CHAPTER 6

IRIS CRYPTOSYSTEM

6.1 INTRODUCTION

Cryptography provides a secure proliferation of information exchange across the insecure channel. It authenticates messages based on the key but not on the user. It 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. 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 alternative that can be used to resolve key management, large key computational process and address the non-repudiation problems. 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 unauthorised to work with the system.

Thus, a reliable alternative to the password security is the biometric guard for the cryptography keys, that is, whenever user wishes to access a secured key, biometric samples are captured, authenticated by the classifiers and then key is released to encipher and decipher the desired data. In general biometric cryptosystem has been classified by three categories, first method is to release the cryptography key from secure area in accordance with biometric matching algorithm and it requires the secured communication line to avoid eavesdroppers 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 disastrous to the system. A 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, and 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 artefacts. However the more stable pattern produced by the iris is secured in the person’s lifetime and produce limited number of bits variations in the features, which help 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 (1994) proposed a method of directly using biometric as cryptography key in the patent of German. In (Davida et al 1998, Davida et al 1999), 2048-bit iris code was used for enciphering and deciphering process. Key generation 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 and Tuyls 2003, Clancy et al 2003, Monrose et al 2001), the key generation was based on biometrics such as fingerprints 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 (2004). The survey of multi-biometric cryptosystems was discussed by Uludag et al (2004). A method of iris compression for cryptography documentation on off-line verification was proposed by Daniel et al (2004). 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 (2005) 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.

The block diagram of the proposed iris cryptosystem is illustrated in Figure 6.1. 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 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 autocorrelators and heterocorrelators 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 analysed 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.
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. 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 6.2 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 and 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 as described in Equation (6.1)

$$C_i = Ency(s_1, s_2, ..., s_N \oplus I_1, I_2, ..., I_p) \quad (6.1)$$

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 $0 \leq WD \leq 0.19$ 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 (6.2).
Figure 6.2 The process of SIC system

\[ S_i = Decy(C_1, C_2, ..., C_n \oplus I_1, I_2, ..., I_p) \]  \hspace{1cm} (6.2)

where \( S_i \) is set of source alphabet bits. 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.

6.3 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 Figure 6.3. 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 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 subjects have probability of error rate at most 0.19, so that, less complexity have been created in the decryption process.

Figure 6.3 Non-repudiation iris 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 autocorrelators or heterocorrelators 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.

6.4 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 (1988) enhanced the bidirectional associative memories (BAM), which behaves as a heteroassociative content addressable memory (CAM) storing and recalling the vector pairs. The bidirectional associative memory with multiple training, which can be guaranteed to recall a single trained pair under suitable initial conditions of data and sufficient condition for a correlation matrix to make the energies of the training pairs were described by Yeou-Fang et al (1990). Essential conditions for generalisation of correlation matrix of BAM which guarantees the recall of all the training pairs was discussed by Yeou-Fang et al (1991). This thesis adopts two different methods to recall the corrupted patterns. The first one is related to autoassociative and the other one is concerned with heteroassociative.

6.4.1 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 and is adopted 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 \( \phi_c \). Let \( M \) be the number of stored bipolar patterns \( p_1, p_2, \ldots, p_m \) and \( i^{th} \) pattern is \( (p_{i1}, p_{i2}, \ldots, p_{in}) \) where \( n \) is the number of bits in the stored pattern. The connection matrix \( CM \) is derived using (6.3).

\[
CM_{ij} = \sum_{i=1}^{n} p_i^T \quad \text{for } i = 1..n, \text{for } j = 1..n \quad (6.3)
\]

**Step 2:** The autocorrelator recalls the original patterns \( \theta \) using Equations (6.4 - 6.5).

\[
\theta_j = g((\phi_{cj} * CM), p_j) \quad \text{for } j = 1..m \quad (6.4)
\]

\[
g(\chi, \varphi) = \begin{cases} 
1 & \text{if } \chi > 0 \\
\varphi & \text{if } \chi = 0 \\
-1 & \text{if } \chi < 0 
\end{cases} \quad (6.5)
\]

where \( \theta_j \) is the recalled original pattern, \( \phi_c \) 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 \( \rho \) is a vigilance parameter.
The parameter $\rho$ 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 $p_1=[1 \ 1 \ -1]$, $p_2=[-1 \ -1 \ 1]$, $p_3=[1 \ -1 \ 1]$ then the connection matrix (CM)

$$
\begin{bmatrix}
3 & 1 & -1 \\
1 & 3 & -3 \\
-1 & -3 & 3
\end{bmatrix}
$$

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 $O=[-1 \ -1 \ 1]$.

### 6.4.2 Heterocorrelators

In this approach noisy variation of different types of iris codes are not explicitly estimated and stored in the verification database. If they may explicitly be estimated then it leads to leak of security information to the adversary. Hence, heterocorrelations 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 and this model recalls a $y$ if $x$ is given or vice-versa. It is called heteroassociative memory. This memory is used to recall the original patterns from the
corrupted patterns. For the recall operation, heteroassociative requires a correlation memory or connection matrix, which aids to retrieve original patterns. This is so-called heterocorrelators. 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 ($\delta$). Let M be the number of stored bipolar pairs as given in Equation (6.6).

$$\langle \{ P_1 \cdot Q_1 \}, \{ P_2 \cdot Q_2 \}, \ldots, \{ P_m \cdot Q_m \} \rangle$$  \hspace{1cm} (6.6)

where $P_i = \{ p_{i1}, p_{i2}, \ldots, p_{in} \}$, $Q_i = \{ q_{i1}, q_{i2}, \ldots, q_{io} \}$, P and Q represent stored and exemplar patterns of distorted bipolar data, respectively. The connection matrix (CM) is derived using Equation (6.7).

$$CM_{ij} = \sum_{i=1}^{n} E_i \left[ P_i^T \right] \left[ Q_i \right] \text{ for } i = 1 \ldots n, \text{ for } j = 1 \ldots o$$  \hspace{1cm} (6.7)

where CM is a correction matrix used in the heterocorrelation process and $E$ is a set of energy constants i.e., $E \in R^+$. R is a set of real numbers. Calculate $\kappa'$ and $\kappa$ from Equations (6.8) and (6.9) and assign to $\delta'$ and $\delta$, respectively.

**Step 2:** The heterocorrelator recalls the original bit sequences ($\varphi$) using Equations (6.8 – 6.12).

$$\kappa' = \Theta(\delta \cdot CM)$$  \hspace{1cm} (6.8)

$$\kappa = \Theta(\kappa' \cdot CM^T)$$  \hspace{1cm} (6.9)
\[ \Theta(\lambda) = \varphi = \varphi_1, \varphi_2, \ldots, \varphi_n \]  \quad (6.10)

\[ \lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_n\} \]  \quad (6.11)

\[ \varphi_i = \begin{cases} 
1 & \text{if } \lambda_i > 0 \\
\varphi_i & \text{if } \lambda_i = 0 \\
-1 & \text{if } \lambda_i < 0 
\end{cases} \]  \quad (6.12)

where \( \delta \) is a set of partially corrupted bipolar bits generated by the decryption process, \( \Theta \) is a threshold function of heterocorrelation, \( \lambda \) represents multiplication result of the correction matrix for the given distortion bit patterns, \( \varphi \) is set of the recalled bits, \( \kappa' \) represents result of exemplars and \( K \) is a sequence of corrected bits.

**Step 3:** After performing error correction process, find out the weighted distance between corrupted and corrected exemplar bits using Equation (6.13).

\[ \Phi = \left[ \sum_{i=1}^{n} |\delta'_i - \kappa'_i| \right] \]  \quad (6.13)

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 heterocorrelators.

If \( \Phi \leq \rho \) 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.

where $\rho$ is a vigilance parameter and it is calculated as $\rho = (n - \text{mod}(n,2))$ i.e., $0 \leq \rho \leq (n - \text{mod}(n,2))$ and $n$ represents number of bits in an exemplar. The parameter $\rho$ 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 $\rho$ 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.

6.5 EXPERIMENTAL RESULTS

The proposed approach has been implemented and results were analysed based on 2500 iris patterns. 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.
6.5.1 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 once 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 shown in Figure 6.4.

![Figure 6.4 Encryption and decryption time complexity of SIC and NRIC](image)

Figure 6.4 Encryption and decryption time complexity of SIC and NRIC
6.5.2 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 Figure 6.5.

![Figure 6.5 Auto and hetero correlators’ recalling time](image)

6.5.3 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 artefacts 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 thesis, 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 artefacts are fully concerned with three possessions such as acquisition time users’ co-operation, non-iris fractions occurring on iris and artefacts 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 6.6 shows the accuracy of recalling patterns using auto and hetero correlators.
6.5.4 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 artefacts. In this experiment, the number of bits corrupted in different sessions were 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 6.7 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
were 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 \( A = \{a_1, a_2\} \) 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.

![Probability of error bits](image)

**Figure 6.7 Error bit variation for the same subject in different criterion**

Thus the retrieving 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.

### 6.5.5 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. Hence encryption algorithm needs an efficient solution, 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 life long biometric templates. Thus the iris-based cryptosystem performs better accuracy by using re-enrolments. In this thesis, 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 artefacts 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.
6.6 CONCLUSION

This thesis 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 heterocorrelators 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.