A STUDY ON AUTHENTICATED ADMITTANCE OF ATM CLIENTS USING BIOMETRICS BASED CRYPTOSYSTEM

M. Subha[1] and S. Vanithaasri[2]
[1]Assistant Professor & [2]M.phil Research Scholar,
Department of Computer Science, Vellalar College for Women (Autonomous),
Erode -12, Tamil Nadu, India.

ABSTRACT

The paper proposes highly authenticated biometric security system for the ATM access. The conventional fingerprint static points are applied in the existing works for authentication. The ridge features, minutiae points of fingerprint and iris are considered in the proposed system for increasing the matching scores against the occurrence of distortions and non-linear deformations. Consecutive steps are processed in the proposed system. First, preprocessing steps of the proposed system is done by introducing some appropriate algorithms. Secondly, key points are generated based on the iterative process to traverse for evaluating the costs of each fingerprint (ridge length, ridge direction, ridge curvature, ridge type) and iris (points) simultaneously using the cryptosystem features for identification of valid users from the database. Hence, the authentication is high in the proposed application of ATM access.

KEYWORDS: *Fingerprint matching, minutiae points, iris recognition, key points, cryptosystem.*

I. INTRODUCTION

Biometrics and cryptography play an important role in the field of security. Crypto-biometrics is an emerging architecture where cryptography and biometrics are merged to achieve high level security systems. The advantage that Biometrics presents is that the information is unique for each individual and that it can identify the individual in spite of variations in the time. A blend of these two technologies can produce a high level of security system, known as crypto biometric system that assists the cryptography system to encrypt and decrypt the messages using bio templates. Fingerprint and Iris points are an essential index in the enforcement of security and maintenance of a reliable identification [5]. Fingerprint is currently being used as variables of security during voting, operation of bank account among others. It is also used for controlling access to highly secured places like offices, equipment rooms, control centers and so on. Iris recognition is also a proven, accurate means to identify people. An efficient method for personal identification based on the pattern of human iris. Iris recognition is a method for biometric authentication that uses pattern-recognition techniques based on high-resolution images of the iris of an individual. It will be highly secure and reliable authentication if the fingerprint identification is used in fusion with the Iris recognition [6][11]. In this paper, the fingerprint and iris are considered for providing mutual authentication between the server and the user. At first, the fingerprint features are obtained from the fingerprint image using segmentation, orientation field estimation and morphological operators. Consecutively the texture features are acquired from the iris image by segmentation, estimation of iris boundary and normalization. Minutiae points and iris texture, the two extracted features are then fused at feature level to build the multimodal biometric template.

In this paper, the fingerprint and iris are considered for providing mutual authentication between the server and the user. At first, the fingerprint features are obtained from the fingerprint image using segmentation, orientation field estimation and morphological operators. Fig 1(a). Consecutively the texture features are acquired from the iris image by segmentation, estimation of iris boundary and normalization. The two extracted features of minutiae points and iris textures are then fused at feature level to build the multimodal biometric template. Then the user's fingerprint and iris images are converted and stored as encrypted binary template, which is used for authentication by the server [6]. Thus the user's biometric verification data are first transformed into a strong secret and is then stored in the server's database during registration. During log-in procedure authentication is done both at client side and server side without transmitting the biometric measurement from the user to the server. Further the user and the server communicate with each other with a secret session key that is generated from the biometric for the rest of the transactions.

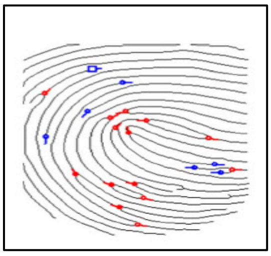
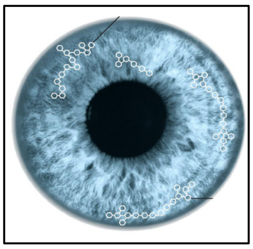


Fig. 1(a). Fingerprint points



1(b). Iris points

II. PROBLEM DEFINITION

Many researchers have been carried out in the field of authentication and Key Exchange protocols, which are based on passwords. The Password based user authentication systems are low cost and easy to use but however, the use of passwords has intrinsic weaknesses. The user chosen passwords are inherently weak since most users choose short and easy to remember passwords [10]. If only fingerprint matching is used then it cannot be reliable one and it has the chances of attacks. If the fingerprint used in fusion with iris recognition, then the chances of knowing the user's account is reduced because of verifying the two biometrics matching scores.

III. PROPOSED SYSTEM

In the proposed work, to provide mutual authentication and key generation in the ATM access, the biometric information from both the fingerprint and iris are considered. The multimodal biometric information is fused for mutual authentication and key generation.

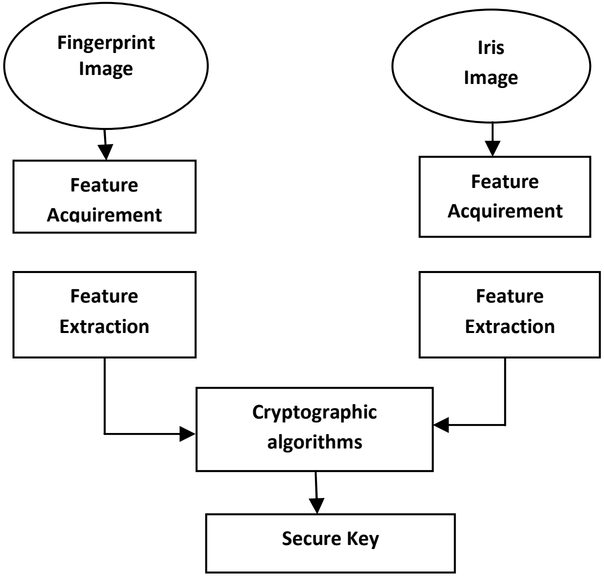


Figure2. The proposed system flow diagram

The use of multimodal biometrics for key generation provides better security, as it is made difficult for an intruder to spool multiple biometric traits simultaneously. This system is a biometric-only system in the sense that it requires no user key cryptosystem and, thus, no Public Key Infrastructure (PKI). This makes the system very attractive considering PKIs are proven to be expensive to deploy in the real world. Moreover, it is suitable for online web applications due to its efficiency in terms of both computation and communication.

3.1. Fingerprint preprocessing

The major Minutia features of fingerprint ridges are: ridge ending, bifurcation and short ridge. The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges which are significantly shorter than the average ridge length on the fingerprint [4].Before extracting the proposed ridge features, we need to perform some preprocessing steps. These steps include typical feature extraction procedures as well as additional procedures for quality estimation and circular variance estimation. We first divide the image into 8x8 pixel blocks. Then, the mean and variance values of each block are calculated to segment the fingerprint regions in the image. We then apply the method described in [1] to estimate the ridge orientation and the ridge frequency is calculated using the method presented in [2]. The Gabor filter [9] is applied to enhance the image and obtain a skeletonized ridge image. Then, the minutiae (end points and bifurcations) are detected in the skeletonized image. The quality estimation procedure is performed in order to avoid extracting false minutiae from poor quality regions and to enhance the confidence level of the extracted minutiae set.

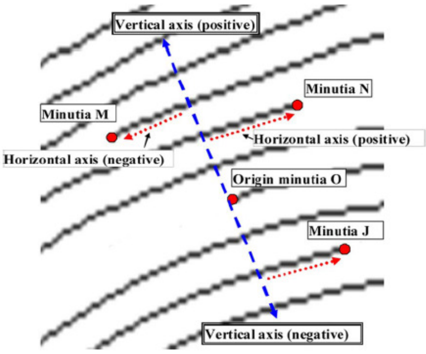


Fig 3. Ridge based co-ordinate system

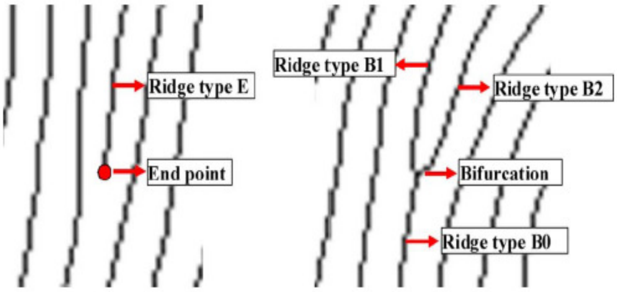


Fig 4. Examples of Ridge Types

3.1.1. Extraction of Minutiae Points:

Minutiae extraction: The process of minutiae point extraction is carried out in the enhanced fingerprint image. The steps involved in the extraction process are Binarization and Morphological Operators. Binarization is the process of converting a grey level image into a binary image. It improves the contrast between the ridges and valleys in a fingerprint image and thereby facilitates the extraction of minutiae. The grey level value of each pixel in the enhanced image is examined in the binarization process. If the grey value is greater than the global threshold, then the pixel value is set to a binary value one; or else, it is set to zero. In minutiae extraction algorithms, there are only two levels: the black pixels that denote ridges, and the white pixels that denote valleys. Morphological operators are applied to the binarized fingerprint image. It eliminates the obstacles and noise from the image. Furthermore, the unnecessary spurs, bridges and line breaks are removed by these operators. The process of removal of redundant pixels till the ridges become one pixel wide is facilitated by ridge thinning. The thinning algorithm to a fingerprint image preserves the connectivity of the ridge structures while forming a skeleton version of the binary image. The ridges are thinned using the appropriate algorithms and the ridge scores are taken based on the ridge end or ridge bifurcation [4]. Thus the cryptographic keys are produced using the extracted points.
The overall procedure for extracting ridge features is as follows:

1) The preprocessing steps are implemented for extracting the skeletonized ridge factors from a fingerprint.
2) The ridge valley structures are traversed along the vertical axis from each minutia origin.
3) When the vertical axis intersects with the ridges attached to a minutia, extract the ridge features and form a ridge feature vector between the origin and the minutia.
4) Keep traversing all the ridges until vertical axis reaches a background region or reaching a poor quality region or reaching a high circular variance region in the fingerprint.
5) If all minutiae are used as the origin minutiae, terminate the procedure. Otherwise return to the step 2.

The termination conditions include the following three cases:

1) The vertical axis reaches a background region in the fingerprint image.
2) The vertical axis reaches a poor quality region in the fingerprint image.
3) The vertical axis reaches a high circular variance region in the fingerprint image.

3.1.2. Fingerprint matching

The procedure for fingerprint matching is as follows:

1. Initially match any pair of ridge-based coordinate systems extracted from the enrolled fingerprint image and the input fingerprint image using dynamic programming.
2. Select the top degree of matched ridge-based coordinate pairs.
3. For every initially matched pair, a breadth-first search (BFS) is performed to detect the matched ridge-based coordinate pairs incrementally.
4. Check the validity of the matched coordinate pairs using the relative position and orientation of the minutiae and count the number of matched minutiae.
5. Repeat the above two steps and then return the maximum number of matched minutiae.
6. Compute the matching score.

Hence, the ridge feature vectors in a ridge based coordinate system are gathered in sequence based on the ridge counts and stored as the elements of an ordered sequence. Then all the enrolled coordinates of ridges are compared sequentially.

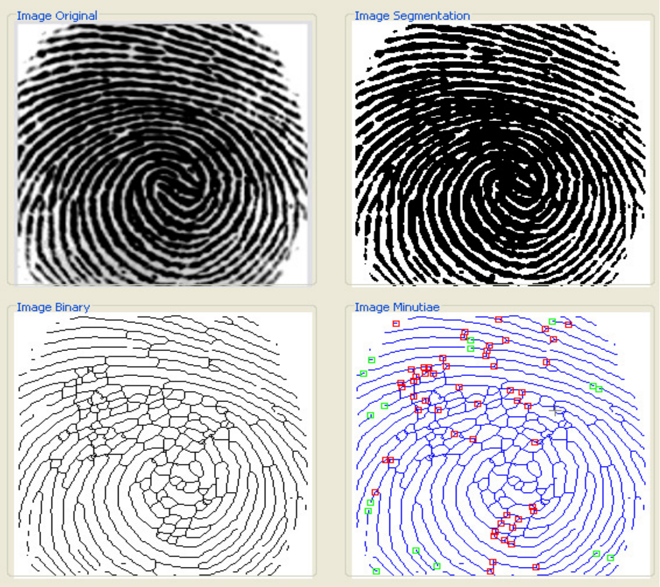


Fig 5. Extraction of Fingerprint minutiae points

3.2. IRIS PREPROCESSING

An annular part between the pupil and the white sclera called the human iris, has an astonishing structure and presents a bounty of interlacing minute characteristics such as freckles, coronas, stripes and more. These perceptible characteristics that are usually called the texture of the iris are unique to every subject [7]. The procedures included in the feature extraction process of the iris image are as follows:

3.2.1. Segmentation: Iris segmentation is a significant module in iris recognition since it defines the effective image region utilized for consequent processing such as feature extraction. The iris image is first fed as input to the canny edge detection algorithm that produces the edge map of the iris image for boundary estimation. The exact boundary of pupil and iris is located from the detected edge map using the Hough transform.

3.2.2. Iris Normalization: When the iris image is proficiently localized, then the subsequent step is to transform it into the rectangular sized fixed image. Daugman's Rubber Sheet Model [8] is utilized for the transformation process.

On polar axes, for each pixel in the iris, its equivalent position is found out. This process consists of two resolutions. They are Radial resolution and Angular resolution. The former is the number of data points in the radial direction whereas, the later part is the number of radial lines produced around iris region. Utilizing the following equation, the iris region is transformed to a 2D array by making use of horizontal dimensions of angular resolution and vertical dimension of radial resolution.

$$I[x(r, \theta), y(r, \theta)] \rightarrow I (r, \theta) \qquad (1)$$

where, I (x, y) is the iris region, (x, y) and (r, θ) are the Cartesian and normalized polar coordinates respectively. The range of θ is $[0\ 2\pi]$ and r is $[0\ 1]$. $x(r, \theta)$ and $y(r, \theta)$ are described as linear combinations set of pupil boundary points.

To perform the transformation, the formulas are given in (2) to (7).

$$x(r, \theta) = (1- r)xp (\theta) + xi (\theta) \qquad (2)$$

$$y(r, \theta) = (1- r)yp (\theta) + yi (\theta) \qquad (3)$$

$$xp (\theta) = xp0(\theta) + rpCos(\theta) \qquad (4)$$

$$yp (\theta) = yp0(\theta) + rpSin(\theta) \qquad (5)$$

$$xi (\theta) = xi0 (\theta) + riCos(\theta) \qquad (6)$$

$$yi (\theta) = yi0 (\theta) + riSin(\theta) \qquad (7)$$

where (xp , yp) and (xi , yi) are the coordinates on the pupil and iris boundaries along the direction. (xp0, yp0), (xi0 , yi0) are the coordinates of pupil and iris centers [12].

3.2.3. Extraction of iris texture*:* The normalized 2D form image is disintegrated up into 1D signal, and these signals are made use to convolve with 1D Gabor wavelets. The frequency response of a Log-Gabor filter is as follows,

$$G(f) = \exp\left(\frac{-(\log(f/f_0))^2}{2(\log(\sigma/f_0))^2}\right) \qquad (8)$$

where $f0$ indicates the centre frequency, and σ provides the bandwidth of the filter. The Log-Gabor filter outputs the biometric feature of the iris.

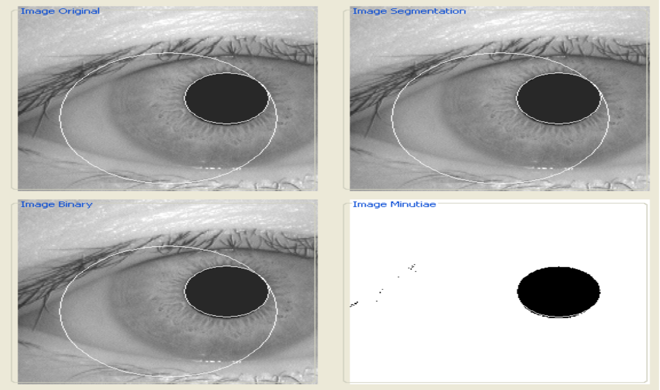


Fig 5. Extraction of Iris features

3.3. Feature Level Fusion of Fingerprint and Iris Features

There are two sets of features used for fusion. They are Fingerprint features and Iris features. The next step is to fuse the two sets of features at the feature level to obtain a multimodal biometric template that can perform biometric authentication. Each minutiae point extracted from a fingerprint is represented as (x, *y*) coordinates. In this we store those extracted minutiae points in two different vectors: Vector F1 contains all the *x* co-ordinate values and Vector F2 contains all the *y* co-ordinate values.

$$F1 = [\ x1\ x2\ x3\ \ldots\ldots xn\ ]\ ;\ |\ F1\ | = n \qquad (9)$$

$$F2 = [\ y1\ y2\ y3\ \ldots\ldots yn\ ]\ ;\ |\ F2\ | = n \qquad (10)$$

The texture properties obtained from the log-gabor filter are complex numbers ($a + ib$). Similar to fingerprint representation, we also store the iris texture features in two different vectors: Vector I1 contains the real part of the complex numbers and Vector I2 contains the imaginary part of the complex numbers.

$$I1 = [\ a1\ a2\ a3\ \ldots\ldots am\ ]\ ;\ |\ I1\ | = m \qquad (11)$$

$$I2 = [\ b1\ b2\ b3\ \ldots\ldots bm\ ]\ ;\ |\ I2\ | = m \qquad (12)$$

Thereby, the input to the fusion process will be four vectors F1, F2, I1, and I2. The fusion process results with the multimodal biometric template.

The steps involved in fusion of biometric feature vectors are as follows.

1) ***Shuffling of individual feature vectors:*** The first step in the fusion process is the shuffling of each of the individual feature vectors F1, F2, I1 *and* I2. The steps involved in the shuffling of vector F1 are,

Step 1: A random vector *R* of size F1 is generated. The random vector *R* is controlled by the seed value.

Step 2: For shuffling the ith component of fingerprint feature vector F1,

a) The ith component of the random vector *R* is multiplied with a large integer value.

b) The product value obtained is modulo operated with the size of the fingerprint feature vector F1.

c) The resultant value is the index say ‘ *j* ’ to be interchanged with. The components in the ith and jth indexes are interchanged.

Step 3: Step (2) is repeated for every component of F1 . The shuffled vector F1 is represented as S1 . The above process is repeated for every other vectors F2, I1 and I2 with S1, S2 and S3 as random vectors respectively, where S2 is shuffled F2 and S3 is shuffled I1 . The shuffling process results with four vectors S1, S2 , S3 and S4 .

2) Concatenation of shuffled feature vectors: The next step is to concatenate the shuffled vectors process S1, S2, S3 and S4. Here, we concatenate the shuffled fingerprints S1 and S2 with the shuffled iris features S3 and S4 respectively. The concatenation of the vectors S1 and S3 is carried out as follows:

Step 1: A vector M1 of size |S1| + |S2| is created and its first |S3| values are filled with S3.

Step 2: For every component S1,

a) The corresponding indexed component of M1 say ‘ t ’is chosen.

b) Logical right shift operation is carried in M1 from index ‘ t ’.

c) The component of S1 is inserted into the emptied tth index of M1 . The aforesaid process is carried out between shuffled vectors S2 and S4 to form vector M2. Thereby, the concatenation process results with two vectors M1 and M2.

3) Merging of the concatenated feature vectors: The last step in generating the multimodal biometric template BT is the merging of two vectors M1 and M2.

The steps involved in the merging process are as follows:

Step 1: For every component of M1 and M2 ,

a) The components M11 and M21 are converted into their binary form.

b) Binary NOR operation is performed between the components M11 and M21 .

c) The resultant binary value is then converted back into decimal form.

Step 2: These decimal values are stored in the vector BT, which serves multimodal biometric template.

IV. FINGERPRINT AND IRIS IMAGE REGISTRATION

The following computations take place at the user side during registration process:
1) The user is asked to give the fingerprint input at least five times and the similar minutia is extracted to form minutia template (FP). Alike from many iris images of the user the similar iris features are extracted to form the iris template (IF). The combined feature template is computed and it is said to be Combined Multimodal Features (CMF).
2) The user then encrypts the minutia template using AES-128 bit symmetric cipher in ECB mode.
3) The user then sends (UID, EAES(CMF)) to the server for storage in its database. Thus the Implementation of multimodal hardening protocol leads to the generation of Strong secret.

V. MULTIMODAL CRYPTOGRAPHIC PROTOCOL

The Algorithm makes the following Assumptions:

1) Let p, q be two large prime numbers such that p = 2q + 1.
2) Let g Î QRp are of order q where QRp is the group of quadratic residues modulo p.
The outline of the multimodal Authentication protocol is given below to enable mutual authentication and key exchange between the User and the Server.
Step 1: To initiate a request for service, user computes MB1= EAES (CMF).
Step 2: The user Computes B1 ≡ gMB1 (mod p). The user sends the user ID along with B1 to the server.
Step 3: Server selects the encrypted minutia template with the user-Id using a table look-up procedure and computes B2 ≡ gMB2 (mod p), where MB2 is the encrypted minutiae template stored at the server side during registration. Then the server compares whether B1 ≡ B2 (mod p). If it holds the server is assured of the authenticity of the user otherwise aborts the authentication protocol. Then the server sends B2 to the user.
Step 4: Upon reception of B2 , User verifies whether B1≡ B2 (mod p). If so authenticated otherwise aborts the authentication protocol.

VI. APPLICATION OF THE PROPOSED SYSTEM

The proposed work is well suited for the authenticated admittance for the ATM clients to make their transactions. The fingerprint and iris features of the client is verified using the proposed cyptosystem and the corresponding client is given with the right to access only when the currently extracted features generate the key points and using the generated key the features are matched with the features stored in the database.

VII. CONCLUSION AND FUTURE WORK

The proposed approach consists of three modules namely, 1) Feature extraction, 2) Multimodal biometric template generation and 3) Cryptographic key generation. Initially, we extracted the minutiae points and texture properties from the fingerprint and iris images respectively. Then, we fused the extracted features at the feature level to obtain the multibiometric template and subsequently generated a 256-bit secure cryptographic key from the multi-biometric template. The advantage that Biometrics presents is that the information is unique for each individual and that it can identify the individual in spite of variations in the time (it does not matter if the first biometric sample was taken year ago).The pillars of e-learning security are: authentication, privacy (data confidentiality) authorization (access control), data integrity and non-repudiation. Biometric is a technique that can provide all this requirements with quite lot reliability. The biometrics can be even more effective and safe method (is very difficult to falsify), if the gait recognition is used in addition with the fingerprint and iris merged cryptosystem.

REFERENCES

[1]. C.Lee, S. Lee, J. Kim, and S. Kim, " Preprocessing of a fingerprint image captured with a mobile camera", in *Proc. IAPR* Int. Conf. Bio-metrics (ICB), Hong Kong, Jan. 2006, pp. 348-355, Springer LNCS-3832.

[2]. D.Maio and D. Maltoni, "Ridge-line density estimation in digital images", in Proc. 14th ICPR, 1998, vol. 1, pp.534-538

[3]. Debnath Bhattacharyya, Poulami Das,Samir Kumar Bandyopadhyay and Tai-hoon Kim, "IRIS Texture Analysis and Feature Extraction for Biometric Pattern Recognition", International Journal of Database Theory and application, vol. 1, no. 1, pp. 53-60, December 2008.

[4]. Heeseung Choi, Kyoungtaek Choi, and Jaihie Kim "Fingerprint Matching Incorporating Ridge Features With Minutiae", IEEE Transactions on Information Forensics and Security, Vol.6, No.2, June 2011.

[5]. Iwasokun Gabriel Babatunde, Akinyokun, Oluwole Charles, Alese Boniface Kayode, Olabode Olatunbosun, "Adaptive and Faster Approach to Fingerprint Minutiae Extraction and Validation", Internstional journal of Computer Science and Security (IJCSS), Vol(5) : Issue (4) : 2011.

[6]. Jagadeesan. A, Dr. K. Duraiswamy, "Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 2, February 2010.

[7]. J. Daugman, "Statistical Richness of Visual Phase Information: Update on Recognizing Persons by Iris Patterns," International Journal of Computer Vision, vol. 45, no. 1, pp. 25-38, 2001.

[8]. John Daugman, "How Iris Recognition Works", in Proceedings of International Conference on Image Processing, vol.1, pp. I-33- I-36, 2002.

[9]. L. Hong, Y. Wan, and A. K. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 20, no. 8, pp. 777–789, Aug. 1998. [10]. M.Bellare, D. Pointcheval, and P.Rogaway, " Authenticated Key Exchange Secure Against Dictionary Attacks", Advances in Cryptology Eurocrypt, 2000 .

[11]. Rajeswari Mukesh, A. Damodaram, V. Subbiah Bharathi, "Finger Print Based Authentication and Key Exchange System Secure Against Dictionary Attack", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, October 2008.

[12]. S. Uma Maheswari, P. Anbalagan and T.Priya, " Efficient Iris Recognition through Improvement in Iris Segmentation Algorithm", International Journal on Graphics, Vision and Image Processing, vol. 8, no.2, pp. 29-35, 2008.

AUTHORS

M.Subha was born on 24-01-1976, she received the B.Sc (Computer science), MCA and M.Phil (computer science) degree from the Bharathiar university, Coimbatore in 1996, 2003, and 2006 respectively. She received the Ph.D (computer science) degree from mother Teresa women's university, kodaikanal in Jan 2012. She is an Assistant Professor in the PG Department of computer Application Vellalar College for women (Autonomous) Erode since 2004. Totally she has ten years teaching experiences. She published four papers in international journals and two papers in national journals. Also she has presented more than twenty papers in the international, national and state level Conference and seminars. Her research interests include Wired and Wireless networks (MANET) with focus on Routing, Security and Intrusion Detection and Image Processing.

S. Vanithaasri received the B.Sc (Computer science) degree in 2009 from Periyar University, Salem and M.Sc (computer science) degree in 2011, respectively from Bharathiar university, Coimbatore. She is currently doing M.Phil (computer science) degree from Bharathiar University, Coimbatore.