International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:8, 2008

An Efficient Biometric Cryptosystem using Autocorrelators

R. Bremananth, and A. Chitra

***Abstract*—**Cryptography provides the secure manner of information transmission over the insecure channel. It authenticates messages based on the key but not on the user. It requires a lengthy key to encrypt and decrypt the 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 a person's iris pattern. 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 the larger 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 this proposed approach, the iris features are extracted using multi resolution wavelets. It produces 135-bit iris codes from each subject and is used for encrypting/decrypting the messages. The autocorrelators are used to recall original messages from the partially corrupted data produced by the decryption process. It intends to resolve the repudiation and key management problems. Results were analyzed in both conventional iris cryptography system (CIC) and non-repudiation iris cryptography system (NRIC). It shows that this new approach provides considerably high authentication in enciphering and deciphering processes.

***Keywords*—**Autocorrelators, biometrics cryptography, iris patterns, wavelets.

I. Introduction

CRYPTOGRAPHY system authenticates the messages with respect to a cipher key. If the key is matched a particular encrypted message can easily be decrypted. But there is no assurance to decrypt the message by its owner instead of virtual cipher keys. Hence, biometric crypto system assists the cryptography system to encrypt and decrypt the messages using bio-templates. These templates cannot be same for the different persons and secrecy / privacy is also improved by this system. In traditional cryptography system, key management is a cumbersome process that is, key must be generated each time with large computations and dissemination of keys are also very difficult process at the non-secure channels. It consumes lot of system time and produces overburden to the application domains. In addition to that non-repudiation cannot be easily handled in the traditional cryptosystem. The Biometric Key Cryptography (BKC) is an emerging reliable alterative that can solve key management problem, larger key computational process and address the non-repudiation problem. The proposed approach is broadly classified into two phases, the first phase is a compact way to obtain iris feature codes from the human irises that are executed in the cryptography system and next phase is described as the algorithm to encrypt and decrypt the messages using iris bits. The problem 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 be occurred due to environments, illuminations, distance variation and other artifacts. However the more stable pattern produce by the iris is secured in the person's lifetime and produce limited number of bits variations in the features, which helps to decrypt the messages in massive manner. The CIC is based on the iris-matching algorithm, which releases iris key to decrypt the messages with respect to matching criteria maintained in the system. The matching process is completely ignored in the NRIC system in which XOR operation is directly manipulated with the encipher text and is generated partially corrupted data. These data can be corrected using associative memory concept. In the current literature, the novel way to correct noisy patterns is related with associative memories, in that autocorrelators is facilitated to get back distorted patterns perfectly without any exemplars. Hence, the proposed approach adopts autocorrelators to recall the original messages from the noisy data produced in the decryption process. In this paper, multi resolution wavelets were used to acquire iris code, iris matching was performed with XOR operation and autocorrelators were used to recall corrupted bits. The results were analyzed based on 2500 iris images acquired from 500 persons and this system was tested with both CIC and NRIC symmetric key cryptography system.

The organization of this paper is as follows: Section 2 briefs a short review of the previous work. Section 3 describes the process of proposed iris recognition system. Section 4 depicts the proposed iris cryptography system and its issues. Section 5 illustrates the experimental results based on real time iris patterns. Concluding remarks are given in section 6.

Manuscript received May 16, 2005.

R. Bremananth is a research scholar with the Department of CSE, PSG College of Technology, Coimbatore-641004. He is working as a Senior Lecturer, Sri Ramakrishna Engineering College, Coimbatore-641022, India (phone: 91-422-2461588, 2460088, 2606147, e-mail: bremresearch@gmail.com).

Dr. A. Chitra is a professor with the Department of CSE, PSG College of Technology, Coimbatore-641004, India (achitra@cse.psgtech.ac.in).

II. Literature Appraisal

In [1][2], 2048-bit iris code was used for enciphering and deciphering process. Key generation was based on the error bits of the iris codes. This system used the pattern of error correction bits stored in the database thus impostors can eavesdrop key information from it. In [3][4][5], the key generation was based on biometrics (fingerprints and voice) but they required more calculations to release the key than the traditional cryptography system. The survey of multi-biometric cryptosystems was discussed in [6]. In the current literature relatively less work has been done on iris based biometric cryptosystem. The proposed approach suggests a compact way to extract feature from the iris patterns and can fairly be used in the on-line cryptography system and it provides an efficient solution for non-repudiation approach as well.

III. The Proposed Methodology

The proposed approach is broadly classified into two phases, in the first phase iris features are extracted from the acquired iris patterns and iris matching is performed to recognize the iris patterns. The second phase is fully concerned with the cryptography related issues, symmetric cryptosystem and recalling process of NRIC system using autocorrelators. The block diagram of the proposed approach is illustrated in Fig. 1.

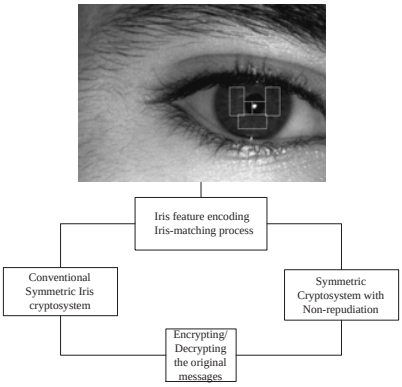


Fig. 1 Block diagram of the proposed iris cryptography

A. Iris Location Finding

Iris location finding process is based on tracing flash circle occur in the pupil area by the Canny operators. After applying this operator, noises of spectacles, lighting spot and other artifacts were appeared in the resultant image. From that image filtering and finding a flash point is a difficult process in real time implementation. Thus we use the weight-based circular method to locate a partially sheared circle appeared in the image. The purpose of incorporating weight scheme in the circular method is to distinguish camera flash location from other artifacts. Moreover, initial computation of finding the radius of the flash circle is a difficult process. Hence we use weight-based scheme to find the circular area properly. But some of the camera may produce two flash spots that could be emerged on the pupil area of the eye image. From those images either one of the spot can be used for localizing the iris portion. Fig. 2 shows the visualization of a camera flash detection process.

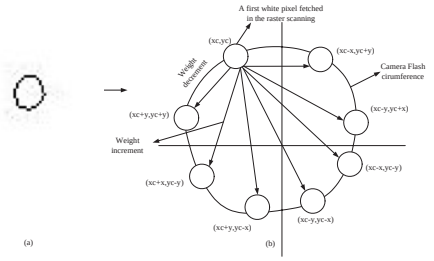


Fig. 2 Visualization of flash detection process using weight based scheme (a) flash spot of iris image (b) computational process of flash circumference

The weight-based localization is done in a manner such that the degree by which the weight increases or decreases is directly proportional to the distance in between the current flash pixel (xc,yc) and the next pixel. Similarly the decrease in weight is directly proportional to the step size of each weight increment. The weight computation is derived as, it can be stated that weight decrement is directly proportional to $(i - p)$. Therefore,

$$W_d = C_1(i - p) \quad (1)$$

Weight decrement is directly proportional to γ. Therefore,

$$W_d = C_2\gamma \quad (2)$$

From (1) and (2) we can drive,

$$W_d^{\,2} = C_1C_2(i - p)\gamma \quad (3)$$

Therefore,

$$W_d = \sqrt{C_1C_2(i - p)\gamma} \quad (4)$$

where C_1 and C_2 are decay constants and they should satisfy the conditions $0 < C_1 < 1$, $0 < C_2 < 1$, respectively. By using the (4) weight values are decremented until again white pixel is found, if circumference is very larger then weight value is incremented by the default γ. Hence γ is called as weight increment factor of the circular. The segmentation process of iris is discussed in the following section with feature encoding process.

B. Iris Feature Encoding

Iris feature encoding is a process to convert iris pattern into a set of suitable mathematical codes. The human iris is a well-distributed pattern unique in nature but these biological patterns may be contaminated due to environment change, capturing distance, external noise, occlusion of eyelids/eyelashes and other artifacts during acquisition process. For this reason, the same person's iris pattern may mathematically be changed from 0 to 0.19 probabilities in the

computational process. An efficient algorithm is required to extract iris features, in current literature some methods [7][8][9][10][11] are available but each has its own merits and demerits. Hence a new approach for iris feature extraction is carried out and is aptly suited for cryptography system. For that, iris patterns are locally processed by multi resolution analysis (MRA) using Daubechies wavelets. In the iris segmentation process, the selected portions of the iris are chosen for MRA that are having well distributed patterns. Most probably left, right and bottom segments of the iris are better distributed as well as these segments are less obscured by eyelids/eyelashes during eye image acquisition. Fig. 3 shows results of iris segmentation process. The left end point P_l (x, y) of the line segment is used to extract the left rectangle from the iris portion, like wise, points P_r (x, y) and P_b (x, y) are used to extract right and bottom rectangles from the iris respectively. Elastic deformation occurs in the iris portions due to lighting variations, for this reason, segment size variations are adapted in accordance with dilation and erosion of pupil boundary.

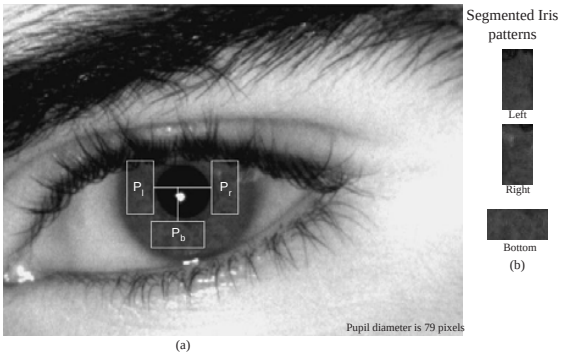


Fig. 3 (a) Visualization of iris Segmentation process
(b) Segmented iris patterns

Signal processing applications have been materialized using wavelet theory. It has been applied in many area of digital image processing such as detecting self-similarity, de-noising, compression, analysis, and recognition. This technique has proven the ability to provide high coding efficiency, spatial and quality features. Hence this system is employed with wavelet theory to extract iris feature efficiently. This is because wavelets can efficiently provide a signal representation in which some of the iris coefficients represent long data or short data, which holds narrow band or wide band, respectively. In this approach, the Daubechies wavelet is used to decompose the segmented iris portions into multiple resolution subbands. These subbands are employed to transform well-distributed complex iris patterns into a set of one-dimensional iris feature code. The decay is a process to divide the given iris portion into four subbands such as approximation, horizontal, vertical, and diagonal coefficients. Each coefficient represents a spatial area corresponding to one-quarter of the segmented iris image size. The low and high frequencies represent a bandwidth corresponding to $0 < |\omega| < \pi/2$ and $\pi/2 < |\omega| < \pi$ respectively. Fig. 4 shows the process of MRA of an iris left segment. The wavelet transformation is defined in (5)-(6).

$$W(a,\tau_X,\tau_Y) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)\psi_{a,\tau_X\tau_Y}(x,y)dxdy \quad (5)$$

$$\psi_{a,\tau_X\tau_Y}(x,y) = \frac{1}{|a|}\psi\left(\frac{x-\tau_X}{a},\frac{y-\tau_Y}{a}\right) \quad (6)$$

where f(x,y) is a segmented iris image, $W(a,\tau_x,\tau_y)$ is a wavelet transform function, $\psi_{a,\tau_X\tau_Y}(x,y)$ the wavelet basis function, a is a scaling factor, τ_x and τ_y are translation factors of x and y axes, respectively.

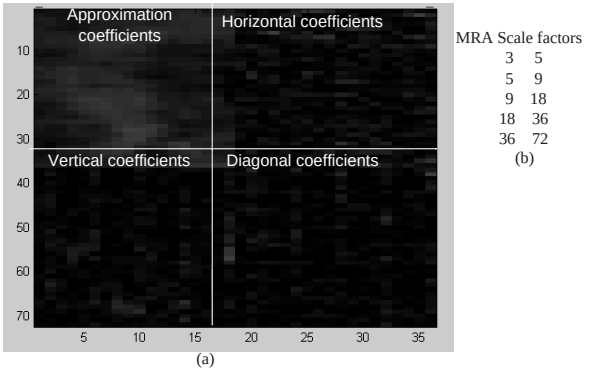


Fig. 4 Illustration of multi resolution analysis of left iris segment

After the four level of decay process, horizontal, vertical and diagonal coefficients of the iris segment are used for iris feature encoding process. The decomposition coefficients are described in (7) to extract iris feature codes.

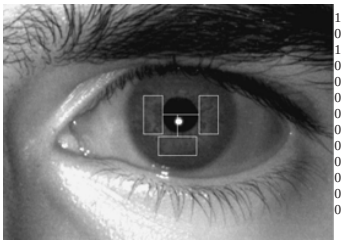
$$IFC(x) = \begin{cases} 1 & if\ (H_{ijk}, V_{ijk}, D_{ijk}) > 0 \\ 0 & if\ (H_{ijk}, V_{ijk}, D_{ijk}) \le 0 \end{cases} \quad (7)$$

$$For\ \ i = 1..m,\ For\ \ j = 1..h,\ For\ \ k = 1..w\ and\ For\ \ x = 1..N$$

where IFC(x) is x^{th} iris feature code, H_{ijk} , V_{ijk} and D_{ijk} represent horizontal, vertical and diagonal coefficients in i^{th} level decay process, m is maximum number of decomposition, h and w are the height and width of the decomposed iris image respectively and N is the number of iris feature code. Iris feature encoding process extracts 135-bit code from each iris pattern. These bits of sequence are called iris feature set. This set is used for verification and recognition process in the iris-matching module. An enviable feature set of an iris is rendered in Fig. 5. Although Iris patterns are unique in nature, a user could position the same eye on a biometric device for years and never be generated identical iris templates. This is due to change in imaging position, distance, lighting conditions, and eyelashes-eyelid being occluded, spectacle reflection and hard contact lens. These artifacts may create uncertainty in the iris matching and iris cryptosystem system.

C. Iris Matching

In the iris matching process, intra and inter class iris features are efficiently separated and they prevent imposters from entering into the secure system. To authenticate any genuine user, iris feature sets are treated as trained sets and stored in the encrypted file. Verification subjects' irises are represented as test sets. At any instant when no test set is present, the probability density for a trained set is normal, that is, $p(x|\omega_1) \sim K(\mu_1, \sigma^2)$ and when the test set is present, the density is $p(x|\omega_2) \sim K(\mu_2, \sigma^2)$.



(a) (b)

Fig. 5 (a) Illustration of feature selection (b) Binary value iris feature codes

A decision threshold X^* is used to determine the probability of a hit and a false alarm. Iris trained and test sets are compared to determine whether the test set belongs to the intra class or inter class. Iris matching is computed based on minimum distance between two iris feature sets defined as, $\min\{WD(IFC(x_{trained}), IFC(x_{test}))\}$, where $WD(IFC(x_1), IFC(x_2))$ represents weighted distance in between two iris feature sets. The weighted distance is calculated using exclusive-or operation that provides faster iris matching process as defined in (8). Eyeball may be rotated in the image acquisition process due to head tilt, thus 4 times left or right shift operation is carried out with the iris bits in the matching process.

$$WD(IFC(x_{trained}), IFC(x_{test})) = \frac{\left| IFC(x_{trained}) \oplus IFC(x_{test}) \right|}{N} \quad (8)$$

where N is the number of bits in the iris feature set.

The weighted distance (β) is used to determine the number of error bits in between two iris classes. The distance of the intra class iris feature set is discriminated by the constraint $0 \le \beta \le 0.19$ and the inter class iris features is discarded with the constraint $\beta > 0.19$.

IV. Iris Cryptosystem

The iris key can be executed in two different approaches namely, conventional iris cryptosystem and non-repudiation cryptosystem. The architecture of these two approaches is elaborated in following sections.

A. Conventional Iris Cryptosystem (CIC)

Iris patterns are also used for fabricating a key to encipher and decipher the plain text in between sender and receiver over insecure channels. 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 CIC system. In order to decrypt a message the recipient needs an identical copy of the iris code. Fig. 6 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 end, which can be used for the decryption process. The proposed approach uses XORed operation to encrypt and decrypt the message. The significant steps of CIC encryption algorithm is described as follows:

Step 1: Let K be the key sequence produced by iris feature encoding algorithm for an encryption transformation. The sequence of iris bits is $I_1, I_2, ..., I_p \in K$. It is called an iris key sequence. In the experiment, in order to divide the messages into 8-bit, the 135-bit iris code is converted to 136-bit code with 1-bit padding. Therefore, key becomes $I_1, I_2, ..., I_{136} \in K$.

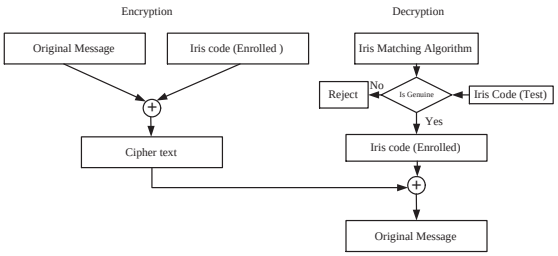


Fig. 6 The process of CIC system

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 binary string, The bits of messages undergo XORing with iris key sequence and generate a non-breakable cipher-bit as described in (9).

$$C_i = Ency((S_1, S_2, ..., S_n) \oplus (I_1, I_2, ..., I_p)) \quad (9)$$

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 enrolled iris codes. If weighted distance is $0 \le WD \le 0.19$ then the matched enrolled iris code is used for deciphering the messages.

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 sent by the encryption process. Enrolled iris codes are XORed with set of cipher bits and produce the original messages is as depicted in (10).

$$S_i = Decy(C_1, C_2, ..., C_n \oplus I_1, I_2, ..., I_p) \quad (10)$$

where S_i is set of source alphabet bits. In the CIC 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 solve repudiation problem the iris database and iris-matching algorithm are eliminated from the CIC system. The detailed description of this process is discussed in the next section.

B. Non-repudiation Iris Cryptosystem (NRIC)

Unlike CIC system, the NRIC system bypasses the iris-matching process and avoids iris database in the decryption process. The testing iris code can directly be XORed with cipher bits transmitted from the encryption process as illustrated in Fig. 7. As we have seen already, iris codes are changed from session to session with minimum variation (β<=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 bits 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 subject have probability of error rate at most 0.19, so that, less complexity is created in the decryption process. The cipher bits are XORed with the test iris code that produces the partially corrupted bits. These bits are subsequently corrected by the error bit correction module using autocorrelators, which performs probability of error correction based on iris-weighted distance.

C. 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 autoassociative memory. For the recall operation, autoassociatives require the correlation memory or connection matrix, which aids to retrieve original patterns from the partially corrupted pattern. It is called as autocorrelators. We adopt this model in the error correction process of NRIC. 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 to bipolar patterns (ϕ). Let M be the number of stored bipolar patterns $p_1, p_2, ..., p_m$ for example, ith patterns is $(p_{i1}, p_{i2,\cdots}, p_{in})$ where n is the number of bits in the store pattern. The connection matrix CM is derived using (11).

$$CM_{ij} = \sum_{i=1}^{n} \left[p_i^T \right] \left[p_i \right] \; for\, i = 1...n, \; for\, j = 1..n \quad (11)$$

Step 2: The autocorrelator recalls the original patterns (θ) using the (12) (13).

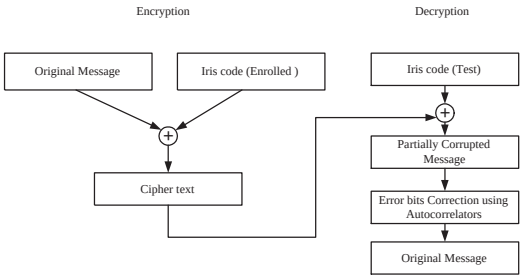


Fig. 7 The critical steps involved in non-repudiation iris cryptosystem

$$\theta_j = g((\phi_j * CM), p_j) \;\; for\; j = 1..m \quad (12)$$

$$g(\chi, \varphi) = \begin{cases} 1 \; if \;\; \chi > 0 \\ \varphi \; if \;\; \chi = 0 \\ -1 \; if \;\; \chi < 0 \end{cases} \quad (13)$$

where θ_j is the recalled original pattern, ϕ 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 genuine subject 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

$$p_1 = [1 \;\; 1 \;\; -1], p_2 = [-1 \;\; -1 \;\; 1], p_3 = [1 \;\; -1 \;\; 1]$$

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 $p = [-1 \;\; 1 \;\; 1]$ then the computation with CM produce the threshold conditions: g(-3,-1),g(-1,1), and g(1,1). It gives the original pattern $O = [-1 \;\; -1 \;\; 1]$.

V. Experiments

The proposed approach has been implemented and results were analyzed in Java and MATLAB languages. The time efficiency has been observed on Pentium IV 2.4 GHz machine with 256 MB RAM. The experimental result is based on 2500 eye images from 500 subjects. Five different experiments have been performed for analyzing the efficiency of the proposed system. The types of experiments are: Statistical analysis of the iris weighted distance, time complexity of autocorrelators,

encryption and decryption time with respect to the size of the messages, and strength of autocorrelators with the complexity of iris key. The detailed descriptions of each experiment are discussed in the following sections.

A. Statistical Analysis

Statistical decision plays a vital role in large population problems. As for as iris feature is concerned, the iris database is increased in proportion to the number of iris features enrolled in the system. Hence, making a decision whether a specified iris feature belongs to a particular class or not is the statistical hypotheses. It is useful to make assumptions about the population involved that may or may not be true. In iris recognition process, subjects' iris was compared with remaining irises available in the database, a match and non-match decisions were taken based on weighted distance (β) in the range between $0.0 \le \beta \le 0.19$ and $\beta > 0.19$ respectively. Iris Database consists of 2500 different iris images, i.e., N (N-1) = 6247500 possible comparisons were made. As per statistical theory, the system is investigated based on an idealized situation where the iris-features are measured more and more accurately for an increasingly larger database. That is, normal distribution, which provides distribution between the relative frequency density and iris feature distances. Normal distribution (ND) is defined in (14).

$$ND(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) \quad (14)$$

where x is the weighted distance with mean μ and standard deviation σ.

Fig. 8 shows histogram of iris codes, intra-class (same) and inter-class (different) normal distribution of iris-weighted distances. The experimental results were observed that the mean of weighted distance of intra-class iris codes was μ=0.10813 with standard deviation σ= 0.0392 and degree of freedom, $\nu = \mu(1-\mu)/\sigma^2$, ν=62.621991. Inter-class iris code mean was μ=0.27104 with standard deviation σ=0.040730. This statistical analysis shows that the proposed method allows the genuine subject to access the system in the compressed manner and refuses impostors in extensive manner that is aptly suited for cryptography system.

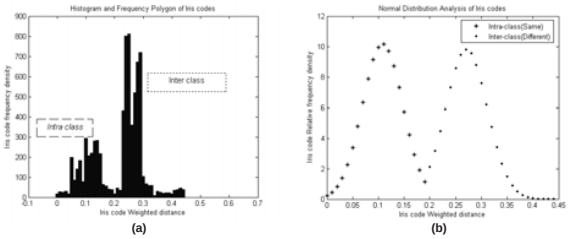


Fig. 8 Iris weighted distance (a) Histogram of iris codes (b) Normal dissemination of iris codes

B. Time Complexity of Autocorrelator

The time complexity of autocorrelations is dependent on size of the connection matrix in the error correction process. The connection matrix is formed based on the number of bits processed by the cipher text. For the experiments, 26 patterns were accessed and each has 8-bit length then the connection matrix size was 8 by 8. In accordance with the number of patterns and bits the time complexity of autocorrelators were evaluated which is shown in Fig. 9.

C. Encryption and Decryption Time

The time complexities of encryption and decryption process have been evaluated in the conventional and non-repudiation iris cryptosystem. In the CIC system, encryption process required less time than decryption process. Since the decryption is based on iris feature extraction and iris matching process. It consumes nearly 1.52 seconds. It is included in the decryption processing time. The time evaluation of encryption and decryption process is given in Fig. 10. The NRIC system required slightly more time than the CIC approach because its error bit correction operation is based on neural family that required more time to predict the original patterns from the partially corrupted patterns.

D. Probability of Error Bits and Intruder Complexity

The probability of presence error in the non-repudiation process was assessed based on the number of bits variation. It occurred due to the environment, illumination, occlusion of eyelids/eyelashes and other artifacts. In this experiment, the number bit corrupted in different sessions were studied. The system was verified in which situations brute force search by an intruder can crack the iris crypto key. For the experiment, different eye images have been captured in different sessions for the same subject. The variation of iris bits is illustrated in Fig. 11.

No. of Patterns	No. of Bits/Pattern	Recalling time(msec.)
3	3	0.190107
3	5	0.316845
3	8	0.506952
5	3	0.316845
5	5	0.528075
5	8	0.84492
10	3	0.63369
10	5	1.05615
10	8	1.68984
15	3	0.950535
15	5	1.584225
15	8	2.53476
26	3	1.647594
26	5	2.74599
26	8	4.393584

(a)

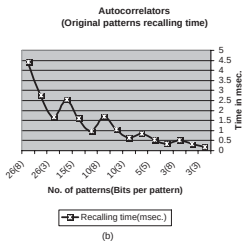


Fig. 9 Time complexity of autocorrelators (a) Recalling time (b) Visualization of original pattern recalling time

These variations produced the number of corrupted bits in the decryption process. 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 this approach was made 2^{n-26} times of the complexity for brute force search to an intruder. For example, if 100 bits were error then 2^{74} times of complexity for brute force search was made by an intruder to get back the original message. Thus the complication of retrieving the original

messages has been given to the impostors in the iris cryptosystem. 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. Experimental results were shown that this approach could easily be adopted in the on-line cryptography system.

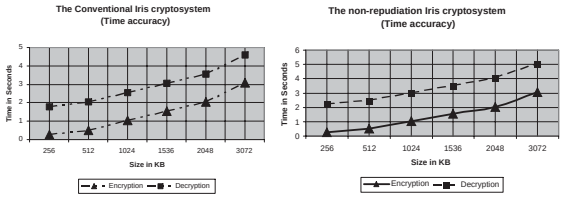


Fig. 10 Encryption and decryption time accuracy of the iris cryptosystem

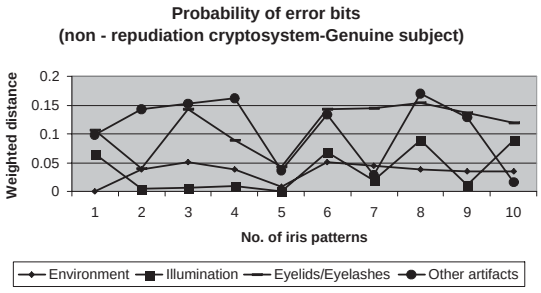


Fig. 11 Error bit variation for the same subject in different

VI. Conclusion

This paper proposed a novel approach for iris based cryptography system. The crypto keys have been generated using iris patterns, which is stable through out person's lifetime, as well, its inter-class variability for a person are very large. Since it creates more complexity to crack or guess the crypto keys. This approach has reduced the complicated sequence of the operation to generate crypto keys as in the traditional cryptography system. It can generate more complex iris keys with minimum amount of time complexity, which is aptly suited for any real time cryptography. This approach was executed with autocorrelators that resolves key repudiation problem occur in the traditional system. The autocorrelators can predict the number of bits corrupted in the decryption process with the help of vigilance parameter. It prevents intruder to get back the original messages, in 2^{110} times of complexity. The synthesis of iris code with existing encryption system and their related problems create a new path for cryptography research. The Experimental results illustrate that the proposed approach can easily be incorporated into the existing encryption standards as well as the key generation and the key release issues were also considerably reduced. This approach will be improved further with fusion to any cryptography system.

References

[1] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in Proc. IEEE Symp. Privacy and Security, pp. 148–157, May 1998.

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

[3] M. G. Linnartz, P. Tuyls. New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates, AVBPA 2003, pp. 393–402, 2003.

[4] T. Clancy, N. Kiyavash, D.J.Lin. "Secure Smartcard-Based Fingerprint Authentication", Proc. of the 2003 ACM SIGMM workshop on Multimedia, Biometric Methods and Applications, pp 45-52, 2003.

[5] F. Monrose, M. Reiter, Q. Li, S. Wetzel. Cryptographic key generation from voice, Proc. IEEE Symp. on Security and Privacy, pp. 201-213, 2001.

[6] Uludag, U., Sharath Pankanti, Salil Prabhakar, Anil Jain, Biometric Cryptosystems: Issues and Challenges, Proc. of the IEEE, VOL.92, No.6, pp.948-960, June 2004.

[7] John Daugman, How Iris Recognition Works, IEEE Transactions On Circuits and Systems For Video Technology, Vol. 14, No. 1, pp.21-30, January 2004.

[8] Li Ma, Tieniu Tan, Yunhong Wang, and Dexin Zhang, Efficient Iris Recognition by Characterizing key Local variations, IEEE Transaction on Image processing, Vol.13, No.6, June 2004.

[9] Shinyoung Lim , Kwanyong Lee, Okhwan Byeon, and Taiyun Kim, Efficient Iris Recognition through Improvement of Feature Vector and Classifier, ETRI J., Vol. 23, No. 2, PP. 61-70, June 2001.

[10] A.Chitra and R.Bremananth, Efficient Identification Based on Human Iris Patterns, Proceedings of Fourth Indian Conf. on Computer Vision, Graphics and Image processing (ICVGIP), PP. 177-183, December 2004.

[11] A. Chitra and R.Bremananth, Secure PID using iris pattern based on circular symmetric and Gabor filters, Proceedings of Inter. Conf. Advanced Computing and Communication (ADCOM), PP. 36, December 2003.

[12] Canny, John. "A Computational Approach to Edge Detection", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 8, No. 6, pp. 679-698, 1986.

[13] Rafael C. Gonzalez, Richard E. Woods, Steven L.Eddins, "Digital Images processing using MATLAB", Pearson Education, 2004.

[14] Jane Miller, "Statistics for Advanced level", Second edition, Cambridge University press, 1996.

[15] Michael Negin Thomas A. Chmielewski,et al., "An iris biometric system for public and personal use", IEEE catalog No. 0018-9162, 2000.

R. Bremananth received the B.Sc and M.Sc. degrees in Computer Science from Madurai kamaraj and Bharathidsan University, India in 1991 and 1993, respectively. He has obtained M.Phil. degree in Computer Science & Engineering from Bharathiar University. He is currently working towards the Ph.D. degree in the Department of CSE, PSG College of Technology, India. He is a Senior Lecturer Department of Computer Science, Sri Ramakrishna Engineering College, Coimbatore. He has 10 years of teaching experience and published several research papers in the National and International conferences/Journals. His fields of research are pattern recognition, computer vision, image processing, biometrics, multimedia and soft computing.

Mr. Bremananth is a member of Indian society of technical education, advanced computing society and IETE, India

A Chitra received the Ph.D. and M.E. degrees in Computer Science and Engineering from Bharathiar Uinversity, India. She is currently a Professor in the Department of Computer Science and Engineering, PSG College of Technology, India. She has 15 years of teaching experience and published several papers in the national and international conferences/Journals. Her fields of research are soft computing, image processing, biometrics, and computer vision.

Dr. Chitra is a fellow of Advanced Computing Society and Computer Society of India.