CHAPTER III

CRYPT-IRIS BASED PERCEPTION AND AUTHENTICATION APPROACH

The previous chapter focused on various conventional routing protocols of MANET. The performance of these protocols was comparatively analyzed by utilizing the simulated data available from literature to focus on their limitations. In this chapter important concepts related to biometrics and iris recognition system are discussed. A crypt-iris based perception and authentication approach is developed in MATLAB that takes into consideration a standardized database for analysis. Biometric perception is considered to be the most neoteric technology for sustaining security in various systems by involving exclusive identification features. The attainment of biometric perception depends upon image procurement and biometric perception system. This proffered algorithm focuses on attaining image procurement as well as biometric perception by an effective exploitation of bi-orthogonal wavelets for encoding biometric information. The biometric system is enhanced by incorporating cryptographic features which results in better solution against various security breaches.

3.1 INTRODUCTION

MANET is infra-structure less network that perform the basic networking function, as a router and also packet forwarding, contrary to the other mobile networks. Due to the various intrinsic vulnerabilities present in MANET, security is a basic and paramount requirement for users who desire services such as authentication, integrity, non-repudiation, confidentiality, key and trust management and access control for performing protected peer-to-peer communication over multi-hop wireless channel. Therefore, security, routing and QOS are critical issues, that require immediate research attention due to the dynamic, unpredictable nature of most ad-hoc networks and also as they vary from each other greatly from the viewpoint of the area of application. Security solutions utilized by most of the conventional approaches include simple encryption, username-password authentication scheme on one hand and cryptography that implicates a strong demand for secure and efficient key management mechanism on the other hand. Also, there is a requirement of a proper
authentication mechanism that should restrict the access of foreign nodes to the network. Security mechanisms are indispensable for mobile ad-hoc networks as they are inherently vulnerable to attacks hence, posing both challenges and opportunities for future research analysis and design. Therefore, this research study focuses on one of the most unique, popular and considered to be the most enhanced security solution for various networks and devices, referred as biometrics.

The study of the physical and behavioural characteristics of human beings for the purpose of authentication is referred as biometrics. Commonly exploited biometrics modalities are represented in figure 3.1 which can be classified as behavioural or physical. Depending upon the sort of typical behaviour of a user the behavioural modalities make an attempt to identify the user, for e.g. how a person walks, how holds a pen, how presses the key when enter Personal Identification Number (PIN), etc.

![Biometric Modalities](image)

**Figure 3.1 Biometric Modalities**
Physiological methods on the other hand identify physical traits namely; fingerprint, face, **iris**, retina, etc., typical to a particular user. Two categories are stated by biometric systems namely identification and verification. “Who you are” is specified by identification system while “Are you the one whom you claim to be” is specified by the verification system. From olden times biometric identification is applied. Thumb impressions, signature, photographs and identity cards are quite important for the verification of the identity of human beings. Automated biometric is the growing area of research of biometric technology. Face, fingerprint, voice, iris, speech, hand geometry, retina, etc., are some of the traits of human beings utilized by a biometric system. For various critical processes reliable personal recognition is quite important. Systems safeguarded for security and reliability, against criminal attacks are important in modern day world, that’s why various public and private organisations have improved the traditional security systems with biometric systems. Main aim of developing a secure biometric system is to establish identity based on who the person is rather than what are the possessions of system or what a person remembers (e.g. ID card or password).

For MANET, user authentication is quite critical for preventing various unauthorised users from causing modification of resources of the network. Due to the dynamic nature of such systems there is an extremely high chance of system being captured in a hostile environment therefore, there is frequent and continuous requirement of authentication. Various validation factors namely, knowledge factors, possession factors and biometrics factors are exploited for performing user authentication. Passwords as knowledge factors and tokens as the possession factors are quite easy to be implemented but distinguishing an authenticated user from impostor becomes difficult since, no direct connection exist betwixt user and password or user or token. The technology of biometrics deals with recognition of fingerprints, irises, faces, retina, etc., provides various possible solutions for the authentication problems that exist in MANET.

Processes in a biometric system and iris recognition system are discussed in starting sections of this chapter followed by the proposed neotric iris perception algorithm with its simulation study. The later portions of the chapter focus on threshold cryptography and implementation of novel crypt-iris based authentication approach. Result analysis and conclusions of the chapter are done in the last sections.
3.2 PROCESSES IN A BIOMETRIC SYSTEM

Figure 3.2 depicts the processes in biometric system independent of the trait being utilized. Data capturing marks the beginning process which acquires the biometric sample. This follows with feature extraction which leads to the creation of biometric signature. The developed biometric signature is compared with a particular or several biometric signatures that are being registered in the knowledge database, together designated as biometric templates. They are collected during the enrolment process which corresponds to an identity that is subject verified. When the acquired biometric signature matches with the template then the identity being claimed is the same identity being stored otherwise it belongs to a different identity.

The comparisons done between the templates determine the basic distinction betwixt the nodes that are exploited for performing biometric recognition namely verification and identification. One to one match is resulted by the verification process where the identity of the person is verified by the biometric system. On presenting a new sample to the system, calculation of the difference between the new sample and its corresponding template (which is stored previously in the system) is done and the comparison of the computed difference and predefined threshold takes place. New sample is being accepted if the difference comes out to be smaller otherwise rejection of sample occurs.

![Figure 3.2 Processes in Biometric System](image-url)
Analysis of any biometric system cannot be completed without performing various specificity and sensitivity tests. True acceptance occurs when the accepted new sample and template are being specified from the same subject otherwise the acceptance is referred as false acceptance. False Acceptance Rate (FAR) is the percentage of the false accepts. If the new rejected sample and the corresponding biometric templates are not coming from a same subject the rejection is true rejection otherwise its false rejection. The trade-off between FAR and FRR is depicted in figure 3.3. If FAR=FRR equal error rate is obtained. Better performance of the system is indicated by smaller ERR. Selection of ERR to achieve optimal performance is done by setting the acceptance threshold value but it happens rarely as it depends on the application of biometric.

For e.g. during money withdrawal through ATM it's better to risk a few false accepts than to annoy the customers again and again, when the authorized users are rejected by the system. One to one match happens in identification where the new biometric sample is compared with all the existing templates and the template with the minimum difference, greater similarity is being chosen as the ID result. A correct match occurs if the new sample and selected template are coming from the same subject.

![Figure 3.3 Trade-off Between FAR and FRR](image-url)
3.3 IRIS RECOGNITION

Boles and Boashash (1998); Daugman (1994); Ma et al. (2002); Wildes (1997); Wildes et al. (1994); have focussed that biometric identification is becoming quite a popular tool and gaining more acceptance in various sectors. One of the highly accurate and reliable methods to be considered for biometric identification is iris recognition as the iris is considered to be very stable, highly unique and easy to capture when compared with other biometric identifiers. For personal identification, image processing and signal processing the unique epigenetic patterns of a human iris are employed for extracting information which is encoded to formulate a “biometric template”. This biometric template is stored in a database and also utilized for identification purposes. The proposed wavelet based crypt-iris recognition and authentication approach is developed for securing MANET which results in a highly secure environment. Figure 3.4(a) focuses on view of human eye and its various parts and (b) depicts the headmost prospective of annular component called iris. Iris regulates the extent to which light can insinuate through the pupil and this function is carried by the sphincter and the dilator muscles by modifying pupil size. Iris may have T average diameter of 12 mm whereas pupil size varies from 10% to 80% of the iris diameter. An iris template can be created from 173 out of relatively 266 peculiar inclinations hence; iris perception is the most assuring biometric mechanics. There is a requirement of procreation of various iris perception algorithms as it is proving to be an enhanced security tool for MANET.

![Figure 3.4 (a) Front View of Human Eye (b) A View of Iris](image_url)

The general framework of iris recognition algorithm divides it into four parts namely, segmentation that isolates the iris in an eye image under consideration; mapping maps each pixel of the isolated iris from concentric domain to non-concentric domain; encoding
performs quantization and mapping of the filter coefficients into a binary bit stream hence, building a template; finally matching is done to reflect the similarity score by various matching algorithms like hamming distance, correlation coefficient, etc. Data Management is very important for testing the designed algorithm on sufficiently large as well as a diverse data set provided by the Chinese Academy of Science, CASIA, West Virginia University and Lions Eye Institute, LEI (standard databases). As specified by Sweldens 1995 an iris perception algorithm performs recognition for ideal conditions as well it is quite flexible to be adapted for the non-ideal cases like off angle images, noise, etc. The various steps required for developing a secure iris perception algorithm are described below.

3.3.1 Isolation or Segmentation

Segmentation is termed as the first stage of iris recognition that isolates the actual iris region in a digital eye image. Figure 3.4(a), depicts the front view of human eye that can be approximated by two circles, one for the iris/sclera and another for the iris/pupil boundary. The upper and lower parts of the iris region are occluded by the eyelids, eyelashes, and specular reflections (referred as noises of iris image) that can occur within the iris region corrupting the iris pattern. Therefore, a technique is required for isolating and excluding the above mentioned artefacts as well as for locating the circular iris region. Segmentation is one of the most critical stages of iris recognition algorithm as its success depends on the imaging quality of various eye images. CASIA iris database do not contain specular reflections due to the use of near infra-red light for illumination whereas the images in the LEI database contains some specular reflections, caused by imaging under natural light. Also, persons with darkly pigmented irises will present very low contrast between the pupil and iris region if imaged under natural light, making segmentation more difficult. Therefore, accurate segmentation is required as data can be falsely represented in an iris pattern, that will cause corruption of the biometric templates generated hence, resulting in poor recognition rates as specified by Barry and Ritter. Various methods are available in literature for performing the segmentation/isolation of the iris image as discussed below.

●Hough Transform

For determining the parameters of various simple geometric objects (lines or circles) a standard computer vision algorithm referred as the Hough transform is applied as described by Kong and Zhang (2001); Ma et al. (2002); Tisse et al. (2002); Wildes et al. (1994). This
transform is also employed for deducing the radius and centre coordinates of the parts of eye namely pupil and iris regions. In starting of Hough transform, generation of edge map takes place by calculation of the first derivatives of intensity values in an eye image and then thresh-holding of the result is done. In Hough space votes are casted from the edge map for the parameters (centre coordinates $x_c$ and $y_c$ and the radius $r$) of circles passing through each edge point, which are able to define any circle according to the equation:

$$x^2 + y^2 - r^2 = 0$$

-- (3.1)

Kong and Zhang (2001); Wildes et al. (1994) have also utilized parabolic Hough transform for approximating the upper and lower eyelids with parabolic arcs, which are represented as:

$$((-x-h_j) \sin \theta_j + (y-k_j) \cos \theta_j)^2 = a_j((-x-h_j)\cos \theta_j + (y-k_j)\sin \theta_j)$$

-- (3.2)

where:

$a_j =$ parameter to control the curvature.

$h_j, k_j =$ parameters for representing the peak of the parabola.

$\theta_j =$ angle of rotation relative to the x-axis.

For performing the preceding edge detection step Wildes et al. (1994) have biased the derivatives in the horizontal direction for detecting the eyelids and in the vertical direction for detecting the outer circular boundary of the iris, which is depicted in Figure 3.5(a) (b) (c) (d).

---

Figure 3.5 (a) An Eye Image (020_2_1 from the CASIA database) (b) Corresponding Edge Map (c) Edge Map with only Horizontal Gradients (d) Edge Map with only Vertical Gradients

http://www.pccegoa.org/pcce/etc/synopsysETCprojects.htm
The main motivation for performing edge detection is that the eyelids are usually horizontally aligned and also the eyelid edge map will cause corruption of the circular iris boundary edge map if all gradient data is utilized. For locating the iris boundary only the vertical gradients are taken that will reduce influence of the eyelids for performing circular Hough transform as for successful localisation, not all of the edge pixels defining the circle are required. Hence, making circle localisation more accurate and more efficient as there are less edge points to cast votes in the Hough space.

● **Daugman’s Integro-differential Operator**

To locate the circular iris and pupil regions and the arcs of the upper and lower eyelids Daugmann utilises the integro-differential operator which is defined as:

\[
\left| G(r) \ast \frac{\partial}{\partial r} \oint_{|x,y| = r} \frac{I(x,y)}{2\pi r} \, ds \right| \quad -- (3.3)
\]

where:

\( I(x, y) = \) intensity value at the location \((x, y)\) in the image.

\( ds = \) circular arc.

\( 2\pi r = \) used to normalize the integral.

\( G(r) = \) Gaussian filter used as a smoothing function.

\(* = \) convolution operation.

Computation of the integral is done over a parabolic instead of a circular arc by excluding the regions detected for the eyelids from the iris image. The integro-differential can be specified as the variation of the Hough transform but fails where there is noise (reflections) in the eye image as it works only on a local scale.

● **Active Contour Models**

Ritter (1999) has utilized active contour models for the localising of the pupil in eye images where pre-set internal and external forces are responded by active contours by deforming internally or moving across an image until the equilibrium is reached. A number of vertices are contained by the contour whose positions are changed by two opposing forces, an internal force which is dependent on the desired characteristics, and an external force that is dependent on the image. Each vertex is moved between time \(t\) and \(t + 1\) specified by the equation:

\[
v_i(t+1) = v_i(t) + F_i(t) + G_i(t) \quad -- (3.4)
\]
where:
\( F_i \) = internal force.
\( G_i \) = external force.
\( v_i \) = position of vertex \( i \).

The internal forces are calibrated for the localisation of the pupil region so that the contour forms a globally expanding discrete circle and the external forces are usually found using the edge information. For accuracy improvement Ritter (1999) has utilized the variance rather than the edge image. A Discrete Circular Active Contour (DCAC) is created by locating a point which is interior to the pupil from a variance image. Then DCAC is moved under the influence of internal and external forces after equilibrium is reached, and the pupil is localised.

**Eyelash and Noise Detection**

Kong and Zhang (2001) have presented a method for eyelash detection. Two types of eyelashes are treated i.e. separable eyelashes which are isolated in the image and multiple eyelashes, which are bunched together and overlap in the eye image. Eyelashes that are separable are detected using One Dimensional (1D) Gabor filters as the convolution of a separable eyelash with the Gaussian smoothing function results in a low output value. If resultant point \(<\) than a threshold, the point belongs to an eyelash and multiple eyelashes are detected utilising the variance of intensity. If the variance of intensity values in a small window \(<\) than a threshold, the eyelash is specified by centre of the window point. A connective criterion is utilized by Kong and Zhang (2001) model connecting each point in an eyelash to another point in an eyelash or to an eyelid. During thresh-holding, specular reflections along the eye image are detected as the intensity values at these regions will be higher than any other regions in the image.

### 3.3.2 Normalization

Daugman (2002) has described that after segmentation of the iris region successfully next is the transformation of this region, so that it has fixed dimensions to allow comparisons. Due to the pupil dilation, varying levels of illumination and dimensional inconsistencies occur between eye images, mainly due to the stretching of the iris caused by pupil dilation from varying levels of illumination. Various other types of inconsistencies like varying imaging distance, rotation of the camera, head tilt, and rotation of the eye within the eye socket also
occur. Iris regions having same constant dimensions produced by normalization process, so two photographs of the same iris specified with different conditions will have characteristic features at the same spatial location. As the pupil region is not always concentric within the iris region and is usually slightly nasal, care must be taken when trying to normalize the ‘doughnut’ shaped iris region to have a constant radius. Various methods are available in literature for performing normalization of iris images which are discussed below.

● Daugman’s Rubber Sheet Model

Sanderson and Erbetta (2000) have illustrated the homogenous rubber sheet model devised by Daugman that remaps each point within the iris region to a pair of polar coordinates (r,0) as enumerated in figure 3.6 where, r is on the interval [0,1] and 0 is angle [0,2\pi].

![](image)

**Figure.3.6 Daugman’s Rubber Sheet Model**

Iris region’s remapping of the (x, y) Cartesian coordinates to the normalized non-concentric polar representation is modelled as:

\[
I(x(r, \theta), y(r, \theta)) \rightarrow I(r, \theta)
\]  -- (3.5)

with

\[
x(r,\theta) = (1-r)x_p(\theta) + rx_l(\theta)
\]  -- (3.6)

\[
y(r,\theta) = (1-r)y_p(\theta) + ry_l(\theta)
\]  -- (3.7)

where:

I(x, y) = iris region image.

(x, y) = original Cartesian coordinates.

(r, \theta) = corresponding normalized polar coordinates.

x_p, y_p and x_l, y_l = coordinates of the pupil and iris boundaries along the \( \theta \) direction.

Pupil dilation and size inconsistencies are taken into account by the rubber sheet model to produce a normalized representation with constant dimensions. Hence, modelling the iris
region as a flexible rubber sheet is anchored at the boundary with the reference point specified as the pupil centre.

**Image Registration**

An image registration technique is employed by Wildes et al. (1994) that geometrically wraps a newly acquired image \((I_a(x, y))\), into an alignment with a selected database image \((I_d(x, y))\). A mapping function \((u(x,y),v(x,y))\) that transforms the original coordinates in the image intensity values of the new image is made to be close to those of corresponding points in the reference image. Choosing of the mapping function should be done so as to minimise the equation below:

\[
\int \int (I_d(x,y) - I_a(x-u,y-v))^2 \, dx\,dy
\]  
-- (3.8)

While being constrained similarity transformation of image coordinates \((x, y)\) to \((x', y')\) is captured through equation below:

\[
\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} - S R(\theta) \begin{pmatrix} x \\ y \end{pmatrix}
\]  
-- (3.9)

where:

\( S = \) scaling factor.

\( R(\theta) = \) matrix representing rotation by \( \theta \).

**Histogram Equalization**

Histogram information reveals that the iris image is under-exposed or over exposed.

![Histogram Equalization](https://www.google.co.in/search?q=http://en.wikipedia.org/wiki/Inverse_transform_sampling)

**Figure 3.7 Histogram Equalization**

It finds a map \( f(x) \) such that the histogram of the modified (equalized) iris image is flat (uniform). The cumulative probability function (cdf) of a random variable approximates a uniform distribution as shown in figure 3.7. Histogram equalization method when compared with other methods of normalization enhances the contrast of iris images by transforming the values in an intensity image so that the histogram of the output iris image approximately matches a specified histogram. This method usually increases the global contrast of iris images, especially when the usable data of the image is represented by close contrast values. By performing this adjustment, the intensities can be better distributed on the histogram allowing areas of lower local contrast to gain a higher contrast. Histogram equalization accomplishes this task by effectively spreading out the most frequent intensity values.

- **Virtual Circles**

  According to Boles (1998), iris images are first scaled to have constant diameter so that on comparison of the two images, one is considered as the reference image. When the two irises achieve the same dimensions, extraction of features from the iris region is done by storing the intensity values along virtual concentric circles with origin at the centre of the pupil. To get the same number of data points extracted from each iris, normalization resolution is selected, making the technique essentially similar as the Daugman’s rubber sheet model. However, scaling is done at match time and nothing is mentioned regarding how to obtain rotational invariance.

### 3.3.3 Feature Encoding and Matching

Calderbank et al. (1998); Daubechies and Sweldens (1998); Sweldens (1997); Sweldens (1995); have focussed that for accurate recognition of individuals, extraction of the most discriminating information must take place from an iris pattern being normalized. Encoding must be done of only the significant features of the iris so that comparisons between templates can be made. For creation of a biometric template most of the iris recognition systems make use of band pass decomposition of the iris image. A corresponding matching metric is required after template is generated in the feature encoding for providing a measure of similarity between two iris templates. The metric should provide intra class comparisons to specify one range of values when comparing the templates generated from the same eye and inter class comparison when comparing another range of values when templates are created from different irises, providing distinct and separate values so that a decision can be made
with high confidence whether two templates are from the same iris or from two different irises. A number of methods are available in literature for performing feature encoding, which are discussed below.

**Wavelet Encoding**

Wavelets can be used to decompose the data in the iris region into components that appear at different resolutions. Wavelets can be utilized as they have the advantage over traditional Fourier transform. Fourier transformation method allows matching of the features that occur at same position by localising the feature data which does not provide a compact resolution of the image. Therefore, in wavelet based encoding methods a number of filters referred as bank of wavelets are applied to the Two Dimensional (2D) iris region, one for each resolution of each wavelet (scaled version of some basis function). The output of applying the wavelets is then encoded for providing a compact and discriminating representation of the iris pattern.

**Gabor Filters**

For providing an optimum conjoint representation of a signal in space and spatial frequency, Gabor filters are utilized which are constructed by modulating a sine/cosine wave with a Gaussian function to provide the optimum conjoint localisation in both space and frequency. A sine wave is perfectly localised in frequency but not localised in space. Quadrature pairs of Gabor filters provide decomposition of a signal with real part (a cosine modulated by a Gaussian) and an imaginary part (a sine modulated by a Gaussian) which are also referred as even symmetric and odd symmetric components respectively. The frequency of sine/cosine wave of the filter specifies the centre frequency of the filter and the bandwidth is specified by the width of the Gaussian. 2D Gabor filters are utilized by Daugman (2002) for encoding iris data pattern represented over an image domain \((x, y)\) as:

\[
f(i, j) = \frac{1}{2\pi \lambda' \gamma} \exp\left[-\frac{1}{2}\left(\frac{i'^2}{\lambda^2} + \frac{j'^2}{\gamma^2}\right)\right] \cos(2\pi F_u i')
\]

where:

\[
i' = \cos(\theta_v) + j\sin(\theta_v)
\]

\[
j' = -\sin(\theta_v) + j\cos(\theta_v)
\]

\(F_u = \) frequency of the sinusoidal plane wave.

\(\theta_v = \) orientation of Gabor filter.
\( \lambda \) and \( \gamma \) = standard deviations of Gaussian envelope along \( x \) and \( y \) directions respectively referred as scales.

**Log-Gabor Filters**

As enumerated by Struc et al. (2009), to overcome disadvantage of the gabor filter (even symmetric filter will have a DC component (mean value of the waveform) whenever the bandwidth is larger than one octave), log gabor filter is utilized where zero DC component can be obtained for any bandwidth by using a gabor filter which is Gaussian on a logarithmic scale whose frequency response is given as:

\[
G(f) = \exp \left( \frac{-\left(\log\left(\frac{f}{f_0}\right)\right)^2}{2\left(\log\left(\frac{\sigma}{f_0}\right)\right)^2} \right) \tag{3.11}
\]

where:

\( f_0 \) = centre frequency.
\( \sigma \) = bandwidth of the filter.

**Zero-crossings of the 1D wavelet**

Boles and Boashash (1998) have utilized one dimensional wavelet for encoding iris data pattern. The mother wavelet is defined as the second derivative of a smoothing function \( \theta(x) \).

\[
\varphi(x) = \frac{d^2 \theta(x)}{dx^2} \tag{3.12}
\]

The wavelet transform of a signal \( f(x) \) at scale \( s \) and position \( x \) is given by:

\[
Wsf(x) = f \ast \left( S^2 \frac{d^2 \theta(sx)}{dx^2} \right)(x) = S^2 \frac{d^2}{dx^2} (f \ast \theta_s)(x) \tag{3.13}
\]

where:

\( \theta_s = (1/S) \theta(x/s) \).
\( Wsf(x) \) = proportional to the second derivative of \( f(x) \) smoothed by \( \theta_s(x) \).
\( f \ast \theta_s(x) = \text{zero crossings of the transform that correspond to points of inflection region.} \)

**Haar Wavelet**

Lim et al. (2001) utilized Haar wavelet referred as the mother wavelet that computes a feature vector with 87 dimensions from multi-dimensional filtering. Each dimension has a real value ranging from -1.0 to +1.0. The feature vector is sign quantised so that any positive value is represented by 1 and negative value as 0. This results in a compact biometric template.
consisting of only 87 bits. Lim et al. (2001) by comparison showed that the recognition rate of Haar wavelet transform is slightly better than Gabor transform by 0.9%.

- **Laplacian of Gaussian Filters**

Wildes et al. (1994) developed a system that decomposes the iris region by application of Laplacian Gaussian filters:

\[ \nabla G = \frac{1}{\pi \sigma^4} \left(1 - \frac{\rho^2}{2\sigma^2}\right) e^{-\rho^2/2\sigma^2} \quad -- (3.14) \]

where:

\( \sigma = \) It is the standard deviation of the Gaussian function

\( \rho = \) It is the radial distance of a point from the centre of the filter.

**A number of matching algorithms available in literature are discussed below.**

- **Hamming Distance (HD)**

It provides a measure of how many bits are same between two bit patterns. Using the Hamming distance of two bit patterns, a decision can be drawn whether the patterns are generated from different or from the same irises. In comparing the bit patterns X and Y, Hamming Distance (HD) is defined as the sum of disagreeing bits (sum of the exclusive-OR between X and Y) over N (the total number of bits in the bit pattern) represented as:

\[ HD = \frac{1}{N} \sum_{j=1}^{N} X_j \text{XOR} Y_j \quad -- (3.15) \]

An individual iris region contains features having high degrees of freedom. Each iris region produces a bit-pattern that is totally independent to that produced by another iris. Two iris codes are produced from the same irises that are highly correlated. When two bits patterns are completely independent, an iris template is generated from different irises, having HD between the two patterns = 0.5. As independence implies that the two bit patterns will be totally random there is 0.5 chance of setting any bit to 1 and vice versa. If the bit pattern of half of the bits agree and half disagree the two patterns will be derived from the same iris hence, HD between them will be close to 0.0, as they are highly correlated and the bits should agree between the two iris codes. Daugman (2002) employed HD as the matching metric for calculation of the distance only with bits that are generated from the actual iris region.
- **Weighted Euclidean Distance (WED)**

WED is utilized for comparing the two templates, especially if the template is composed of integer values. Zhu et al. (2000) discuss how WED provides a measure of similar collection of values between two templates, given by equation below:

\[
\text{WED} (K) = i = \sum_{i=1}^{N} \frac{(f_i - f_i^{(k)})^2}{(\delta_i^{(k)})^2}
\]  

-- (3.16)

where:

- \(f_i\) = \(i^{th}\) feature of the unknown iris.
- \(f_i^{(k)}\) = \(i^{th}\) feature of iris template \(k\).
- \(\delta_i^{(k)}\) = standard deviation of the \(i^{th}\) feature of iris template \(k\).

- **Normalized Correlation (NC)**

Wildes et al. (1994) has utilized Normalized Correlation (NC) betwixt the acquired and database representation for goodness of match which is represented as:

\[
\sum_{i=1}^{n} \sum_{j=1}^{m} \frac{(P1[i,j]-\mu1)(P2[i,j]-\mu2)}{nm\sigma1\sigma2}
\]  

-- (3.17)

where:

- \(P1\) and \(P2\) = two images of size \(n, m\).
- \(\mu1\) and \(\sigma1\) = mean and standard deviation of \(P1\).
- \(\mu2\) and \(\sigma2\) = mean and standard deviation of \(P2\).

Normalized correlation is advantageous over standard correlation as it is able to account for local variations in image intensity that corrupts the standard correlation calculation.

### 3.4 THE PROPOSED NEOTRIC IRIS PERCEPTION APPROACH

The proposed neotropic “crypt-iris based perception and authentication approach” has been implemented in MATLAB to provide enhanced security solutions for MANET through biometrics and elliptic curve cryptography. It undergoes the various steps namely: Segmentation (Iris Segmentation/ Disjuncture), Normalization, Encoding (Template Formation or Encoding), Matching and Authentication. The basic operations of the proposed neotropic “crypt-iris based perception and authentication approach” is specified in figure 3.8 (a) (b) with their description and simulation results described in subsequent subsections.
Figure 3.8 (a) Basic Operations of Neotric Crypt-Iris Based Perception and Authentication Approach
3.4.1 Iris Segmentation/ Disjuncture

A circular Hough transform is explored for detecting the iris and pupil boundaries which involves canny edge detection to generate an edge map. Gradients are biased in the vertical direction for the outer iris/sclera boundary. Vertical and horizontal gradients are weighted equally for the inner iris/pupil boundary. A modified version of canny edge detection MATLAB® function is implemented which allows weighting of the gradients.

The following function is developed in MATLAB for performing iris disjuncture process through Hough transform with canny edge detection:

```matlab
function [x_in,y_in,radi_in,x_out,y_out,radi_out,size_reduction] = fun_iris_extraction(img,fig_show)
rows = size(img,1);
size_reduction = rows/150;
```
re_size_img = imresize(img,1/size_reduction);
[row1,col1] = size(re_size_img);
row_lim = row1*0.1;
col_lim = col1*0.1;
edge_img = edge(re_size_img,'canny');
i = 0;
for radis = 100:-1:10
    i = i + 1;
    [y0,x0,accu] = houghc(edge_img,radis,4,3)
    " [y0detect,x0detect,Accumulator] = houghcircle(Imbinary,r,thresh,region)"
where:
Imbinary - a binary image pixels that have value equal to 1 are interested pixels for HOUGHLINE function.
r - radius of circle
thresh - a threshold value that determines the minimum number of pixels that belong to a circle in image space, threshold must bigger than or equal to 4(default).
region - a rectangular region to search for circle centers within[x,y,w,h] (not be larger than the image area, Default is image area)
y0detect - row coordinates of detected circles.
x0detect - column coordinates of detected circles.
Accumulator - the accumulator array in Hough space.
Canny= Canny edge detection MATLAB® function

Depending on the database utilized radius values are set, like for the CASIA database iris radius range from 90 to 150 pixels while the pupil radius ranges from 28 to 75 pixels. For making the detection of circle process more efficient and accurate, the Hough transform for the iris/sclera boundary is performed first, followed by the Hough transform for the iris/pupil boundary within the iris region instead of performing the transformation for the whole eye region, as the pupil is always within the iris region. With the completion of the process radius and x, y centre coordinates for both circles are stored. The linear Hough transform is utilized for isolating the eyelids by first fitting a line to the upper and lower eyelid. Figure 3.9 shows the flowchart of proposed Hough transform algorithm. Then next another horizontal line is drawn intersecting the first line at the iris edge which is closest to the pupil that allows maximum isolation of eyelid regions. An edge map is created by canny edge detection utilizing only horizontal gradient information. The function developed in MATLAB for performing the linear Hough transform specifies that, if the maximum Hough space < a set threshold, no line is fitted as it corresponds to non-occluding eyelid and the lines are restricted to lie exterior to the pupil region and interior to the iris region. Linear Hough
transform is considered more advantageous over its counterpart which is the parabolic version, as it has less parameter to deduce resulting in computationally less demanding process.

The results of segmentation carried out using Hough transform utilizing canny edge detection proved to be successful providing accuracy of 100%. All the images specified from standardised database (CASIA or LEI) were segmented quite efficiently with the proposed algorithm providing discrete and clear inputs for the normalization state. As normalization process needs inputs i.e. area of interest selected in the segmentation stage and if segmentation not done properly will affect the other stages and will not lead to the development of an efficient iris perception approach. Accuracy and efficiency of the proposed methodology developed in this research study provides an enhanced security solution for MANET which depends on the fact that each stage of the recognition process is

---

**Figure 3.9 Flowchart of Hough Transform**

The results of segmentation carried out using Hough transform utilizing canny edge detection proved to be successful providing accuracy of 100%. All the images specified from standardised database (CASIA or LEI) were segmented quite efficiently with the proposed algorithm providing discrete and clear inputs for the normalization state. As normalization process needs inputs i.e. area of interest selected in the segmentation stage and if segmentation not done properly will affect the other stages and will not lead to the development of an efficient iris perception approach. Accuracy and efficiency of the proposed methodology developed in this research study provides an enhanced security solution for MANET which depends on the fact that each stage of the recognition process is
accurately carried out that will further result in successful authentication. Fig 3.10 depicts 3 iris images of same eye (with specular reflections) and their segmentation results.

Figure 3.10 Three Iris Images Segmented through Hough Transform Depicting Areas of Interest
The images belonging to class 6 of the database of the proposed methodology are selected and segmentation is performed on them through Hough transform and canny edge detection methods. The proposed methodology successfully carries out iris segmentation of all the images specified in the database, extracting the area of interest from the iris image and removing all the unwanted parts from it, resulting in an accurate input for the next stage of iris perception approach.

3.4.2 Normalization

Normalization is performed through histogram equalization method. When compared with the other methods of performing normalization available in literature, histogram equalization enhances the contrast of iris images by transforming the values in an intensity image so that the histogram of the output iris image approximately matches a specified histogram. Figure 3.11 shows normalization and feature encoding process. This method usually increases the global contrast of iris images, especially when the usable data of the image is represented by close contrast values. By performing this adjustment the intensities can be better distributed on the histogram allowing areas of lower local contrast to gain a higher contrast. Histogram equalization accomplishes this task by effectively spreading out the most frequent intensity values.

![Figure 3.11 Normalization and Feature Encoding](image-url)
To evaluate histogram equalization for iris images, let \( f \) be a given iris image represented as \( m \times n \) matrix of integer pixel intensities ranging from 0 to \( L - 1 \) where \( L \) is the number of possible intensity values, often 256. Let \( p \) denote the normalized histogram of \( f \) and \( p_n = \frac{\text{number of pixels with intensity } n}{\text{total number of pixels}} \) and \( n = 0, 1, \ldots, L - 1 \). The histogram equalized iris image \( g \) will be defined by:

\[
g_{ij} = \text{floor}((L - 1) \sum_{n=0}^{L-1} p_n)
\]

where, floor() rounds down to the nearest integer. This is equivalent to transforming the pixel intensities, \( k \) of \( f \) by the function:

\[
T(k) = \text{floor}((L - 1) \sum_{n=0}^{k} p_n)
\]

The motivation for this transformation is the assumption of the intensities of \( f \) and \( g \) as continuous random variables \( X, Y \) on \([0, L - 1]\) with \( Y \) defined by:

\[
Y = T(X) = (L - 1) \int_{0}^{X} p_X(x) dx
\]

where:

\( p_X = \) probability density function of \( f \).
\( T = \) cumulative distributive function of \( X \) multiplied by \((L - 1)\).

The following function is developed in MATLAB for performing normalization process through histogram equalization for the proposed methodology:

```matlab
function [data_stream, mask_stream, norm_ract_iris] = fun_create_pal(img_path, fig_show)

img_rgb = imread(img_path);
img = rgb2gray(img_rgb);
norm_img = fun_pre_processing(img);
[x_in, y_in, radi_in, x_out, y_out, radi_out, size_reduction] = fun_iris_extraction(img, fig_show);
ract_iris = circle_to_strip([x_in*size_reduction, y_in*size_reduction, radi_in*size_reduction, radi_out*size_reduction, norm_img]);
ract_iris_1 = ract_iris';
resize_ract_iris = imresize(ract_iris_1, [20 200]);
norm_ract_iris = fun_pre_processing(resize_ract_iris);
[data_stream, mask_stream] = fun_bin_stream(norm_ract_iris);

if fig_show == 1
    figure;
    colormap(gray);
    subplot(1,2,1);
    imagesc((ract_iris_1));
    title 'Iris Template'
end
```

```
Figure 3.12 Normalization of Iris Images
When compared with other conventional iris recognition algorithms, proposed normalization process is able to perfectly reconstruct the same pattern from images with varying amounts of pupil dilation, as deformation of the iris results in small changes of its surface patterns. Even in the images where pupil is smaller, the proposed normalization process is able to rescale the iris region to achieve constant dimension. The proposed methodology generates the rectangular representation from 10,000 data points in each iris region taking into account all the rotational inconsistencies (misalignment in the horizontal (angular) direction). Rotational inconsistencies will be accounted in the matching stage. The output of the previous segmentation stage where area of interest was selected by a perfect Hough transform and canny edge detection provided the input for the normalization stage. Normalization if not perfectly done will lead to an inappropriate matching, that will not build a perfect security solution for MANET which is the key requirement of this research study. Figure 3.12 depicts three iris images from class 6 which have been segmented (Section 3.4.1, Figure 3.10) with their perfect normalization performed, that further becomes the input template for next stage.

### 3.4.3 Template Formation or Encoding

Template formation or encoding in the proposed methodology is performed through convolving the normalized iris pattern with bi-orthogonal wavelets 3.5. The 2D normalized pattern is broken up into 1D-signals. The angular direction is taken rather than the radial which corresponds to columns of the normalized pattern, as the maximum independence occurs in the angular direction. Transformation of the segmented iris information into a normalized iris data is done using the bi-orthogonal tap. In the proposed method rather than utilizing the traditional Multi-Resolution Analysis (MRA) scheme, a novel lifting technique is explored for the construction of bi-orthogonal filters. The main advantage of this scheme over the classical construction methods is that it does not rely on the Fourier transform and results in faster implementation of wavelet transform. Figure 3.13 depicts the basic concept of lifting scheme that starts with a trivial wavelet referred as the "Lazy wavelet", which has the formal properties of basic wavelet but is not capable of performing the analysis. A new wavelet having improved properties is gradually developed by adding a new basis function which is the main inspiration behind the name of the scheme. The lifting scheme can be visualized as an extension of the Finite Impulse Response (FIR) schemes where for any two-channel, FIR sub band transform can be factored into a finite sequence of lifting steps making the implementation of these lifting steps faster and efficient.
Figure.3.13 Lifting Scheme for Bi-orthogonal Wavelets

Figure.3.14 Bi-orthogonal Wavelet 3.5 and its Related Coefficients

The bi-orthogonal filter family is shown in figure 3.14. Bi-orthogonal 3.5 tap is selected for encoding the iris information by adjusting the frequency content of the resulting coefficients to get a separated band structure. In the lifting scheme the filters are designed using the lifting
steps as they are completely invertible. Transformation of the data into a different and new basis is performed by the filters, where large coefficients correspond to relevant image data and small coefficients corresponds to the noise. Thresh-holding is performed once again and referred as image de-noising. The data encoded by the wavelet is scalable and localized, making matching possible of the features at same location using various scales resulting in information of bit-stream of 1s and 0s referred as the "iris template". For performing comparison band pass Gabor pre-filtering is performed for encoding the information and generating the filter using Gaussian filters. Then utilizing this approximation for generating wavelet coefficients that are quadrature quantized, resulting in information of bit-stream of 1s and 0s. This is performed for all the iris images and the formulated bit-pattern is referred as the 'iris template’ having angular resolution of 20, radial resolution of 200 and length as 8000 bits. The noisy parts of the image are located by the mask template that is formed along with the iris template.

For performing wavelet analysis in this particular study, the digital iris images are encoded using wavelets to formulate the iris template. The intensity values at known noise areas in the normalized pattern are set to the average intensity of surrounding pixels to prevent influence of noise in the output of the filtering. Phase quantisation at the output of filtering is then done to four levels, where two bits of data for each phasor are produced then the output of phase quantisation is chosen to be a grey code, so that when going from one quadrant to another, only 1 bit changes hence, minimising the number of bits disagreeing. Algorithm below describes bi-orthogonal wavelet based encoding using lifting scheme.

```matlab
function [data_stream,mask_stream] = fun_bin_stream(ract_iris)
  ract_iris = double(ract_iris);
  els = {'p',[0.125 0.125],0};
  lsbiorInt = liftwave('bior3.5');
  lsnnewInt = addlift(lsbiorInt,els);
  [CA,CH,CV,CD] = lwt2(ract_iris,lsnewInt);
  [THR,SORH,KEEPAPP] = ddencmp('den','wv',ract_iris);
  C = [CA CH; CV CD];
  C1 = abs(C);
  C_data = (C1 >= THR).*C;
  max_val = max(C_data(:));
  min_val = min(C_data(:));
  C_data_norm = (C_data - min_val)/(max_val - min_val);
  C_data_quant = round(C_data_norm*3);
  rep = [0 0;0 1;1 0;1 1];
```
for i = 1:size(C_data_quant,1)
    for j = 1:size(C_data_quant,2)
        C_data_quant_new(i,2*(j-1)+1:2*j) = rep(C_data_quant(i,j)+1,:);
    end
end
C_noise = (C1 < THR).*C;
max_val = max(C_noise(:));
min_val = min(C_noise(:));
C_noise_norm = (C_noise - min_val)/(max_val - min_val);
C_noise_quant = round(C_noise_norm*3);
for i = 1:size(C_data_quant,1)
    for j = 1:size(C_data_quant,2)
        C_noise_quant_new(i,2*(j-1)+1:2*j) = rep(C_noise_quant(i,j)+1,:);
    end
end
data_stream = C_data_quant_new(:);
mask_stream = C_noise_quant_new(:);
end

Iris templates generated after encoding process are shown in figure 3.15. Bitwise iris templates contain number of bits of information. The total number of bits in the template = 2 * the angular resolution times the radial resolution * number of filters utilized.

![Figure 3.15 (a) Iris Image Templates Generated After Encoding Process (b) Code of Iris Template Being Generated](image)

3.4.4 Matching Process

Matching unlike other conventional eye recognition processes is not done by taking only one single matching criterion into consideration but in the proposed methodology matching is performed through two parameters. Hamming distance as well as normalized correlation coefficient is utilized as metrics for recognition since, bit-wise comparisons are necessary.
Noise masking is incorporated by the Hamming distance algorithm so that only significant bits are used in calculating HD. The Hamming distance is calculated using only the bits generated from the true iris region, and thus the modified HD formula is given as:

$$HD = \frac{1}{N-\sum_{k=1}^{N} X_{nk}(OR)Y_{nk}} \sum_{j=1}^{N} X_j (XOR)Y_j (AND)Xn'_j(AND)Yn'_j$$ \hspace{1cm} (3.21)

where:

- $X_j$ and $Y_j$ = two bit-wise templates to compare.
- $Xn'_j$ and $Yn'_j$ = corresponding noise masks for $X_j$ and $Y_j$.
- $N$ = number of bits represented by each template.

Although in theory two iris templates generated from the same iris will have a Hamming distance of 0.0, in conventional methods this has not happened as normalization is not perfect and also there will be some noise that goes undetected, so some variation will be present when comparing two intra-class iris templates. But in this novel approach, normalization is perfectly done also encoding done through bi-orthogonal wavelets providing a bit stream away from noises. Hence, Minimum Hamming Distance=0 and Maximum Normalized Correlation Coefficient=1 both are achieved. For taking into account the rotational inconsistencies the Hamming distance of two templates is calculated, one template is shifted left and right bit-wise. Hamming distance values are calculated from successive shifts i.e. bit-wise shifting in the horizontal direction corresponding to rotation of the original iris region by the angular resolution used. If an angular resolution of 180 is utilized each shift will correspond to a rotation of 2 degrees in the iris region and corrects for misalignments in the normalized iris pattern caused by rotational differences during imaging. The lowest bit is taken from the calculated Hamming distance values corresponding to the best match between two templates. The number of bits moved during each shift = 2* the number of filters used, as each filter will generate two bits of information from one pixel of the normalized region. The actual number of shifts required to normalize rotational inconsistencies is determined by the maximum angle difference between two images of the same eye and one shift is defined as one shift to the left, followed by one shift to the right. The shifting process performed in HD calculation is illustrated in Figure 3.16.
Next matching parameter utilized is the Normalized Correlation (NC) betwixt the acquired and database representation for goodness of match which is represented as:

\[
\sum_{i=1}^{n} \sum_{j=1}^{m} \frac{(P1[i,j]-\mu_1)(P2[i,j]-\mu_2)}{nm\sigma_1\sigma_2} \quad -- \text{(3.22)}
\]

where:
- \(P1\) and \(P2\) = images of size \(n \times m\)
- \(\mu_1\) and \(\sigma_1\) = mean and standard deviation of \(P1\)
- \(\mu_2\) and \(\sigma_2\) = mean and standard deviation of \(P2\).

Normalized correlation is advantageous over standard correlation as it is able to account for local variations in image intensity that corrupts the standard correlation calculation. The proposed iris perception approach is able to achieve ideal value of matching i.e. Maximum Normalized Correlation = 1.

Three iris images (having specular reflections) of class 6 belonging to the database of the proposed methodology are taken and undergone various succesful stages of the neotric iris perception approach. Figure 3.17 depicts that the selected iris image matches with the perfect class 6 achieving ideal value of matching i.e. Minimum Hamming Distance = 0.
Main achievement of the proposed crypt-iris based perception methodology for MANET is taking into account not one but two matching parameters hence, enhancing the proposed approach. Figure 3.18 illustrates that the selected iris image matches with perfect class achieving ideal value of matching i.e. Maximum Normalized Correlation = 1 which is not
achieved by any conventional iris recognition algorithms. Next section focuses on the concept of threshold cryptography and the subsequent subsection utilizes the iris template generated by neotric iris perception approach to produce domains of elliptic curve cryptography for further authentication. Hence, a novel “crypt iris based authentication approach” is developed which further enhances security of the proposed iris perception approach discussed in previous section and subsections through elliptic curve cryptography, resulting in a neotric “crypt-iris based perception and authentication approach”, leading to an enhanced and effective security solution for MANET utilizing traits of both biometric and cryptography which doubly secures MANET.

3.5 THRESHOLD CRYPTOGRAPHY (TC)

Biometric provide number of advantages but some security and privacy apprehensions still can occur; biometric can be genuine but not necessarily private (secret). Eliminating or abolishing biometric is not possible. If once lost, they are exposed permanently and to apprehend humans cross-matching is employed barring their approval. Consequently, impinging the constraints of biometrics as discussed, iris templates generated through proposed neotric iris perception methodology are taken to produce domains of elliptic curve cryptography for enhancing security of MANET. The vulnerability of the devices having constraint resources increases as MANET suffers from various attacks like DOS due to their wireless nature. Hence, for ensuring availability of nodes in MANET implementation of threshold cryptography takes place. The intended receiver receives the actual message without having to compromise any of the security issue like confidentiality, integrity and authentication. Sharing of a key or splitting the message either before or after encryption by multiple individuals is performed by threshold cryptography. Avoidance of just one individual node for performing the job is done by TC with the main objective for sharing the authority in a way such that each individual node in the network performs computation on the secret message without revealing any secret information of its partial message or key.

Threshold cryptography maintains a distributed architecture for a hostile environment by referring certain number of nodes as the threshold which are required for the encryption and decryption of the message, maintaining confidentiality and integrity against various malicious nodes. Verification of correct data sharing is achieved without revealing the secret key. So, in this research thesis threshold cryptography is considered as a perfect solution for securing MANET along-with neotric iris perception approach. In various computer networks where
nodes have large storage capacity and computational power, threshold cryptography elliptic curve in nature is implemented for providing security solutions against various attacks as illustrated by Baek and Zheng (2003).

Lauter (2004) has described elliptic curve cryptography as an approach of public key cryptography based upon the various elliptic curves over finite fields. Being compared with its counterpart (public key cryptography based RSA) elliptic curve cryptography has proved its importance since, it has the ability for providing same security but with smaller key sizes (less storage requirement) and fast rate (computational efficiency) as specified in Table 3.1 and 3.2 respectively. Therefore, it is considered in various applications like smart card encryption etc. Crescenzo et al. (2005); Eodh (2004); Zhou et al. (2002); defined a rule for addition (specifying normal addition properties) of two points on the curve which is one of the critical property of ECC for obtaining a third point on the curve. An abelian group is formed from the points and the addition law.

Table 3.1 Key Sizes in Bits for Equivalent Level of ECC and RSA

<table>
<thead>
<tr>
<th>Symmetric</th>
<th>ECC</th>
<th>DH/RSA/RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>163</td>
<td>1024</td>
</tr>
<tr>
<td>128</td>
<td>283</td>
<td>3072</td>
</tr>
<tr>
<td>192</td>
<td>409</td>
<td>7680</td>
</tr>
<tr>
<td>256</td>
<td>571</td>
<td>15,366</td>
</tr>
</tbody>
</table>

Table 3.2 Sample ECC Exponentiation over GF (P) and RSA Encrypt Decrypt Timings in Millisecond

<table>
<thead>
<tr>
<th></th>
<th>163ECC</th>
<th>192ECC</th>
<th>1024RSAe (public key operation)</th>
<th>1024RSAd (private key operation)</th>
<th>2048 RSA e (public key operation)</th>
<th>2048 RSA d (private key operation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ultra Sparc II 400 MHz</td>
<td>6.1</td>
<td>8.7</td>
<td>1.7</td>
<td>32.1</td>
<td>6.1</td>
<td>205.5</td>
</tr>
<tr>
<td>Strong ARM 200 MHz</td>
<td>22.9</td>
<td>37.7</td>
<td>10.8</td>
<td>188.7</td>
<td>39.1</td>
<td>1273.8</td>
</tr>
</tbody>
</table>

An extra zero point (0) is included for defining addition for any two points which does not satisfy the equation of elliptic curve. 0 is referred as the point of the curve and the number of distinct points on the curve specifies the order of the curve taking into account the zero point.
Multiplication along with addition of two points (KP) is defined where, K is a positive integer and P a point as the sum of K copies of P, where: 2P=P+P. Threshold cryptography is illustrated as; Alice, Bob, Cathy, David ........ agree on an elliptic curve (non secret) and a fixed curve (non secret) and a fixed curve point (non integer secret point F). A_k is chosen as a secret random integer by Alice (as a secret key) and publishes AP (curve point) and A_kF (public key). Same processes are performed by Bob, Cathy and David. Now if Alice wishes to send a message to Bob it simply computes A_kBP and utilizes the secret key for a conventional symmetric block cipher, Data Encryption Standard (DES). B_kAP is computed by Bob as:

\[ B_kAP = B_k \cdot (A_kF) = A_k \cdot (B_kF) = A_kBP \]  

-- (3.23)

Security of the above scheme is analysed on the various assumptions where computation of K is difficult for a given F. Selection of the finite field then takes place having GF(P) as the field with: P= large prime, xy= omitted hence, we get:

\[ y^2 = x^3 + ax^2 + b \]  

-- (3.24)

With GF (2m) as the field, xy term is included to achieve:

\[ y^2 + xy = x^3 + ax^2 + b \]  

-- (3.25)

where:

b^0=0

Hence, a fixed curve is chosen. For a point P on an elliptic curve GF (pm), Lim K \( \rightarrow \infty \), KP\( \rightarrow 0 \) a fixed point is shown.

For some value of b where b>a and ap = bp which leads to cp =0 where, c=b-a, for least value of c. Above statement if true it is referred as the order of the points. The curve and the fixed point are chosen so that the curve order of fixed point F is a large prime number for achieving enhanced security. Also, order of the fixed point satisfies Menezes-Okamoto-Vanstone (MOV) condition for prevention of various possible attacks hence, upgrading security. From the above discussions it can be concluded that for the fixed point F = n bit prime number, the computation of K from KF takes place and F roughly takes 2n^2 operations, enhancing application of elliptic curves.

So it can be illustrated about ECC with point addition as the basic operation, its curves can be distinguished and avoided. Attacks on ECC are based on discrete logarithmic problems which work much slower due to added complexity and methods have been designed to avoid such attacks. Also, number of transistors are cut back with same security level and ECC is faster with short messages. The discussions above conclude the various advantages of ECC over other cryptographic algorithms so the proposed methodology specified in this research
study has utilized ECC for further enhancing security of MANET along with the neotric iris perception approach together resulting in “crypt-iris based perception and authentication approach”.

3.6 IMPLEMENTATION OF NOVEL CRYPT-IRIS BASED AUTHENTICATION APPROACH

The proposed methodology attempts to achieve enhanced security solution utilizing iris templates which are generated from the individual eye image. These iris templates are utilized to generate the domain parameters of the elliptic curve and private keys. Iris as one of the most reliable biometric features is chosen in the proposed methodology due to its unique signature which is unlikely to be produced from another individual eye or even from other eye of the same person. Enhanced security solutions are achieved as only the individual eye produces the iris signature. The system design architecture of ECC together with Iris Perception Approach (IPA) is shown in figure 3.19. Calculation of various domain parameters of ECC along with the private keys which are generated through iris template is shown in figure 3.20. The most enhanced factor of the proposed methodology is that an individual produces a different private key each time during key regeneration.

Figure.3.19 System Design Architecture of ECC with IPA
Iris signature is the main base for generating the domains of ECC and the private key. The following algorithm describes the "crypt-iris based perception and authentication approach.

1. Select image of individual eye from the database.
2. Perform IPA as stated in section 3.5 to obtain iris signature.
3. Iris signature obtained in step 2 is being hashed to generate domains and private key for ECC.
4. Authentication is then performed between two users.

The above algorithm gives an individual a variety of different private keys as each time a new key is regenerated by user hence, enhancing authentication of IPA, which is the chief security goal for MANET. Figure 3.21 shows the basic GUI for ECC embedded with iris perception algorithm. Proposed approach of ECC utilizes iris signature generated by neotric IPA (section 3.5) and produces a strong authentication system for MANET. Simulated through MATLAB the proposed methodology obtains various successful results, as shown in figure 3.22-3.41.

Figure 3.21 depicts the basic two user authentication system (A and B) utilizing iris templates.
for generating domain values of elliptic curve hence, resulting in a strong secure authentication system for MANET.

Figure 3.21 Basic Graphical User Interface (GUI) for “Crypt-Iris Based Perception and Authentication Approach”

Figure 3.22 Selection of Iris Image for A's Authentication
Figure 3.23 Hough Circles Traced for Detecting Area of Interest of A's Iris Image

Figure 3.24 Iris Template Generated and Normalized for A's Authentication
Figure 3.25 Successful A’s Authentication

Figure 3.26 Selection of Iris Image for B’s Authentication
Figure 3.27 Hough Circles for Detecting Area of Interest of B's Iris Image

Figure 3.28 Iris Template Generated and Normalized for B's Authentication
Figure 3.29 Successful B’s Authentication

Figure 3.30 Encryption Parameters of A and B Generated by their Corresponding Iris Templates
Figure 3.31 A Sends its Public Key to B

Figure 3.32 Scatter Plot of Encrypted Data
Figure 3.33 Scatter Plot of Elliptic Group $E_{p}(a, b) = E997(1,-500)$

Figure 3.33 depicts scatter plot of elliptic group $E_{p}(a, b) = E997(1,-500)$, where X-axis and Y-axis represents different values of x and y which are calculated with the help of equation $y^2 = x^3 + ax + b \mod p$. All the points generated by elliptic curve are utilized for mapping purpose. Plain text point’s $p_m$ will be encrypted as cipher text points with the help of the points given in the scatter plot.

Figure 3.34 Scatter Plot of Encrypted Data $E_{997}(1,-500)$
Figure 3.34 represents scatter plot of encrypted data $E_{997}(1,-500)$ where all points are encrypted with help of receiver's (A's) public key.

Figure 3.35 Message Being Encrypted

Figure 3.36 Authentication with Iris Image at Receiver End
Figure 3.37 Authentication at Receiver End with Hough Circles Being Traced

Figure 3.38 Authentication at Receiver End with Generation of Scatter Plot
Figure 3.39 Authentication Successful

Figure 3.40 Message Being Decrypted
Figure 3.41 Authentication Failed

Figure 3.41 depicts an authentication failure if user tries to access another image than the one utilized for encryption purpose, which justifies the strong authenticated approach of the proposed methodology. The various results obtained in the sections above of neotric "crypt-iris based perception and authentication approach" are summarized below.

3.7 ANALYSIS OF RESULTS

The implementation of the neotric "crypt-iris based perception and authentication approach" is performed in the previous sections and subsections. All the results are analysed and listed below:

• First step of iris perception algorithm is segmentation and accurate segmentation is necessary as without it, data can be falsely represented in an iris pattern that will cause corruption of the biometric templates generated hence, resulting in poor recognition rates. Number of algorithms exists for performing iris disjuncture but in this research study Hough transform is utilized for successful disjuncture of areas of interest from iris image. Hough transform makes circle localisation more accurate and more efficient as there are less edge points to cast votes in the Hough space as compared with other conventional iris segmentation approaches.
When compared with previous iris recognition algorithms, normalization process in this approach is able to perfectly reconstruct the same pattern from images with varying amounts of pupil dilation, as deformation of the iris results in small changes of its surface patterns. Even in the images where pupil is smaller the proposed normalization process is able to rescale the iris region to achieve constant dimension. Normalization if not perfectly done will lead to an in-appropriate matching, that will not result in a perfect security solution for MANET, which is the key requirement of the proposed methodology. Perfect normalization results in the proposed methodology leads to better feature encoding and perfect pattern matching stages.

- Feature encoding is implemented through convolving the normalized iris pattern with Bi-orthogonal wavelets 3.5 by breaking the 2D normalized pattern into a number of 1D-signals. In the proposed method rather than utilizing the traditional Multi-Resolution Analysis (MRA) scheme, a novel lifting technique is explored for the construction of bi-orthogonal filters. The main advantage of this scheme over the classical construction methods is that, it does not rely on the Fourier transform and results in faster implementation of wavelet transform. The feature encoding process produces a bitwise template containing number of bits of information.

- Matching unlike other conventional eye recognition processes is not done by taking one single matching criterion into consideration but in the proposed approach matching is done through two parameters namely Hamming Distance (HD) as well as Normalized Correlation (NC) coefficient since, bit-wise comparisons are necessary. Although in theory two iris templates generated from the same iris will have a Hamming distance of 0.0, in conventional methods this has not occurred. The value of a correlation coefficient ranges between -1 and 1. Greater the absolute value of a correlation coefficient stronger will be the linear relationship. The strongest linear relationship is indicated by a correlation coefficient of -1 or 1. The weakest linear relationship is indicated by a correlation coefficient equal to 0. In this neotric approach normalization is perfectly done also encoding is performed through Bi-orthogonal wavelets providing a bit stream away from noises hence, achieving ideal matching conditions; Minimum Hamming Distance=0 and Maximum Normalized Correlation=1.

- The proposed methodology has unique feature of generating HD and NC even of non iris images and matching them by their specified percentage to the particular databases they slightly match to, that helps in recognising whether the biometric template is correct or not.
Further, a two user authentication system for enhancing security of MANET is developed and implemented involving iris signature to generate domains of ECC and private key, providing two levels of security solutions.

By analyzing the proposed neotric "crypt-iris based perception and authentication approach" through two performance parameters values i.e. minimum hamming distance and maximum normalized correlation helps in achieving various security goals of MANET. Authentication is provided as the nodes whose biometric templates achieves ideal matching conditions; minimum HD=0 and maximum NC=1 find an exact match in the database. Only those nodes will be authorised for data transmission and communication along the network. No node will be able to pretend to be trusted therefore; data transfer will not be affected across the network.

By utilizing iris templates generated through proposed neotric iris perception approach for producing domains of novel "crypt-iris based perception and authentication method", confidentiality is ensured. Sensitive information is accessible only to the intended sender and receiver whose signature will be authenticated by the proposed methodology.

Integrity is also preserved in this approach as only those nodes whose biometric templates that achieve minimum HD=0 and maximum NC=1, will enter the network and no malicious node will be allowed entry in MANET. Hence, no data will be modified by malicious nodes.

As signature of both sender and receiver are authenticated hence, non-repudiation security goal is also preserved. Neither sender nor receiver can deny the transmission of messages.

Occurrence of various active and passive attacks will be limited in MANET being secured by the approach developed in this research study. No malicious node can affect the transmission of various services hence, DOS attack will be limited. No data packets could be updated, modified or altered without signature matching of the intended sender and receiver.

3.8 CONCLUSIONS

Various results have validated notable design and application of a novel "crypt-iris based perception and authentication approach" to protract security in mobile ad-hoc networks. By using bi-orthogonal wavelets, the proposed approach has led to the development of enhanced security solutions for MANET. Matching unlike other conventional eye recognition processes has not been done by taking one single matching criterion into consideration but in the proposed approach matching has been done through two parameters namely Hamming
Distance (HD) as well as Normalized Correlation (NC) coefficient since, bit-wise comparisons are necessary. Although in theory two iris templates generated from the same iris will have a Hamming distance of 0.0 also strongest linear relationship is indicated by a correlation coefficient of -1 or 1, weakest linear relationship is indicated by a correlation coefficient equal to 0, in conventional methods this has not being achieved. In this neotric approach normalization has been perfectly done also encoding is performed through Bi-orthogonal wavelets providing a bit stream away from noises hence, achieving ideal matching conditions; Minimum Hamming Distance=0 and Maximum Normalized Correlation=1. The proposed methodology has unique feature of generating HD and NC even of non iris images and matching them by their specified percentage to the particular databases they slightly match to, that helps in recognising whether the biometric template is correct or not. Further, a two user authentication system for enhancing security of MANET has been developed and implemented involving iris signature to generate domains of ECC and private key, providing two levels of security solutions. By analyzing the proposed neotric "crypt-iris based perception and authentication approach" through two performance parameter values i.e. minimum hamming distance and normalized correlation, various security goals of MANET like authentication, confidentiality, integrity and non-repudiation has been achieved. Also occurrence of various active and passive attacks has been limited in MANET being secured by the proposed approach. No malicious node can affect the transmission of various services hence, DOS attack has been limited. No data packets could be updated, modified or altered without signature matching of the intended sender and receiver.

As routing is highly challenging task for MANET due to high node mobility various routing protocols have been developed where dynamic optimization in routing is utilized for finding paths satisfying some optimality criterion(shortest distance, minimal bandwidth usage and minimum delay) and constraints(limited power and limited capability of wireless links). The second most critical issue for MANET is to find a best fit shortest path between the source and destination and optimization of QOS parameters. Meta-heuristic based genetic approach is exploited to optimize QOS performance of MANET by developing a simulator in MATLAB, taking into consideration various QOS parameters like average packet delivery ratio, average packet drop rate, average end-to-end delay and average hop count. Next chapter discusses the second module of the proposed methodology which is another critical issue for MANET. It deals with optimizing QOS parameters of MANET by providing an effective routing solution through genetic algorithm.