information Forensics and Security*, Vol.2, No.4, pp.744-747, 2007.

[5] E. Srinivasa Reddy and I. Ramesh Babu, “Performance of Iris Based Hard Fuzzy Vault”, IJCSNS *International Journal of Computer Science and Network Security*, Vol.8, No.1, pp. 297-304, 2008.

[6] L. Hong, A.K. Jain, and R. Bolle, “On-line fingerprint verification”, *IEEE Transaction on Pattern Analysis and Machine Intelligence,* Vol. 19, No. 4, pp. 302–314, 1997.

[7] Kumar and A. Passi, “Comparison and combination of iris matchers for reliable personal authentication”, *Pattern Recogniti*on, Vol. 23, No. 3, pp.1016–1026, 2010.

[8] R.C.Eberhart and J. Kennedy, “*Swarm Intelligence*”, San Diego, CA: Morgan Kaufmann, 2001.

[9] Anil Jain, Karthik Nandakumar and Arun Ross, “Score normalization in multimodal biometric systems”, *Journal of Pattern Recognition society,* Vol. 38, No.12, pp. 2270 – 2285, 2005

[10] Norman Poh and et’al “Benchmarking Quality-Dependent and Cost-Sensitive Score-Level Multimodal Biometric Fusion Algorithms”, *IEEE Transactions on information Forensics and Security,* Vol.4, No.4, pp.849-866, 2009.

[11] Nandakumar, K and Jain.A.K, “Multibiometric Template Security Using Fuzzy Vault”, *2nd IEEE International Conference Biometrics: Theory, Applications and Systems, 2008 (BTAS 2008),* 2008.

[12] Gobinath Subramaniam and et.al, “Des Enabled Fingerprint System*”, Proceedings of the International Conference on Man-Machine Systems (ICoMMS),* Batu Ferringhi, Penang, Malaysia , pp. 3A3-1 to 3A3-5, 2009.

[13] Xiangqian Wu, Ning Qi, Kuanquan Wang and David Zhang, “A Novel Cryptosystem based on Iris Key Generation”, *Fourth International Conference on Natural Computation* (ICNC'08), 2008.

[14] K.Saraswathi and Dr.R.Balasubramaniam, “Biocryptosystems for Authentication and Network Security-A Survey”, *Global Journal of Computer Science and Technology,* Vol.10, No.3, 2010.

[15] Hao Feng and Chan Choong Wah, “Private Key generation from on-line handwritten signatures”, *Journal Of Information, Management and Computer Security,* Vol. 10, pp. 159–164, 2002.

[16] Bruce Schneier, “Applied Cryptography Protocols, Algorithms” Wiley Publication, 2nd Edition.

[17] William Stallings, “*Cryptography and Network Security Principles and practice*”, Prentice Hall, 3rd Edition, 2003.

[18] Feng Zhao and Xiaoou Tang, “Preprocessing and post processing for skeleton-based fingerprint minutiae extraction”, *Elsevier transaction on pattern recognition,* Vol.40, pp.1270-1281, 2006.