Research Journal of Information Technology 6(1): 1-7, 2015
ISSN: 2041-3106; e-ISSN: 2041-3114

Submitted: September 24, 2014 Accepted: October 29, 2014 Published: February 01, 2015

Research Article

Structure and Performance Analysis of Multi Stage Biometric Cryptosystem

[1]S. Kannan and [2]V. Seenivasagam,
[1]Department of Computer Science and Engineering, Thamirabharani Engineering College, Tirunelveli,
[2]Department of Computer Science and Engineering, National Engineering College, Kovilpatti, India

Abstract: The system aims to bind many biometric cryptosystem using a linker and to increase the matching accuracy at low threshold values. We demonstrate a two stage biometric cryptosystem in which each system uses two different biometric templates. Shielding functions is used to encrypt the biometric template. A One-Time Seed (OTS) generated by the OTS generator is used to link the two biometric cryptosystem. Hash algorithm principle is applied to generate OTS. Finally, the performance of the system is analyzed in terms of False Acceptance Rate (FAR) and False Reject Rate (FRR) for the biometric cryptosystem whereas many classic and contemporary biometric cryptosystem work well at high threshold values, but sharply falls when the threshold values are lowered in the matching process.

Keywords: Biometric template, hashing function, one time seed, shielding functions, transforming algorithm

INTRODUCTION

Multi Stage Biometric Cryptosystem (MSBC) is designed to perform authentication process by accumulating evidence from the biometric traits (Rathgeb and Uhl, 2011) (e.g., face, fingerprint and iris). The system provides authentication in multiple stages. MSBC can provide greater accuracy in matching process over large population.

The Biometric System in general has many challenges and issues:

Biometric inequality: The environment and acquisition method plays a significant role in Biometric signals and their representation of a person (Rathgeb and Uhl, 2011). Also angle of communication of the user with acquisition device and variations of user traits due to various changes in physiological phenomena plays crucial role in the representation of biometric templates. (e.g., Variation in an individual face image due to different angle in pose).

Inconsistent presentation: The biometric signal acquired from the acquisition device depends upon both the biometric template and how the biometric template communicated with the device. (e.g., Variations in the pressure and contact of finger on the surface of the sensor).

Imperfect signal/representational acquisition: In real time, Biometric signal varies due to the change in the condition during the acquisition of the biometric signal (e.g., Skin dryness, ageing, Disease in skin, air humidity all results in variations images).

Biometric templates have many vital information of the user. So matching the biometric templates should be done in a fair manner. Thus the accuracy of matching biometric templates (Uludag *et al*., 2004) is very important and plays a key role in the authentication of process of Biometric cryptosystem. In this study we focus mainly on the accuracy of the matching process. The fundamental challenge in designing the biometric template matching scheme is to provide low threshold in matching the biometric traits in different circumstances.

Security is the basic of any authentication system. Many Biometric cryptosystem has limitations in the identification or verification process of Biometric template. The basic of security in Biometric cryptosystems is defined by the identification or verification of the Biometric template. Therefore limitations imposed by Biometric cryptosystems can be overcome by MSBC. The main advantages of MSBC are:

- It significantly improves the accuracy of matching process (biometric identification or verification)
- It overcomes the spoof attacks because there are multiple Biometric Cryptosystems.

In a cryptosystem using biometric traits, central database stores biometric images transformed to keys (Feng *et al*., 2010). As stated before, it is very difficult to get identical key for the same biometric

Corresponding Author: S. Kannan, Department of Computer Science and Engineering, Thamirabharani Engineering College, Tirunelveli, India

traits in different circumstances. (biometric invariance, inconsistent presentation, imperfect signal, representation acquisition) and thus matching becomes hard. In this study, to improve the accuracy in matching process, a MSBC is demonstrated. The focus of this paper is as follows:

- Define the MSBC and define the system based on the biometric level and cryptosystem level.
- Define security and matching of MSBC using two types of error measurement: FAR and FRR.
- Design a model of MSBC (two stage biometric cryptosystem) at the biometric level where different sets of biometric features can be used.
- Discuss the overview of the proposed models.

In the proposed MSBC, we analyze the accuracy and security by matching performance analysis and authentication analysis using CASIA iris database version 4 and MSU fingerprint database.

MATERIALS AND METHODS

Shielding functions: Let X be a biometric vector of fixed length. Let S be a secret key. X and S are combine together to form pre data Y. For this Y an inverse δ-contracting function G^{-1} is applied. This contracting function transforms Y to helper data W such that G(W, X) = S. For each feature of the biometric template the distance between the centre of nearest even-odd or odd-even interval is measured depending on the bits of S whether 0 or 1 is calculated δ-contracting function G. By including all residuals W is adjusted. The simplified illustration of shielding function on biometric template is shown in Fig. 1. A Shielding functions is a biometric cryptosystem that can be used to secure biometric traits represent in the form of binary vectors (e.g., Iris code). The biometric template b^E that we apply is an N-bit binary string. The Shielding functions (Linnartz and Tuyls, 2003) uses function S, which shields a code word c $\in C$ and by witnessing $b^E(0,1)^n$. The set C has set of error correcting code words of length n and N-bit. For C and b^E, a difference vector is calculated over $\delta \in (0,1)^n$ where b^E= c+δ and a hash value h(c) are stored as the shielded code S(c, b^E). Each $b^{E'}$, which is adjusted to X, using an adjusting vector. This vector is designed in such a way that it can rebuild C using the difference vector δ to translate $b^{E'}$ in the direction of b^E. The resultant is hashed and is examined against h(c).

The biometric cryptosystem acquire biometric template b^E at enrollment, selects a code word c $\in C$ calculate and stores the shield F(c, k). An authentication process is done using the witness $b^{E'}$ the system test whether x' yields a successful deshields. The biometric feature Z is used to calculated the G(W, Z) = $s^{-1}$by the authentication . The result of secrets^{-1}, is used to test the previously stored (v) and authentication or rejection is based upon it.

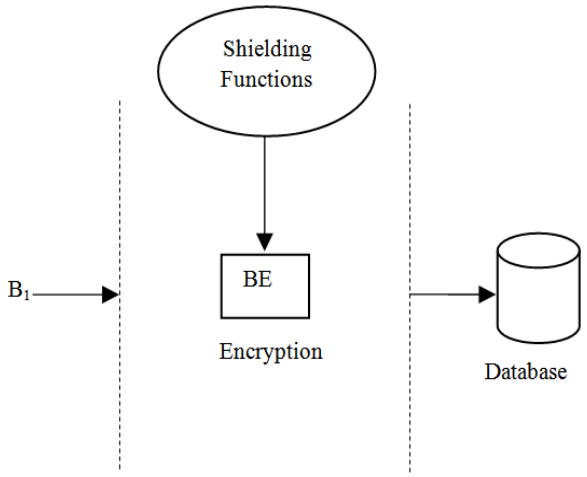

Fig. 1: Biometric cryptosystem using shielding functions

Basic theory of shielding function:

Definition 1: Let a function G(W, Y): $R^{n1+n2} \rightarrow \{0, 1\}^{n3}$ is defined over $\delta \geq 0$, a non-negative real number (Linnartz and Tuyls, 2003). The function G is called "δ-contracting" if and only if for all $X \in R^{n1}$ there exist at least one vector $W \in R^{n2}$ and one binary string $S \in \{0, 1\}^{n3}$ such that G(W, Y) is constant on a sphere with radius δ around X, i.e., G(W, X) = G(W, Y) = S for all $Y \in R^{n1}$ such that $\|X-Y\| \leq \delta$. The δ-contracting property guarantees that Y will be mapped to its counterpart value Z despite of noise for all measurements.

Definition 2: Let G(W, X): $R^{n1+n2} \rightarrow \{0, 1\}^{n3}$ be a function (Linnartz and Tuyls, 2003). The function G called "versatile " if and only if for all $S \in \{0, 1\}^{n3}$ and all $X \in R\ R^{n1}$, there exists (an efficient algorithm to find) at least one vector $W \in R^{n2}$ such that G(W, Y) = S.

A trivial ∞-contracting function is G(W, X) = Constant. However this function is not versatile. The property of versatility is relevant particularly for key establishment. A trivial versatile and ∞-contracting function is G(W, X) = C(W). However, in this solution W reveals the secret S, or at least, the conditional entropy H(S|W) = 0.

Theorem: If W is a constant, i.e., if G(W, Y) = C(Y) then either the largest contracting range of G is δ = 0 or G(W,Y) is a constant independent of Y.

Proof: Assume G is δ-contracting, with δ>0. Choose two points Y_1 and Y_2 such that $G(W, Y_1) = Z_1$ and $G(W, Y_2) = Z_2$. Define a vector $r = \lambda(Y_2-Y_1)$ such that $0 < \|r\| < \delta$. Then, $Z_1 = G(W, Y_1) = G(W, Y_1+r) = G(W, Y_1+2r) = \ldots = Z_2$ Thus $G(W, Y_1) = G(W, Y_2)$ is constant.

Definition 3: Let G(W,Y): $R^{n1+n2} \rightarrow \{0, 1\}^{n3}$ be a δ-contracting function with $\delta \geq 0$ and $\varepsilon \geq 0$ be a non-negative real number. The function G is called "ε

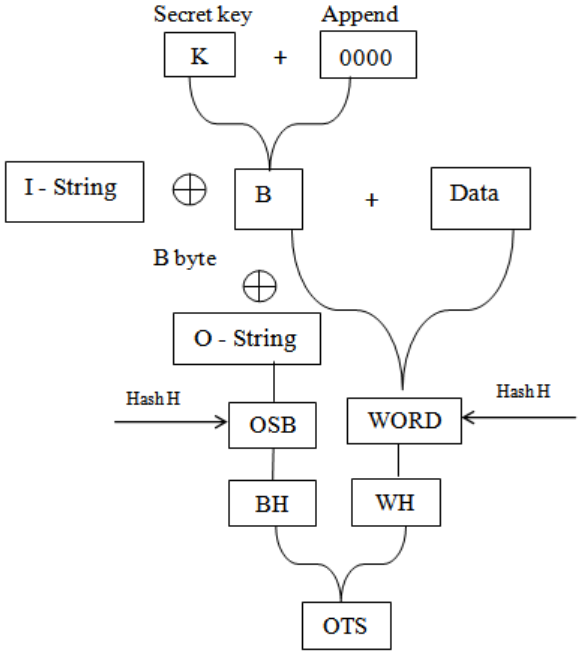

Fig. 2: Generation of OTS using HMAC

revealing" if and only if for all X ∈ R^{n1}there exists (an efficient algorithm to find) a contracting vector W∈ R^{n2} such that the mutual information I(W; S)<ε. Hence W conceals S: it reveals only a well-defined, small amount of information about S. Similarly, we require that V conceals S. However we do not interpret this in the information theoretic sense but in the complexity theoretic sense, i.e., the computational effort to obtain a reasonable estimate of (X or) S from V is prohibitively large, even though in the information theoretic sense V may (uniquely) define over S.

One time seed generator: One Time Seed (OTS) is an authentication code that is transmitted over an unreliable medium. This OTS is used by the user as linker code to interface MSBC. OTS generator works on the principle of Hash based Message Authentication Code (HMAC) algorithm (Arasu *et al*., 2013).

Definition of HMAC: HMAC has a cryptographic hash function H and a secret key K. Using compression function the date is hashed by iteration. Data are taken in blocks of length L 64 bytes (Mineta *et al*., 2008). The length of the authentication key K varies up to the Length L. Two different strings called outer string and inner string is used to produce the stream of word by performing XOR operation over the secret key K and then hashing. The algorithm is depicted in the Fig. 2.

The Algorithms is depicted as follows:

1) Create a B byte string by adding zeros at the end of K.
2) The inner string is XOR-ed with the B byte string produced in the step 1.
3) To the B byte string a sequence of data is added with "word".
4) To the resultant byte produced in the step3 Hash function is applied.
5) The outer string is applied to the XOR of the byte string.
6) The step 5 resultant is appended with the resultant of step 4
7) Finally H is applied to the "word" generated by step 6 and it gives the OTS.

Design model of MSBC: The key idea of MSBC is to form a multiple stage in the authentication process. Different biometric traits are used as framework of the authentication system. A friend function (in this system OTS) is used as the linker between different stages. Biometric templates is transformed into binary strings and binary strings are used as the input into one of the schemes known as shielding functions. Consider we use a two stage biometric cryptosystem and b_1E and b_2 E is two biometric templates we are using in this system. The shielding function is applied and a keyk_1 is extracted from b_1 E. After successful authentication an OTS is generated and this OTS links to the next stage. Now the shielding function is applied over the second biometric template .Thus a series flow of authentication is developed and each stage is cascaded using external friend function (OTS).

We propose an OTS linkage MSBC. It has three basic modules.

- Transforming algorithm
- Linker module
- Biometric cryptosystems

Transforming algorithm: The biometric template ${b_n}^{\epsilon}$of a user is represented in another form using the transforming algorithms. The biometric template ${b_n}^{\epsilon}$ is transformed into new form ${t_n}^{\epsilon}$ given by the transforming algorithm ${t_n}^{\epsilon} = \epsilon^{({b_n}^{\epsilon})}$. The biometric template B^{ϵ} is represented in real valued function such as binary string or point set. The transformed biometric template T^{ϵ} is also a binary string or point set that represented in a new vector using a secured key applied through shielding functions. To transform a real valued vector to binary string we first encircle the real valued vector elements one by one into a single definite circle. This single definite circle is converted into binary string of fixed length. To convert point set to binary string, each point is represented in a table. The number of points in the table its mean and variance are calculated. This mean and variance is used to calculate feature vector by reducing the dimensionality. To transform the binary string to point set, the binary string is divided by the number of segments, where each segment is considered as a point.

Linker module: The OTS generator generates a OTS which is communicated to the user through an external network. This OTS links two biometric cryptosystem build separately. Two biometric cryptosystem BC_1 and BC_2 are built in two different environments and works independently. The OTS is used as the key to pass from one biometric cryptosystem to second biometric cryptosystem.

Biometric cryptosystem: One biometric template $B^{\in} = \{b_1{}^{\in}, b_2{}^{\in}, .., b_n{}^{\in}\}$ is converted into a new secured string S_c during enrollment using the transformed biometric template $T^{\in}\{t_1{}^{\in}, t_2{}^{\in}, \dots, t^{\in}\}$ obtained using the shielding functions. In determining the security and matching performance, the above three modules plays a crucial role. The transforming algorithm without distracting the original characteristics of the biometric template should generate a compact transformed biometric vector (Nagar *et al*., 2011). The OTS generator should work from the confirmation from the first biometric cryptosystem and it should ensure to pass on the next biometric cryptosystem. The biometric cryptosystem should provide a strong framework over the leakage of original information of biometric templates. Thus optimization of the entire three modules is a challenging task in itself and is beyond the scope of this work. Since our objective of this proposed system is to give a viability of the framework of the multistage biometric cryptosystem, we propose simple algorithms for implementing these modules and do not focus on optimizing them.

MULTISTAGE BIOMETRIC CRYPTOSYSTEM IMPLEMENTATION

Biometric cryptosystem implementation using shielding function: Shielding functions are developed by constructing δ-contracting and ε-revealing biometric authentication systems. A model of X and N is zero mean jointly forms Gaussian random vectors with variance n_x^2 and σ_n^2 respectively. For the i-th dimension (1, 2, .. i) we have (n_1, n_2 …. n_i) of Y, W and the δ-contracting function is expressed using the equation:

$$c_i = \begin{cases} 1 \; if \; 2ab \; \le p_i + q_i < (2a+1)b \\ 0 \; if \; (2a-1)b \; \le p_i + q_i < ab \end{cases}$$
$$for \; any \; a = .., -1, 0, 1, \dots \quad (1)$$

where, q is a quantization step size. During enrollment, x_i is measured and the C will find a $w_i$such that the value of x_i+w_i is pushed to the nearest lattice point where x_i+ w_i+δ will be quantized to the same z_i for any small δ. This can be interpreted as a watermark of Quantization Index Modulation (Chen and Wornell, 2001). For the i-th dimension of S, the value of $w_i$will be:

$$q_i = \begin{cases} \left(2a + \frac{1}{2}\right) b - x_i \; if \; s_i = 1 \\ \left(2a + \frac{1}{2}\right) b - x_i \; if \; s_i = 0 \end{cases} \quad (2)$$

where, n = .., -1, 0, 1, 2, ... is chosen such that-q<w_i<q. The value of n is discarded, but the values of w are released as helper data. We analyze the case of a single specific dimension, where a secret message s = {-1, +1} is verified. The contraction range δ equals q/2. The probability that an honest couple Peggy-Victor makes an error in one dimension equals with:

$$P_e = 2Q\left(\frac{q}{2\alpha_n}\right) - 2Q\left(\frac{3q}{2\alpha_n}\right) + 2Q\left(\frac{5q}{2\alpha_n}\right) - \cdots \quad (3)$$

where, Q(x) is the integral over the Guassian pdf unity variance. The next analysis will quantify ε by calculating the leakage of information for our assumptions of the statistical behavior of the input signals X and W, where the statistics of W are determined by those of X and S. The signals in all dimensions are calculated in an identical manner, so we omit the index i.

We observe that for s_i= 1 w = (2n+1/2)q -x, so:

$$f_w(w|s_1 = 1) = \begin{cases} 0 \; for |w| > q \\ \sum_{n=-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_x} \mu \; for |w| > q \end{cases} \quad (4)$$

Here $\mu = exp\left(-\frac{\left((2n+1/2)q-w\right)^2}{2\sigma_x^2}\right)$

where, q * f(w/q) is a function of w/q. The solid lines depict f_W(w|s = 0) and the crosses depict f_W(w|s = 1). Information leaks whenever f_W(w|s = 1) ≠ f_W(w|s = 1). The symmetry properties f_W(w|s) = f_W(q-w|s) and f_W(w|s = 1) = f_W(-w|s = 0) apply. f_W(w|s = 1) has a maximum for w = q/2, which corresponds to highly likely values of x near x = 0. The unconditional probability density of W follows from f_W(w) = f_W(w|s = 1) P(s = 1)+f_W(w|s = 0) P(s = 0)+. and it is neither true that that f_W(w|s = 1) = 1 - f_W(-w|s = 1) nor that f_W(w) is constant. Using Bayes rule, the a posteriori probability p_{w1} on s = 1 can be expressed as:

$$p_{w1} = P(s = 1|W = w) = \frac{f_w(w|s_1=1)}{f(w)} P(s = 1) \quad (5)$$

Similarly, we can define p_{w0} also. Then, the mutual information I(W; S) follows from:

$$I(w; s) = \text{H(S)} - \int_{-q}^{q} H(S|W = w) \, \beta \, dw \quad (6)$$

Here H(S) stands for the information theoretic entropy of a discrete random variable S, defined as H(S) = - Σι P(S = i) $\log_2$ P(S = i). Since S takes the value 0 or 1 with probability 0.5, H(S) = 1 bit. Thus:

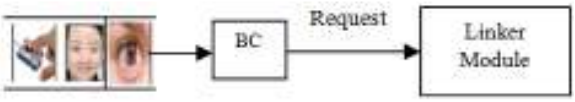

Fig. 3: User authentications the linker through the Biometric verifications

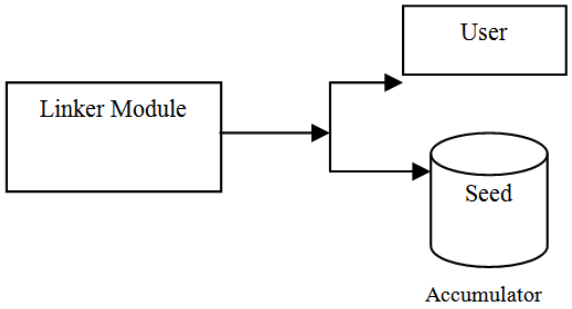

Fig. 4: OTS generation

$$I(w;s) = \mathrm{H(S)} + \rho \quad (7)$$

where,

$$\rho = \int_{-q}^{q} \{p_{w1} \log p_{w1} + p_{w0} \log(1 - p_{w0})\} \beta \, dw$$

$$\mathrm{I(w;\ s)} = 1 + \frac{1}{2}\int_{-q}^{q} \alpha \, log \frac{\alpha}{2\beta} dw + \frac{1}{2}\int_{-q}^{q} \{\gamma\} \, log \left\{\frac{\alpha}{2\beta}\right\} dw \quad (8)$$

Expanding the logarithm into separate terms, i.e., applying the rule log (a/b) = (log a -log b), we get:

$$\mathrm{I(w;\ s)} = 1 + \frac{1}{2}A + \frac{1}{2}\,B - \mathrm{C} \quad (9)$$

where,

$A = \int_{-q}^{q} \alpha \, log \ \alpha \, dw$

$B = \int_{-q}^{q} \{\gamma\} log\{\gamma\} dw$

$C = \int_{-q}^{q} \beta log 2\beta w$

Or simply:

$$\mathrm{I(w;\ s)} = \int_{-q}^{q} \alpha \, log \, \alpha \, dw - \int_{-q}^{q} \beta \, log \, \beta \, dw \quad (10)$$

Here,

$$\alpha = f_w(w|s = 1), \ \beta = f_w(w) \text{ and } \gamma = f_w(w|s = 0)$$

where, the quantization values is as crude as $q/\sigma_n = 1$ and they are sufficient to ensure small leakage ($\varepsilon << 10^{-5}$).

Linker module implementation: HMAC (Mineta *et al*., 2008) concept is used to generate OTS which is used as a linker. The linker module consists of following design elements:

- Generator module which produces OTS when it gets authentication from the biometric cryptosystem.
- Broadcast module delivers the OTS to the user through an external network.
- Verification module matches the OTS from the user with the original generated OTS.

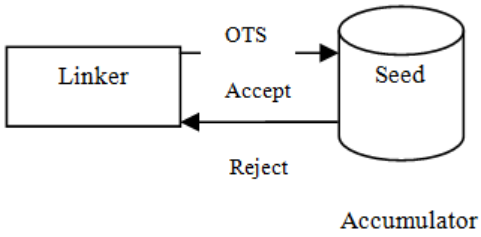

Fig. 5: OTS verification

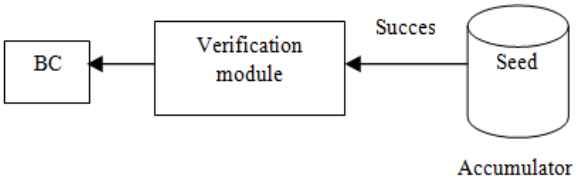

Fig. 6: Linker interface the user with another Biometric Cryptosystem

Design concepts:

Step 1: User authentications the linker through the biometric verifications: In this step, the user is requested to use any one of Biometric Cryptosystem (BC). The Biometric template (Jain *et al*., 2008) is captured and the shielding functions are applied. After authentication, the system sends a request to the Linker module. Figure 3 shows the process of user authentication through the linker.

Step 2: One time seed generation: Linker module uses the concept of HMAC algorithm. Once the Linker module gets authentication of the Biometric cryptosystem, it generates the OTS. The OTS is stored in the accumulator and a copy of the OTS is sent to the user through reliable network. Figure 4 shows how the OTS is generated.

Step 3: Linker side verification: The linker receives the password from the user. It performs a cryptographic function on the user's seed value with the accumulator seed value. If the two values match it considers the user as a valid one. Figure 5 shows the illustration linker side verification.

Step 4: Linker interface of the user with another biometric cryptosystem: Finally the verification module opens the gate to another Biometric

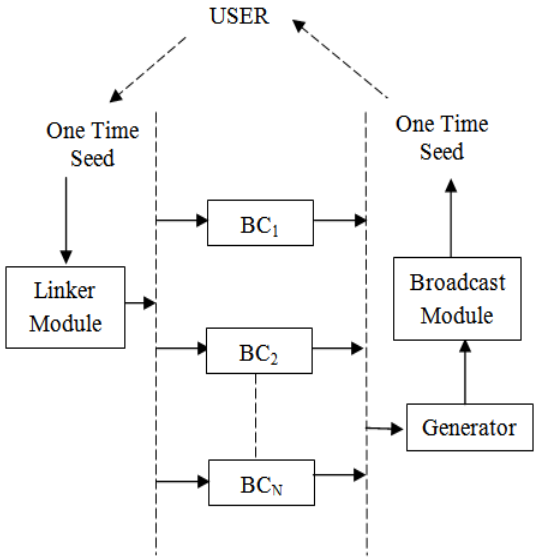

Fig. 7: Architecture of MSBC

Table 1: False acceptance rates and false reject rates for different threshold values for iris

Threshold value	False Acceptance Rate (%)	False reject rate (%)
3	0.01	44.20
4	0.007	49.50
5	0.003	57.60
6	0.001	62.80

cryptosystem (Schimke *et al*., 2005) if the previous operations yields a success or close the gate it the previous operations yields a failure. Figure 6 shows the illustration of linker interface of the user with another biometric cryptosystem. The overall schematic diagram of MSBC is shown in the Fig. 7.

RESULTS AND DISCUSSION

Databases: To evaluate the matching performance and authentication on our MSBC we use two database images, each for one biometric cryptosystem. To evaluate first biometric cryptosystem BC_1 we use MSU fingerprint database and to evaluate second biometric cryptosystem BC_2 we use CASIA iris database version 4. In our experiments, we tested our BC_1 system on the MSU fingerprint database, which consists of ten images (640*480) for each finger collected from 50 individuals and a sum of 500 fingerprint images.

We tested our BC_2 system with 5 iris images selected from 50 CASIA iris databases and total of 250 images.

Matching performance analysis: Matching performance analysis of the system is defined over the Matching performance of the two biometric cryptosystem. Here at the entry level matching threshold is kept at low. Since the BC_1 acts as the gate to the MSBC, the threshold of the second biometric system is decreased to 90% and as it is the real authentication system. So matching performance analysis of the system is given by the matching performance of the BC_2. In BC_2 a total of 2450 (50*48) matching's were done. The matching performance has highly changed when there is a decrease in threshold values. The Table 1 shows the corresponding false acceptance rate false reject rate for the decrease in threshold value.

Authentication analysis: The authentication of our system is based upon the authentication of the BC_2. Increased threshold value (Kuipeng and Peng, 2010) gives very good authentication system. For this purpose we selected three number Iris images of same iris from the CASIA database. Matching is performed between this iris and performance of the system is tested. Matching is done for different threshold values. The false acceptance rate and false reject rates with different threshold values are tabulated in the Table 1.

A graph is plotted against authentic acceptance rate (%) and the false acceptance rate (%) from the graph it is noticed that the system performs well in the small threshold values. The graphical representation of

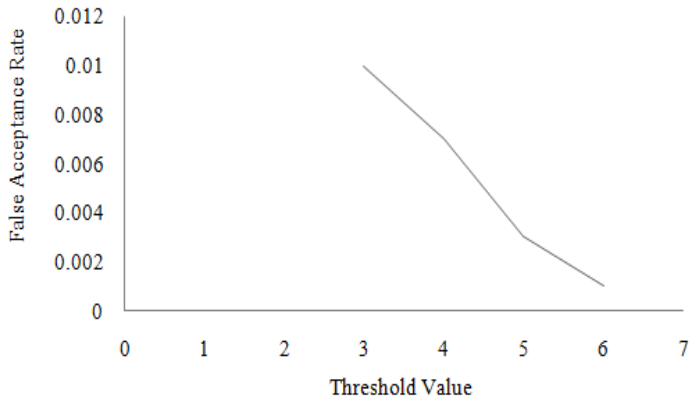

Fig. 8: Distribution of FAR vs Threshold values

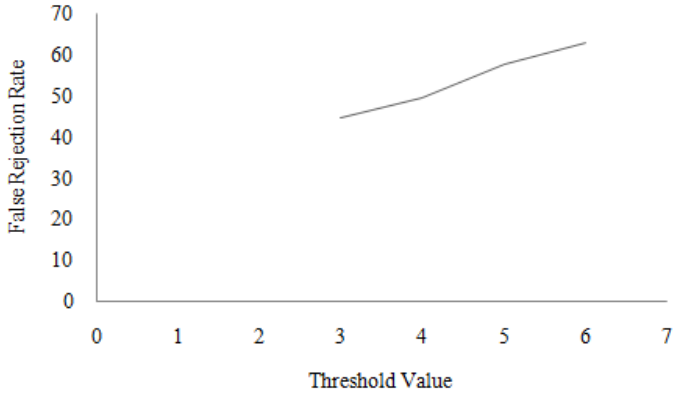

Fig. 9: Distribution of FRR vs Threshold values

threshold values versus false acceptance rate and false rejection rate is shown in Fig. 8 and 9, respectively.

CONCLUSION

We have introduced a multistage biometric cryptosystem. The cryptosystem discussed is much more secure due to the low threshold values used in the matching process. The system provides high security level due to multiple stages. In this study, multistage biometric cryptosystem is defined in which each individual unibiometric cryptosystem is linked to one another by one time seed through an external network. The accuracy of the system is analyzed using FAR/FRR and they are demonstrated using example. From the discussion, the multistage biometric cryptosystem performs much better than other biometric cryptosystem in low threshold values.

REFERENCES

Arasu, S.E., B. Gowri and S. Ananthi 2013. Privacy-preserving public auditing in cloud using HMAC algorithm. Int. J. Recent Technol. Eng., 2(1): 149-151.

Chen, B. and G.W. Wornell, 2001. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. IEEE T. Inform. Theor., 47(4): 1423-1443.

Feng, Y.C., P.C. Yuen and A.K. Jain, 2010. A hybrid approach for generating secure and discriminating face template. IEEE T. Inform. Forensics Secur. Biometrics Compendium, 5(1): 103-117.

Jain, A.K., K. Nandakumar and A. Nagar, 2008. Biometric template security. EURASIP J. Adv. Signal Process., Article ID 579416, pp: 17.

Kuipeng, C. and Z. Peng, 2010. Research of fuzzy algorithm of determining threshold value based on MTS. Proceeding of International Conference on Computational and Information Sciences (ICCIS), pp: 200-202.

Linnartz, J.P. and P. Tuyls, 2003. New shielding functions to enhance privacy and prevent misuse of biometric templates. In: Kittler, J. and M.S. Nixom (Eds.), AVBPA 2003, LNCS 2688, Springer-Verlag Berlin Heidberg, pp: 393-402.

Mineta, Y. and *et al*., 2008. The keyed-Hash Message Authentication Code (HMAC). Federal Information Processing Standard Publication, pp: 6-8.

Nagar, A., K. Nandakumar and A.K. Jain, 2011. Multibiometric cryptosystems based on feature level fusion. IEEE t. Inform. Biomet. Compendium, 7: 1-14.

Rathgeb**,** C. and A. Uhl, 2011. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP J. Inform. Secur.,* 3: 1-25.

Schimke, S., A. Valsamakis, C. Vielhauer and Y. Stylianou, 2005. Biometrics: Different approaches for using gaussian mixture models in handwriting. In: Dittmann, J., S. Katzenbeisser and A. Uhl (Eds.), CMS 2005, LNCS 3677, IFIP International Federation for Information Proceeding 2005.

Uludag, U., S. Pankanti, S. Prabhakar and A.K. Jain, 2004.Biometric cryptosystems: Issues and challenges. Proceedings of the IEEE, 92(6): 948-960.