Crytosystem for Computer security using Iris patterns and Hetro correlators

R. Bremananth
Information Systems and Technology Department,
Sur University College,
Sur, Oman.

Ahmad Sharieh
Information Systems & Technology Department,
Sur University College,
Sur, Oman.

***Abstract*—Biometric based cryptography system provides an efficient and secure data transmission as compare to the traditional encryption system. However, it is a computationally challenge task to solve the issues to incorporate biometric and cryptography. In connection with our previous works, this paper reveals a robust cryptosystem using iris biometric pattern as a crypto-key to resolve the issues in the encryption. An error correction engine based on hetro-correlators has been used to evoke the partially tarnished data fashioned by the decryption process. This process determines the non-repudiation and key management problems. The experimental results show that the suggestion algorithm can implement in the real-life cryptosystem.**

Keywords-Auto-correlators; Biometric; crytosystem; Hetro-correlators.

I. INTRODUCTION

Cryptography provides a secure proliferation of information exchange across the insecure data communication [1]. It authenticates messages based on the mathematical key but not based on the real-life user those who are the genuine owner. Traditional cryptosystem requires a lengthy key to encrypt and decrypt in sending and receiving the messages, respectively. But these keys can be guessed or cracked. Moreover, maintaining and sharing lengthy, random keys in enciphering and deciphering process is the critical problem in the cryptography system. A new approach is described for generating a crypto key, which is acquired from iris patterns. In the biometric field, template created by the biometric algorithm can only be authenticated with the same person. Among the biometric templates, iris features can efficiently be distinguished with individuals and produces less false positives in a large population. This type of iris code distribution provides merely less intra-class variability that aids the cryptosystem to confidently decrypt messages with an exact matching of iris pattern. In traditional cryptography system, key management is a cumbersome process that is, key must be generated each time with an extensive computational process and the dissemination of keys is also a very difficult process at the non-secure channels [1]. It consumes lot of system time and produces overburden to the application domains. In addition, non-repudiation cannot easily be handled in the traditional cryptosystem.

The Biometric key cryptography (BKC) is an emerging reliable alterative that can be used to resolve key management, large key computational process and address the non-repudiation problems [2]. In the cryptography system, data will be secured using a symmetric cipher system and in public-key system digital signatures are used for secure key exchange between users. However, in both systems the dimension of security accuracy is dependent on the cryptography strong keys. They are required to remember and enter the large key whenever needed. Instead of remembering large keys, the user may opt to give password to encrypt and decrypt the cryptography keys. There is no direct tie up between user and password that is, the system running the cryptography algorithm is unable to differentiate the genuine user and impostors who are unauthorized to work with the system.

Thus, a reliable alternative to the password security is the biometric guard for the cryptography keys. Whenever user wishes to access through a secured key, biometric sample is captured, authenticated by the classifiers and then key is released to encipher / decipher the desired data. In general biometric cryptosystem has been classified by three categories. The first method is to release the cryptography key from secure area in accordance with biometric matching algorithm. It requires the secured communication line to avoid eavesdropper's attacks. Furthermore, if the user may store the biometric templates or crypto keys in workstation machines then the system becomes an insecure one. In the next method, the crypto key is embedded as a part of biometric template in a specific location. However, if impostors may determine the location of the keys, again it becomes catastrophic to the system. The third method is based on using biometric features as cryptography keys, which gives more secure manner of proliferation of information exchange.

The proposed approach is broadly classified into three phases. The first phase is related with compact way to obtain iris feature codes from the human irises. The second one describes the algorithm to encrypt and decrypt the messages using iris bits. In the third phase, the error correction engine is employed to recall the partially corrupted bits generated in the decryption using associative memories. The issue of biometric pattern is the partially varied features produced in the feature extraction process, which subsequently makes partially corrupted data in the decryption process. This dissimilarity may occur due to environments, illuminations, distance variation and other artifacts. However more stable pattern produced by the iris is secured in the person's lifetime and produces limited

number of bits variations in the features, which assists to decrypt the messages in massive manner. In addition, re-enrolment of iris keys is required to preserve the system security more consistently.

In the current literature several studies were proposed related with biometric cryptosystem but most of them dealt with fingerprints and few of them were concerned with iris features. Albert Bodo proposed a method of directly using biometric as cryptography key in the patent of German [1]. In (Davida et al. [2][3]), 2048-bit iris code was used for enciphering and deciphering process. Key generation is invoked based on the error bits of the iris codes. This system stored the error correction bits along with iris keys inside the database. Thus, impostors may eavesdrop key information and a count of error correction bits from the local database. In (Linnartz et al. [4], Clancy et al. [5], Monrose et al. [6]), the key generation was based on biometrics such as fingerprints [18] and voices, but they required more calculations to release the key than the traditional cryptography system. The problem of generating cryptograph key from face biometric features had been studied by Yao-Jen Chang et al. [7]. The survey of multi-biometric cryptosystems was discussed by Uludag et al. [8]. A method of iris compression for cryptography documentation on off-line verification was proposed by Daniel et al. [9]. In this study, a modified Fourier-Mellin transformation was employed to create iris template for representing EyeCert system, which consists of two components. The first one is details of personal data related with the subjects, and the second one is the iris feature encoded in the form of barcodes. In another study of iris biometric cryptosystem, Feng Hao et al. [10] proposed a method based on error-free iris key that was devised using a two-layer error correction technique incorporated with Hadamard and Reed-Solomon codes. The extracted code was saved in a tamper-resistant token such as a smart card. In our previous work, (Bremananth et al. [11]) proposed auto-correlator to recoup the corrupted bio-metric crypto key. In this paper, a robust hetro-correlator has been proposed to regain the data.

The block diagram of the proposed iris cryptosystem is illustrated in Fig. 1. It suggests a compact way to extract feature from the iris patterns and these features are treated as crypto key for the on-line cryptography system. This system outperforms other traditional approaches and provides an efficient solution for non-repudiation approach as well. It employs 135-bit iris code which is extracted by wavelet analysis[12][13][14] and applying these codes in enciphering and deciphering of the input stream of binary data which might be originating from voice, text, video, image or other sources. Next, the auto-correlators and hetero-correlators are used to recall original bits from the partially corrupted data produced in the decryption process. It intends to resolve the repudiation and key management problems. However, the performance of error correction model dependents on the correlators used in the system. Hence the guarantee issues of these methods were verified and the experimental results were analyzed in both symmetric iris cryptosystem (SIC) and non-repudiation iris cryptosystem (NRIC). It shows that this new approach provides considerably high authentication in enciphering and deciphering processes. The remainder of the paper has been organized as follows. Section II describes the symmetric iris cryptosystem. Non-repudiation cryptosystem is described in Section III. Error correction engines and their functionalities are given in Section IV. Section V describes the experimental results of the bio-metric cryptosystem and concluding remarks are given in Section VI.

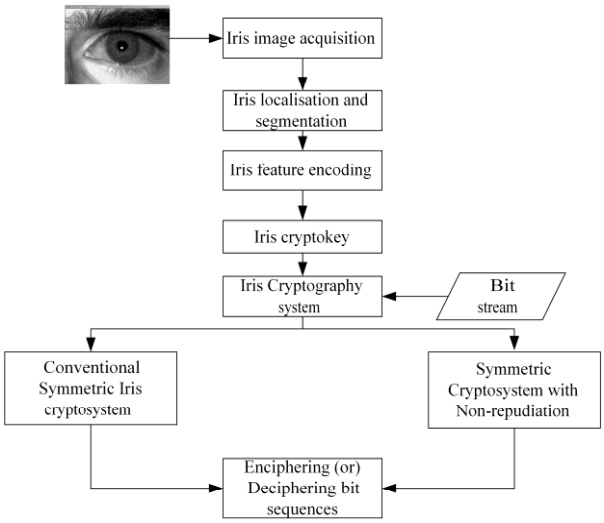

Figure 1. A proposed block diagram of the iris cryptography system.

II. SYMMETRIC IRIS CRYPTOSYSTEM

Iris patterns are used for fabricating a key to encipher and decipher the plain text in between sender and receiver over insecure channels [2][11]. The advantages of iris cryptosystem are to reduce the system processing time to make a complex key for standard cryptography algorithm and to generate cipher keys without getting back from complex key generation sequences. The identical iris code is used in both ends to encrypt and decrypt the message in the SIC system. In order to decrypt a message, the recipient needs an identical copy of the iris code. Figure 2 shows the iris based symmetric cryptography system. The transmission of enrolled iris code over the channel is vulnerable to eavesdropping. Hence, the copy of the enrolled iris code is needed in the recipient side, which is being used by the decryption process. In this approach, XOR operation is used to encrypt and decrypt the message. The significant steps of SIC encryption algorithm is described as follows:

Step 1: Let K be the key sequence $I_1, I_2, ..., I_p$ produced by iris feature encoding algorithm for the encryption transformation. In the experiment 136-bit key sequence (135-bit iris code and one padding bit) is used in the encryption process.

Step 2: Let S be a source alphabet of N symbols $S_1, S_2, ..., S_N$. Each alphabet in S is converted to its equivalent 8-bit binary strings. The bits of messages undergo XORing with iris key sequence and generate a non-breakable cipher-bit described as

$$C_i = Ency(S_1, S_2, ..., S_N \oplus I_1, I_2, ..., I_p) \qquad (1)$$

where C_i is set of cipher bits. The decryption algorithm is described as follows:

Step 1: The testing iris pattern is extracted and iris codes are formed. The iris-matching algorithm verifies the test and the enrol iris codes. If weighted distance (WD) is $0 \le \mathrm{WD} \le 0.19$, then the matched enrolled iris code is used for deciphering the messages, otherwise rejected.

Step 2: Let $I_1, I_2, ..., I_p \in K$ be an enrolled iris code and $C_1, C_2, ..., C_n$ is a set of cipher text produced by the encryption process. Enrolled iris codes are XORed with set of cipher bits and generate the original messages using Equation (2).

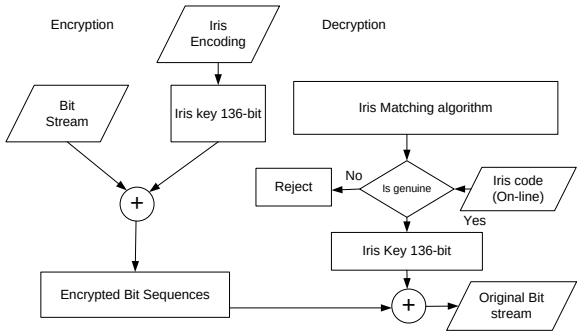

Figure 2. The process of SIC system.

$$S_i = Decy(C_1, C_2, ..., C_n \oplus I_1, I_2, ..., I_p) \quad (2)$$

where S_i is set of source alphabet bits and I = 1,2, 3, … N. In the SIC system, key dissemination problem is completely avoided. However, the system needs iris database and iris-matching algorithm in the decryption process to get back the original messages. In order to resolve repudiation problem, the iris database and iris-matching algorithm are eliminated from the SIC system. The detailed description of this process is discussed in the next section.

III. Non-Repudiation Iris Cryptosystem

Unlike SIC system, the NRIC system bypasses the iris-matching process and do not access iris database in the decryption process. The testing iris code can directly be XORed with cipher bits transmitted by the encryption process as illustrated in Fig. 3. Iris codes are changed from session to session with minimum variation (WD<=0.19) for the same subject eye. Hence the decryption process may produce the probability of partially corrupted cipher bits ranging from 0 to 0.19. Perhaps, if intruder may tap the cipher bits at the non-secure channels then the probability of decrypting the message is complicated from 0.2 to 1 partially corrupted bit in every 135-bit iris code. Thus, it produces more complexity to the intruder to get back the original messages. But the cipher bits accessed by the genuine subjects have probability of error rate at most 0.19, so that, less complexity have been created in the decryption process.

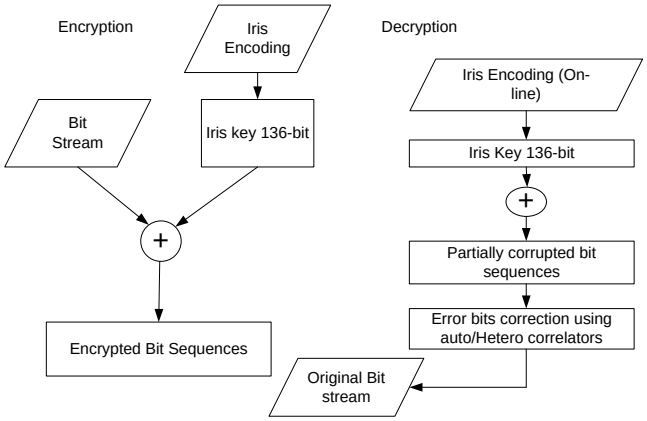

Figure 3. A sequence sketch of Non-repudiation cryptosystem.

In this method cipher bits are directly XORed with the test iris key and produce the partially corrupted bits. These are very close to the original message if the test iris key is actually extracted from the genuine subject; otherwise the partially corrupted bits are larger than the threshold maintained in the system.

Thus impostors can be restricted to access the original scripts. The error bit correction module subsequently corrects these bits by using the two different correction engines such as either auto-correlators or hetero-correlators that perform the probability of error correction based on iris-weighted distance. Thus this process overcomes repudiation problem and reduces the key management issues. However, the performance of the NRIC fully depends on the guarantee of the error correction engines because recalling the original bits is a difficult process in the real time processing of encryption and decryption.

IV. Error Correction Engines

In the process of biometric cryptosystem, the major limitation is a way to get back the original bits from the partially corrupted bits generated by the decryption. In the literature, several studies had been performed to recall the trained patterns from the partially corrupted patterns. Bart Kosko et al. [15] enhanced the bidirectional associative memories (BAM), which behaves as a hetero-associative content addressable memory (CAM) storing and recalling the vector pairs.

The bidirectional associative memory with multiple training can be guaranteed to recall a single trained pair under suitable initial conditions of data. Sufficient condition for a correlation matrix to make the energies of the training pairs was described by Yeou-Fang et al. [16]. An essential condition for generalization of correlation matrix of BAM which guarantees the recall of all the training pairs was discussed by Yeou-Fang et al. [17]. This paper adopts two different methods to recall the corrupted patterns. The first one is related to auto-associative and the other one is concerned with hetero-associative.

A. Autocorrelators

Associative memories are one of the key models of neural network and they can act as a human brain to recall the associated patterns perfectly from the corrupted patterns. If the associated pair (x, y) is the identical pattern, then the model of associative memory is called as auto-associative memory. For the recall operation, auto-associatives require the correlation memory or connection matrix, which aids to retrieve original patterns from the partially corrupted pattern. It is called as auto-correlators and is adopted in the error correction process of NRIC. The algorithm of error bits correction process is described as follows [11]:

Step 1: The partially corrupted data obtained in the decryption process is taken for further processing. This data is transformed to bipolar patterns (ϕ_c). Let M be the number of stored bipolar patterns $p_1, p_2, \ldots, p_m$ and i[th] patterns is $(p_{i1}, p_{i2}, \Lambda, p_{in})$ where n is the number of bits in the stored pattern. The connection matrix CM is derived as

$$CM_{ij} = \sum_{i=1}^{n} \left[p_i^T \right] \left[p_i \right] \text{ for } i = 1..n, \text{ for } j = 1..n \quad (3)$$

Step 2: The auto-correlator recalls the original patterns (θ) using

$$\theta_j = g((\phi_{cj} * CM), p_j) \quad for\ j = 1..m \quad (4)$$

$$g(\chi, \varphi) = \begin{cases} 1 \ if \ \ \chi > 0 \\ \varphi \ if \ \ \chi = 0 \\ -1 \ if \ \ \chi < 0 \end{cases} \quad (5)$$

where θ_j is the recalled original pattern, ϕ_c is a partially corrupted data and $g(\chi, \varphi)$ is the threshold function.

Step 3: Repeat Step 2 until $\sum_{i=1}^{n} |\phi_i - \theta_i| > \rho$, where ρ is a vigilance parameter.

The parameter ρ provides minimum error bit correction in between the genuine subject iris code and partially corrupted cipher bits. This parameter gives more complexity to the intruder to get back the original messages. For example, if the patterns are $p_1 = [1 \quad 1 \quad -1]$, $p_2 = [-1 \quad -1 \quad 1]$, $p_3 = [1 \quad -1 \quad 1]$ then the connection matrix (CM) is: $\begin{bmatrix} 3 & 1 & -1 \\ 1 & 3 & -3 \\ -1 & -3 & 3 \end{bmatrix}$

If partially corrupted data produced in the decryption process is $p = [-1 \quad 1 \quad 1]$ then the computation with CM produce the threshold conditions: g(-3,-1),g(-1,1) and g(1,1). It gives the original pattern $O = [-1 \quad -1 \quad 1]$.

B. Heterocorrelators

In this approach, noisy variation of different types of iris codes are not explicitly estimated and stored in the verification database [17]. If they may explicitly be estimated, then it leads to leak of security information to the adversary. Hence, hetero-correlations are directly used to recall the original patterns from the corrupted patterns that need not have any additional information such as noisy variations. This is nothing but an associative memory, which is an imitation model of human brain's ability to recall associate patterns. In the non-repudiation cryptosystem, the decryption produces noise bits which should be corrected properly and converted to its real bit sequences. If the associated pattern pairs (x, y) are different, then this model recalls y. If x is given, then y can be called. This is referred as hetero-associative memory. This memory is used to recall the original patterns from the corrupted patterns. For the recall operation, hetero-associative requires a correlation memory or connection matrix, which aids to retrieve original patterns. This is so-called hetero-correlators. The algorithm of error bits correction process is described as follows:

Step 1: The partially corrupted data obtained in the decryption process is taken for further processing. This data is transformed into its bipolar patterns (δ). Let M be the number of stored bipolar pairs given as

$$\left\langle \{P_1, Q_1\}, \{P_2, Q_2\}, ..., \{P_m, Q_m\} \right\rangle \quad (6)$$

where $P_i = \{p_{i1}, p_{i2}, \ldots p_{in}\}, Q_i = \{q_{i1}, q_{i2}, .. q_{io}\}$, P and Q represent stored and exemplar patterns of distorted bipolar data, respectively. The connection matrix (CM) is derived as

$$CM_{ij} = \sum_{i=1}^{n} E_i \left[P_i^T \right] \left[Q_i \right] \text{ for } i = 1...n, \text{ for } j = 1..o \quad (7)$$

where CM is a correction matrix used in the hetero-correlation process and E is a set of energy constants i.e., $E \in R^+$, R is a set of real numbers. Calculate κ' and κ from Equations (8) and (9) and assign to δ' and δ, respectively.

Step 2: The hetero-correlator recalls the original bit sequences (φ) using

$$\kappa' = \Theta(\delta \bullet CM) \tag{8}$$

$$\kappa = \Theta(\kappa' \bullet CM^T) \tag{9}$$

$$\Theta(\lambda) = \varphi = \varphi_1, \varphi_2, \ldots, \varphi_n \tag{10}$$

$$\lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_n\} \tag{11}$$

$$\varphi_i = \begin{cases} 1 \ if \ \ \lambda_i > 0 \\ \varphi_i \ if \ \ \lambda_i = 0 \\ -1 \ if \ \ \lambda_i < 0 \end{cases} \tag{12}$$

where δ is a set of partially corrupted bipolar bits generated by the decryption process, Θ is a threshold function of hetero-correlation, λ represents multiplication result of the correction matrix for the given distortion bit patterns, φ is set of the recalled bits, κ' represents result of exemplars and κ is a sequence of corrected bits.

Step 3: After performing error correction process, find out the weighted distance between corrupted and corrected exemplar as

$$\Phi = \left[\sum_{i=1}^{n} \left| \delta_i' - \kappa_i' \right| \right] \tag{13}$$

If $\Phi = 0$ then distance becomes zero and engine decides that the equilibrium point is reached, i.e., corrupted bits in decryption process are safely recalled by hetero-correlators.

If $\Phi \le \rho$, then assign corrected bits to $\delta, i.e., (\delta = \kappa), (\delta' = \kappa')$ and perform step 2 until distance of exemplar becomes zero.

If $\Phi > \rho$, then the engine confirms that adversary does the correction process, therefore system has been terminated.

The ρ is a vigilance parameter and it is calculated as $\rho = (n - \text{mod}(n,2))$ i.e., $0 \le \rho \le (n - \text{mod}(n,2))$ and n represents number of bits in an exemplar. The parameter ρ provides minimum energy for the bits correction between genuine subject and partially corrupted cipher bits and also it prevents local minima of the system. This parameter also gives more complexity to the impostor to get back the original messages.

Finally, recalled bipolar bits are converted to its equivalent binary bits. These sequences of corrected bits represent the original bits. The number of error bit recovery is based on ρ and E parameters. If 7-bit exemplar is used, then the parameters $\rho = 6$ and $E = \{2,3,2\}$ provide a better result in the error correction process.

V. Experimental Results

The proposed approach has been implemented and results were analysed. Efficacies of SIC and NRIC have been evaluated. The NRIC system's time complexity was measured, in that there were no recalling processes involved since the encrypted bits were decrypted by the enrolled iris key. Hence its enciphering and deciphering process depends on the time complexity of iris-matching algorithm.

Next, the performance of the NRIC system was measured by computing the time complexity of auto and hetero-correlators' recalling and encryption/decryption processes. In the next experiment iris key energy complexities was calculated in the case of cracking the messages by the impostors. Finally, the guarantee issues of getting back original bits were evaluated with respect to the energy variation of auto and hetero-correlators. The detailed description of each experiment is discussed in the following sections.

A. Speed performance

Time complexities of encryption and decryption process have been evaluated for the SIC system. In that decryption process required more time than encryption process, since the decryption was performed after extracting and matching the iris features at one time. The complexity of iris matching algorithm was dependent on the size of the iris keys present in the system.

The complexity of searching iris keys iris key matching system with linear search is O(N) and with binary search is O(log N). The NRIC system required slightly more time than the SIC approach because of its error correction engines require more time to predict the original patterns from the partially corrupted patterns. The search time of encryption and decryption processes of SIC and NRIC are illustrated in Fig. 4.

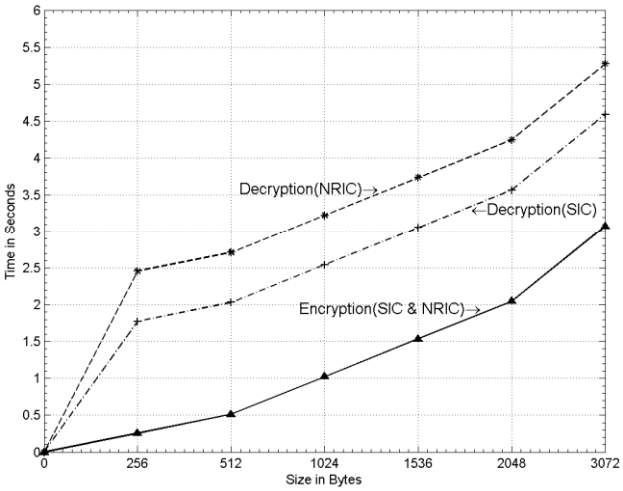

Figure 4. Encryption and decryption time complexity of SIC and NRIC.

B. Recalling time

The recalling time of auto and hetero correlations were dependent on size of the connection matrix in the error correction process. The connection matrix was formed based on the number of bits processed by the cipher text. In accordance with the number of patterns and bits per exemplar, the recalling time of auto and hetero correlators were evaluated and shown in Fig. 5.

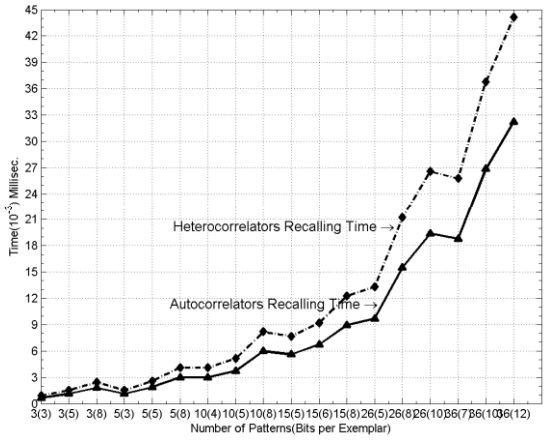

Figure 5. Auto and hetero correlators' recalling time.

C. Performance issues

The guarantee issue of recalling process for correlators was associated with two factors such as connection matrix of the error correction engine and artifacts occurring on the iris patterns. It provides nearly 97% of recalling entire pair of trained patterns because of its local minimum of the energy surface. However, in this paper, vigilance parameter was used to put off local minimum attained by the system, i.e., energy for the bits correction in between genuine subject and partially corrupted cipher bits were computed to prevent the local minima of the system. This parameter also produced more complexity to the impostor to get back the original messages. The factors of artifacts are fully concerned with three possessions such as acquisition time users' co-operation, non-iris fractions occurring on iris and artifacts emerging in the core area of iris. The guarantee issues of error correction process for auto and hetero correlators are based on number of patterns and bits per patterns used in the error correction process.

The guarantee performance of recalling process was evaluated based on the Hamming distance between the corrected bits and trained pairs. Multiple training was used to recall several patterns. In this training, if pattern was not recalled by the connection matrix by satisfying vigilance parameter then train the patterns again by changing energy constants, form a new connection matrix and performing recalling process. This process was repeated until recalling entire patterns by checking vigilance parameter. However, trained patterns require sufficient number of bits to increase the percentage of accuracy. Figure 6 shows the accuracy of recalling patterns using auto and hetero correlators.

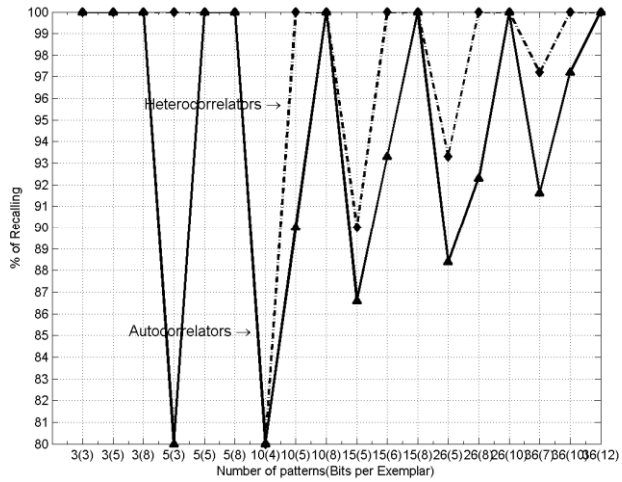

Figure 6 Accuracy of recalling patterns using auto and hetero correlators.

D. Impostor complexity

The probability of the presence of errors in the non-repudiation process was assessed based on the number of bits variation. These variations occur due to the environment, illumination, occlusion of eyelids/eyelashes and other artifacts. In this experiment, the number of bits corrupted in different sessions was studied and verified in which situations brute force search by an intruder can crack the iris crypto key. For the experiment, different eye images were captured at different sessions from the same subjects and their changes measured. Figure 7 illustrates the error bit variation in different criterion. The changes in bits may not be stable for all kind of capturing because due to diverse changes the random alteration of bits was assorted. The efficiency of the iris cryptosystem was evaluated in accordance with key stability and strength. The strength of the key can be evaluated based on entropy principles. If message source alphabet was $A = \{a1, a2\}$ and the symbol probability P (a_1) = 0.088 and P (a_2) = 0.103 then the entropy of the source symbol was 0.6495 bits/symbol. If an intruder can tap the message, the probability of retrieving the original message was ranged from 0.2 to 1 based on the error

bits of iris code. That is, if n bits were error then 2^{n-26} times of complication for brute force search was made to an intruder. Thus the retrieving of the original messages has been made complicated to the impostors. It provided a high key strength for any cryptography system. This key cannot be stolen or missed and gave more stability to the cryptosystem. These types of bio keys can be produced every time the users want to communicate secretly at non-secure channels. In addition, experimental results show that this approach could easily be adopted in the on-line cryptography systems as well.

E. Re-enrolments

Another design issue of integrating biometrics with cryptography is the re-enrolments because biometric cryptosystem is a reliable alternative for password protection while releasing or direct usage of biometric key as a cryptography key.

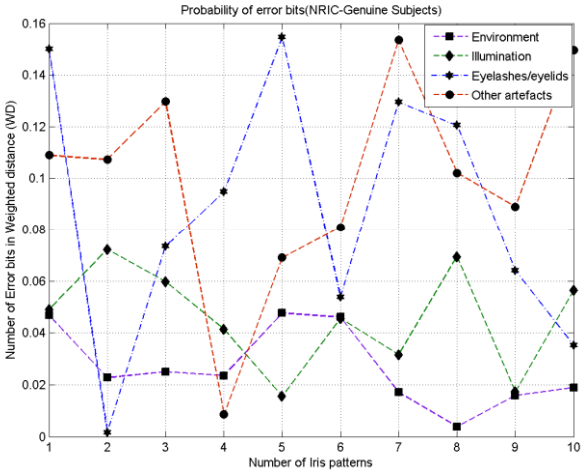

Figure 7. Error bit variation for the same subject in different criterion.

Hence encryption algorithm needs efficient solutions, which are periodically updated biometric templates. Thus user can register their patterns once in a month or other period of time maintained in the system. Since some of the system exploits biometric key for safeguarding mathematical cryptographic keys or others may utilize as a part of the biometric template. Nevertheless if biometric databases are permanently stored in the local workstation for a period of time, which is not secure, a system should employ the recently enrolled iris keys for encryption process that increases the system security and avoids eavesdropper attacks than the lifelong biometric templates.

Thus the iris-based cryptosystem performs better accuracy by using re-enrolments. In this paper, subjects' iris patterns were periodically enrolled once in a week in order to measure the stability of the iris keys. However the keys variation weighted distance was ranging from 0.0 to 0.19. This range was fixed by statistical measures of iris recognition algorithm. Thus these random variations were due to artifacts or other non-iris sources. However the periodic amendment of genuine subjects' iris key produced more brute force search to the impostors than the ordinary system.

VI. CONCLUSION

This research paper suggests a novel approach for iris based cryptography system. The crypto keys have been generated using iris patterns, which is stable throughout a person's lifetime as well. Its inter-class variability for a person is very large since it creates more complexity to crack or guess the crypto keys. This approach has reduced a complicated sequence required to generate keys as in the traditional cryptography system. It can also generate more complex iris keys with minimum amount of time complexity, which is aptly suited for any real time cryptography system. This resolves the key repudiation problem occurring in the traditional system. The hetero-correlators can predict the number of bits corrupted in the decryption process with the help of vigilance parameter. The performance of the proposed approach is found to be satisfactory.

In near-future, multi-modal cryptosystem will be suggested to integrate biometric template to increase degree-of-security in the non-secure data transmission.

REFERENCES

[1] Albert Bodo, 'Method For Producing a Digital Signature with Aid of a Biometric Features', German patent DE 42 43 908 A1, 1994.

[2] Davida G.I., Frankel Y. and Matt B.J., 'On enabling secure applications through off-line biometric identification', Proc. of IEEE Symposium Privacy and Security, Oakland, California, USA, pp. 148-157, 1998.

[3] Davida G.I., Frankel Y., Matt B.J. and Peralta R., 'On the relation of error correction and cryptography to an offline biometric based identification scheme', Proc. Workshop Coding and Cryptography (WCC'99), PARIS (France), pp. 129-138, 1999.

[4] Linnartz M.G. and Tuyls P., 'New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates', AVBPA 2003, Guildford, UK, pp. 393-402, 2003.

[5] Clancy T., Kiyavash N. and Lin D.J., 'Secure Smartcard-Based Fingerprint Authentication', Proc. of ACM SIGMM workshop on Multimedia, Biometric Methods and Applications, New York, USA, pp. 45-52, 2003.

[6] Monrose F., Reiter M., Li Q. and Wetzel S., 'Cryptographic key generation from voice', Proceedings IEEE Symposium on Security and Privacy, Oakland, California, pp. 201-213, 2001.

[7] Yao-Jen Chang, Wende Zhang and Tsuhan Chen, 'Biometrics-Based Cryptographic Key Generation', IEEE International Conference on Multimedia and Expo, Taipei, Taiwan, (0-7803-8603-5/04), pp. 2203-2206, 2004.

[8] Uludag U., Sharath Pankanti, Salil Prabhakar, Anil K. Jain, 'Biometric Cryptosystems: Issues and Challenges', Proceedings of the IEEE, Vol. 92, No. 6, pp. 948-960, 2004.

[9] Daneil Schonberg and Darko Kirovski, 'Iris compression for Cryptographically Secure Person Identification', Proceedings of IEEE Data Compression Conference (DCC'2004), Snowbird, UT, USA, pp. 459-468, 2004.

[10] Feng Hao, Ross Anderson and John Daugman, 'Combining cryptography with biometrics effectively', Technical report of University of Cambridge, No. 640, pp. 3-17, 2005.

[11] Bremananth R and Chitra A, 'An efficient biometric cryptosystem using autocorrelators' International Journal of Signal Processing 2;3, pp.158-164, 2006.

[12] R.Bremananth and A.Chitra, "A novel approach for high authentication based on Iris keys", World Scientific and Engineering Academic Society Transaction on Information science and applications, Issue 9, Vol. 2, pp.1420-1429, 2005.

[13] R.Bremananth, A.Chitra, "A new methodology for person identification system", Sadhana, Indian academy of Sciences, Vol.31, Part 3, pp.259-276, 2006.

[14] R.Bremananth, A.Chitra, "Rotation Invariant Recognition of Iris", Journal of Systems Science and Engineering, Vol.17, No.1, pp.69-78, 2008.

[15] Bart Kosko, 'Bidirectional Associative Memories', IEEE Transactions on systems, Man, and Cybernetics, Vol. 18, No. 1, pp. 49-60, 1988.

[16] Yeou-Fag Wang, Jose B. Cruz and James H. Mulligan, 'Two coding strategies for bidirectional associative memory', IEEE Transactions on Neural networks, Vol. 1, No. 1, pp. 81-92,1990.

[17] Yeou-Fag Wang, Jose B. Cruz and James H. Mulligan, 'Guaranteed recall of all training pair for bi-directional associative memory', IEEE Transactions on Neural Networks, Vol. 2, No. 6, pp. 559-567,1991.

[18] P.Arul, A.Shanmugam, Generate a Key for AES using Biometric for VOIP Network Security, Journal of Theoretical and appllied Information Technology, Vol.5, No. 2, pp. 107-112, 2009.
(http://www.jatit.org/volumes/research-papers/Vol5No2/2Vol5No2.pdf)

AUTHORS PROFILE

Bremananth R received the B.Sc and M.Sc. degrees in Computer Science from Madurai Kamaraj and Bharathidsan University in 1991 and 1993, respectively. He obtained M.Phil. degree in Computer Science and Engineering from GCT, Bharathiar University, in 2002. He received his Ph.D. degree in 2008 from Department of Computer Science and Engineering, PSG College of Technology, Anna University, Chennai, India. He has completed his Post-doctoral Research Fellowship (PDF) from the School of Electrical and Electronic Engineering, Information Engineering (Div.) at Nanyang Technological University, Singapore, in 2011. He has 18+ years of experience in teaching, research and software development. Currently, He is an Assistant Professor in the Information Technology department, Sur University College, Sur, Oman, affiliated to Bond University Australia. He received the M N Saha Memorial award for the best application oriented paper in 2006 by Institute of Electronics and Telecommunication Engineers (IETE). His fields of research are acoustic holography, pattern recognition, computer vision, image processing, biometrics, multimedia and soft computing. Dr. Bremananth is a member of Indian society of technical education (ISTE), advanced computing society (ACS), International Association of Computer Science and Information Technology (IACIT) and IETE. He can be reached at bremresearch@gmail.com.

Ahmad Sharieh had two bachelor degrees: one in Mathematics and one in Computer Sciences. He had master degree in Computer Science and High Diploma in Teaching in Higher Education. He had PhD in Computer and Information Sciences from Florida State University 1991. Sharieh worked as Assistant Professor in Fort Valley College / USA and The University of Jordan (UJ) / Jordan. He worked as Associate Professor with Amman Arab University for Graduate Studies (AAUGS) / Jordan and The University of Jordan. He worked as Dean of King Adbullah School for Information Techology/Jordan. Currently, he is a professor of Computer Sciences and Dean at Sur University College (SUC), Oman. He published articles in journals (27), in conferences (22), and authored and prepared books (14). He gained grant for eight research projects from UJ and Europe. He developed several software systems such as: Teaching Sign Language, e-learning Modeling and Simulation, and Online (Automated) Exams. He is on the editorial board of several journals and conferences and a referee of several others. His research areas are Distributing Systems, Expert Systems, E-Government, E-Learning, Parallel Processing, Pattern Recognition, Software Engineering, Wire/Wireless Communication, Modeling and Simulation.