Palmprint and Iris based Authentication and Secure Key Exchange against Dictionary Attacks

P.Tamil Selvi
Research Scholar
P.S.G.R. Krishnammal College for women
Bharathiar University, Coimbatore, India

N.Radha
Sr.Lecturer
P.S.G.R. Krishnammal College for women
Bharathiar University, Coimbatore, India

ABSTRACT
The Multimodal Biometric based user authentication systems are highly secured and efficient to use and place total trust on the authentication server where biometric verification data are stored in a central database. Such systems are prone to dictionary attacks initiated at the server side. In this paper, we propose an efficient approach based on multimodal biometrics (Palmprint and Iris) based user authentication and key exchange system. In this system, texture properties are extracted from the palmprint and iris images are stored as encrypted binary template in the server's database, to overcome the dictionary attacks mounted by the server. The image processing techniques are used to extract a biometric measurement from the palmprint and iris. During login procedure the mutual authentication is done between the server and user and a symmetric key is generated on both sides, which could be used for further secure communication between them. Thus meet-in-the middle attack that happens between the user and the server can also be overcome. This system can be directly applied to strengthen existing password or biometric based systems without requiring additional computation.

Keywords: Authentication, Dictionary Attack, Palmprint, Fusion, Iris, Key Exchange, Minutiae points.

1. INTRODUCTION
Reliable authorization and authentication has become an integral part of our life for a number of routine applications. Majority of the authentication systems found today are not very flexible (can be broken or stolen) to attacks, rather it can control access to computer systems or secured locations utilizing passwords. Recently in most application areas, biometrics has emerged practically as a better alternative to conventional identification methods. Biometrics, expressed as the science of identifying an individual on the basis of physiological or behavioral traits, seems to achieve acceptance as a suitable method for obtaining an individual's identity [1]. Some of the biometrics used for authentication is Fingerprint, Iris, Palmprint, Retina, Voice, Hand geometry, Signature, Key stroke etc.

Biometric technologies have established their importance in a variety of security, access control and monitoring applications [2]. Biometric systems that generally employ a single attribute for recognition (unimodal biometric systems) are influenced by some practical issues like noisy sensor data, non-universality and lack of distinctiveness of the biometric trait, unacceptable error rates, and spoof attacks.

Multimodal biometric system employs two or more individual modalities, namely, gait, face, iris and fingerprint, to enhance the recognition accuracy of conventional unimodal methods [3]. The multimodal based authentication can aid the system in improving the security and effectiveness in comparison of unimodal biometric authentication, and it might become challenging for an adversary to spoof the system owing to two individual biometrics traits.

In this paper, the palmprint and iris are considered for providing mutual authentication between the server and the user. At first, the palmprint texture features are obtained from the palmprint image using 2-D Gabor phase coding scheme. Likewise, the texture features are acquired from the iris images by segmentation, estimation of iris boundary and normalization. The extracted texture features the two are then fused at feature level to build the multimodal biometric template. Fusion at the feature level is achieved by means of concatenation, shuffling and merging. Thus the user's palmprint and iris images are converted and stored as encrypted binary template, which is used for authentication by the server. 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 at client 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. This concept can also be applied to strengthen the existing single server password based authentication systems.

2. REVIEW OF RELATED WORKS
A lot of research has been carried out in the field of Authentication and Key Exchange protocols, which are based on passwords [4]. 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. In particular, passwords are normally drawn from a relatively small dictionary; thereby prone to Brute-force dictionary attacks, where an attacker enumerates every possible password in the dictionary to determine the actual password.

These systems are essentially intended to defeat offline dictionary attacks by outside attackers and assume that the server is completely trusted in protecting the user password database. Once an authentication server is compromised, the attackers perform an offline dictionary attacks against the user passwords. To eliminate this single point of vulnerability inherent in the single-server systems, password systems based on multiple servers were proposed. The principle is distributing the password database as the authentication function to multiple servers, so that an attacker is forced to compromise several servers to be successful in offline dictionary attacks.

Recently, Brainard [5] proposed a two-server password system in which one server expose itself to users and the other is hidden from the users. Subsequently, Yang [6] extended and tailored this two server system to the context of federated enterprises, where the back-end server is managed by an

enterprise headquarter and each affiliating organization operates a front-end server.

Instead of traditional password based systems, biometric techniques are used for mutual authentication and key generation by Rajeswari Mukesh [7]. It may influence by some practical issues like noisy sensor data, non-universality and/or lack of distinctiveness of the biometric trait, unacceptable error rates, and spoof attacks.

Zhang and Shu[8] applied the datum point invariant property and the line feature matching technique to conduct the verification process via the palmprint features extracted from the inked paper. Recently, more researchers have been working on inkless palmprint images captured using a special palmprint scanner or a general digital scanner.

Wai-Kin Kong [9] proposed palmprint authentication in which 2-D Gabor filter is used to obtain texture information and two palmprint images are compared in terms of their hamming distance. David Zhang [10] proposed feature-level fusion approach for improving the efficiency of palmprint identification. Multiple Gabor filters are employed to extract the phase information on a palmprint image, which is then merged according to a fusion rule to produce a single feature which is measured by their normalized hamming distance.

The fusion of fingerprint and iris features for cryptographic key generation is proposed by A.Jagadeesan [11]. 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.

3. PROPOSED APPROACH

In the proposed work, the multimodal biometric information is used for mutual authentication and key generation. 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.

4. OVERALL ARICHITECTURE

The overall architecture of the multimodal biometric authentication and key exchange system is shown in Figure 1. The server maintains a database of encrypted template of the user's palmprint and iris. In this setting, users communicate with the server for the purpose of user authentication, by rendering his/her palmprint and iris, which is transformed into a long secret held by the server in its database.

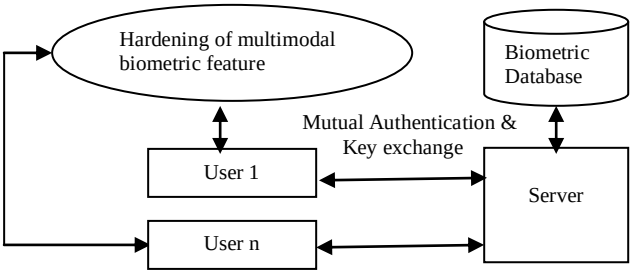

Figure 1. Architecture for multimodal biometric authentication

5. MULTIMODAL BIOMETRICS AUTHENTICATION PROTOCOL

The main part of the protocol design is the defense against offline dictionary attacks by the servers and also to overcome the man-in-the-middle attack done between the user and the server. In any secure system, the user provides his/her palmprint through a palmprint scanner. The palm print image undergoes a series of enhancement steps. Likewise iris image also captured and extracted. This is followed by a multimodal hardening protocol with servers to obtain a hardened palmprint and iris which are stored into a strong secret. Encrypted storage of the texture features of palmprint and iris are done in such a way that they are no longer subjected to offline dictionary attack. During user login, the server uses its encrypted palmprint and iris for user authentication. During authentication, user using palmprint and iris mutually authenticate each other and negotiate a secret session key.

5.1 Features Extraction of Palmprint

The palmprint contain distinctive features such as principal lines, delta points, minutiae, wrinkles, ridge, valley and geometrical features. The geometrical features denote the width of the palm. Delta points and minutiae can be extracted from the fine-resolution images. Principal lines and wrinkles, called palm-lines are very important to discriminate between different palmprints and they can be extracted from low-resolution images. Therefore, palm-lines are one of the most important features in automated palmprint recognition. The palm-lines in a palm are very irregular and even in the same palm they have quite different directions and shapes.

5.1.1 Preprocessing

Before feature extraction, it is necessary to obtain a sub-image from the captured palmprint image and to eliminate the variations caused by rotation and translation. The five main steps of palmprint image preprocessing are as follows:

Step 1: Apply a low-pass filter to the original image. A threshold T_p is used to convert original image into a binary image.

Step 2: Extract the boundaries of the holes (F_ix_j, F_iy_j), (i=1,2) between fingers using a boundary-tracking algorithm. The start points (Sx_i, Sy_i) and end points (Ex_i, Ey_i) of the holes are marked in the process.

Step 3: Compute the tangent of the two gaps. Let (x_1, y_1) and (x_2, y_2) be any points on (F_1x_j, F_1y_j) and (F_2x_j, F_2y_j), respectively. If the line (y=mx+c) passing though these two points satisfies the inequality $F_iy_j = mF_ix_j + c$, for all i and j then the line (y =mx + c) is considered to be the tangent of the two gaps.

Step 4: Line up (x_1, y_1) and (x_2, y_2) to get the Y-axis of the palmprint coordinate system and make a line passing through the midpoint which is perpendicular to the Y-axis, to determine the origin of the coordinate system.

Step 5: Extract a sub-image of a fixed size based on the coordinate system which is located at a certain area of the palmprint image for feature extraction.

5.1.2 Palmprint Features Extraction by Texture Analysis

The texture features of the palmprints are extracted by 2-D Gabor phase coding scheme. The circular Gabor filter is an effective tool for texture analysis and has the following general form

$$G(x, y, \theta, u, \sigma) = \frac{1}{2\pi\sigma^2}\exp\left\{-\frac{x^2+y^2}{2\sigma^2}\right\}\exp(2\pi i(ux\cos\theta + uy\sin\theta)) \quad (1)$$

where i = -1, u is the frequency of the sinusoidal wave, q controls the orientation of the function and s is the standard deviation of the Gaussian envelope. To make it more robust against brightness, Gabor function, G(x, y, θ, u, σ) with a special set of parameters (σ, θ, u) is transformed into a discrete Gabor filter G[x, y, θ, u, σ] which is turned to zero by using the following formula

$$\tilde{G}(x, y, \theta, u, \sigma) = G(x, y, \theta, u, \sigma) - \frac{\sum_{i=-n}^{n}\sum_{j=-n}^{n} G(i, j, \theta, u, \sigma)}{(2n+1)^2} \quad (2)$$

where $(2n+1)^2$ is the size of the filter. In fact, the imaginary part of the Gabor filter automatically has zero DC because of odd symmetry. The sample point in the filtered image is coded to two bits (b_r, b_i) by the following inequalities

$$b_r = 1 \ if \ \ \mathrm{Re}\left[\tilde{G}(x,y,\theta,u,\sigma) * I\right] \geq 0, \quad (3)$$

$$b_r = 0 \ if \ \ \mathrm{Re}\left[\tilde{G}(x,y,\theta,u,\sigma) * I\right] < 0, \quad (4)$$

$$b_i = 1 \ if \ \ \mathrm{Im}\left[\tilde{G}(x,y,\theta,u,\sigma) * I\right] \geq 0, \quad (5)$$

$$b_i = 0 \ if \ \ \mathrm{Im}\left[\tilde{G}(x,y,\theta,u,\sigma) * I\right] < 0, \quad (6)$$

where *I* is the sub-image of a palmprint. Using these coding method palmprint features are generated.

5.2 Extraction of Features from Iris

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 [12]. The procedures included in the feature extraction process of the iris image are as follows

5.2.1 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.

5.2.2 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 [13] is utilized for the transformation process and is depicted in Figure 2.

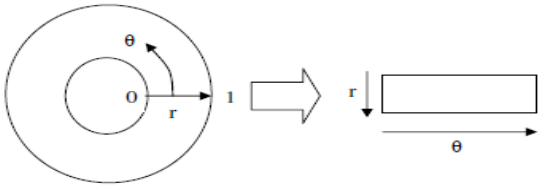

Figure 2. Daugman's rubber sheet model

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 where as, 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.

$$I[x(r, \theta), y(r, \theta)] \rightarrow I(r, \theta) \quad (7)$$

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 (8) to (13).

$$x(r, \theta) = (1 - r)x_p(\theta) + x_i(\theta) \quad (8)$$
$$y(r, \theta) = (1 - r)y_p(\theta) + y_i(\theta) \quad (9)$$
$$x_p(\theta) = x_{p0}(\theta) + r_p\mathrm{Cos}(\theta) \quad (10)$$
$$y_p(\theta) = y_{p0}(\theta) + r_p\mathrm{Sin}(\theta) \quad (11)$$
$$x_i(\theta) = x_{i0}(\theta) + r_i\mathrm{Cos}(\theta) \quad (12)$$
$$y_i(\theta) = y_{i0}(\theta) + r_i\mathrm{Sin}(\theta) \quad (13)$$

where, (x_p, y_p) and (x_i, y_i) are the coordinates on the pupil and iris boundaries along the direction. (x_{p0}, y_{p0}), (x_{i0}, y_{i0}) are the coordinates of pupil and iris centers [14].

5.2.3 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

$$G(f) = \exp\left(\frac{-(\log(f/f_0))^2}{2(\log(\sigma/f_0))^2}\right) \quad (14)$$

where f_0 indicates the centre frequency, and σ provides the bandwidth of the filter. The Log-Gabor filter outputs the biometric feature of the iris.

5.3 Feature Level Fusion of Palmprint and Iris Features

There are two sets of features used for fusion. They are Palmprint 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.

The texture properties are extracted from a palmprint are complex numbers are represented as $(x + iy)$. The extracted texture features which are stored in two different vectors: Vector P_1 contains the real part of the complex numbers and Vector P_2 contains the imaginary part of the complex numbers.

$$P_1 = [x_1\ x_2\ x_3\ \ldots\ldots x_n]\ ;\ |P_1| = n \quad (15)$$
$$P_2 = [y_1\ y_2\ y_3\ \ldots\ldots y_n]\ ;\ |P_2| = n \quad (16)$$

The texture properties obtained from the log-gabor filter are complex numbers $(a + ib)$. Similar to palmprint representation, we also store the iris texture features in two different vectors:

Vector I_1 contains the real part of the complex numbers and Vector I_2 contains the imaginary part of the complex numbers.

$$I_1 = [\, a_1\ a_2\ a_3\ \ldots\ldots a_m\,] \;;\; |\, I_1 \,| = m \qquad (17)$$
$$I_2 = [\, b_1\ b_2\ b_3\ \ldots\ldots b_m\,] \;;\; |\, I_2 \,| = m \qquad (18)$$

Thereby, the input to the fusion process will be four vectors P_1, P_2, I_1, and I_2. The fusion process results with the multimodal biometric template. The steps involved in fusion of biometric feature vectors are as follows

5.3.1 Shuffling of individual feature vectors

The first step in the fusion process is the shuffling of each of the individual feature vectors P_1, P_2, I_1 *and* I_2. The steps involved in the shuffling of vector P_1 are

Step 1: A random vector *R* of size P_1 is generated. The random vector *R* is controlled by the seed value.

Step 2: For shuffling the i^{th} component of palmprint feature vector P_1,
- a) The i^{th} 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 palmprint feature vector P_1.
- c) The resultant value is the index say ' *j* ' to be interchanged with. The components in the i^{th} and j^{th} indexes are interchanged.

Step 3: Step (2) is repeated for every component of P_1 . The shuffled vector P_1 is represented as S_1 .

The above process is repeated for every other vectors P_2, I_1 and I_2 with S_1, S_2 and S_3 as random vectors respectively, where S_2 is shuffled P_2 and S_3 is shuffled I_1 . The shuffling process results with four vectors S_1, S_2, S_3 and S_4.

5.3.2 Concatenation of shuffled feature vectors

The next step is to concatenate the shuffled vectors process S_1, S_2, S_3 and S_4. Here, we concatenate the shuffled palmprints S_1 and S_2 with the shuffled iris features S_3 and S_4 respectively. The concatenation of the vectors S_1 and S_3 is carried out as follows:

Step 1: A vector M_1 of size $|S_1| + |S_2|$ is created and its first $|S_3|$ values are filled with S_3 .

Step 2: For every component S_1 ,
- a) The corresponding indexed component of M_1 say t is chosen.
- b) Logical right shift operation is carried in M_1 from index ' t '.
- c) The component of S_1 is inserted into the emptied t^{th} index of M_1 .

The aforesaid process is carried out between shuffled vectors S_2 and S_4 to form vector M_2. Thereby, the concatenation process results with two vectors M_1 and M_2.

5.3.3 Merging of the concatenated feature vectors

The last step in generating the multimodal biometric template B_T is the merging of two vectors M_1 and M_2. The steps involved in the merging process are as follows:

Step 1: For every component of M_1 and M_2,
- a) The components M_{11} and M_{21} are converted into their binary form.
- b) Binary NOR operation is performed between the components M_{11} and M_{21}.
- c) The resultant binary value is then converted back into decimal form.

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

6. MULTIMODAL HARDENING PROTOCOL

The following computations take place at the user side during registration process:

1) The user is asked to give the palmprint input at least five times and the similar properties are extracted to form palmprint template (PP). 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 combined Features template using AES-128 bit symmetric cipher in ECB mode.
3) The user then sends (UID, E_{AES}(CMF)) to the server for storage in its database.

Thus the Implementation of multimodal hardening protocol leads to the generation of Strong secret.

7. MULTIMODAL AUTHENTICATION 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 is 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=E_{AES}(CMF).

Step 2: The user Computes $B_1 \equiv g^{MB1} \pmod p$. The user sends the user ID along with B_1 to the server.

Step 3: Server selects the encrypted minutia template with the user-Id using a table look-up procedure and computes $B_2 \equiv g^{MB2} \pmod p$, where MB2 is the encrypted minutiae template stored at the server side during registration. Then the server compares whether $B_1 \equiv B_2 \pmod p$. If it holds the server is assured of the authenticity of the user otherwise aborts the authentication protocol. Then the server sends B_2 to the user.

Step 4: Upon reception of B_2, User verifies whether $B_1 \equiv B_2 \pmod p$, if so authenticated otherwise aborts the authentication protocol. If authenticated the user computes the session key by using the formula,

$$K_s = H_{SHA1}(U_{ID}, MB1) \qquad (19)$$

Step 5: Simultaneously the server also generates the session key using the formula,

$$K_s = H_{SHA1}(U_{ID}, MB2) \qquad (20)$$

These steps are performed for avoiding the dictionary attack from an outside attacker.

8. EXPERIMENTAL RESULTS

The experimental results of the proposed approach are presented in this section. The designed proposed system is experimented with the Matlab7.4. For experimentation, the palmprint images are collected from IIT Delhi Palmprint Database is used and the iris images from CASIA Iris Image Database collected by Institute of Automation, Chinese

Academy of Science. The proposed approach is tested with different sets of input images. For every input palmprint image, the extracted texture points and the intermediate results of the proposed approach are shown in Figure 3. Similarly, for iris images, the intermediate results such as the image with located pupil and iris boundary, the image with detected top eyelid region and the normalized iris image are given in Figure 4. Then, the 256 bit cryptographic key generated from the palmprint and iris images using the proposed approach is presented in Figure 5.

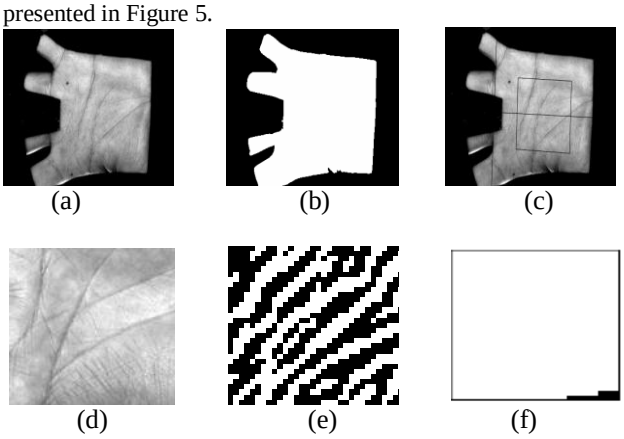

Figure 3. (a) Input Palmprint image (b) Binary image (c) Boundary tracking (d) Preprocessed result (e) Texture features of palmprint (f) Normalized palmprint image

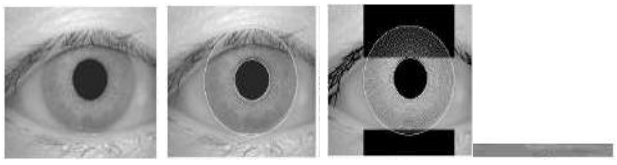

Figure 4. (a) Input iris image (b) Located pupil and iris boundary (c) Detected top and bottom eyelid region (d) Normalized iris image

01111011111110100100100100000000000111111111
11110101000101000100100011011011110111111110100
10010010010000000000011111111111101010001010000
10010001101101101000100010001001001010110110000
10011010110110001101001001100100101100011001000
11010011001100101100110110

Figure 5. Generated 256 bit key

The encryption using AES encryption algorithm is applied and the encrypted key is saved secure in the server and which avoids the dictionary attack. The multimodal hardening protocol and the multimodal authentication protocol is applied for the secure sharing of the cryptographic key.

8.1 Strength of the Protocol

The analysis for the security of the protocol is based on the following Deffie-Hellman assumptions [15]:

Assumption 1: For a cyclic group G, generated by g, we are given g and g^n, n Є N, the challenge is to compute n.

Assumption 2: Given g, g^a, g^b, it is hard to compute g^{ab}.

The relationship between these two assumptions has been extensively studied. It is clear that assumption 2 will not be satisfied in a group where finding a discrete logarithm solution is easy In Maurer and Wolf(1999), Boneh and Lipton (1996), the authors show that in several settings the validity of assumption 2 and the hardness of the discrete logarithm problem are in fact equivalent.

9. CONCULUSION

This Multimodal biometric authentication and key exchange system together with its practical applications offers many appealing performance features. The salient features of this proposal make it a suitable candidate for number of practical applications like Biometric ATMs, Biometric online web applications etc. Compared with previous solutions, our system possesses many advantages, such as the secure against dictionary attack, avoidance of PKI, and high efficiency in terms of both computation and communications. In this system, we have reused ideas in the areas of image processing technique to extract the minutiae from biometric image. Therefore it can be directly applied to fortify existing standard single-server biometric based security applications.

10. REFERENCES

[1] Arun Ross and Anil K. Jain, "Multimodal Biometrics: An Overview", in proceedings of the 12th European Signal Processing Conference, pp. 1221-1224, 2004.

[2] A.K. Jain and A. Ross, "Multi-biometric systems: special issue on multimodal interfaces that flex, adapt, and persist", Communications of the ACM, vol. 47, no. 1, pp. 34–40, 2004.

[3] L.Hong, and A.K.Jain "Can multibiometrics improve performance?", in Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies, pp. 59–64, NJ, USA, 1999.

[4] M.Bellare, D. Pointcheval, and P. Rogaway, "Authenticated Key Exchange Secure Against Dictionary Attacks," Advances in Cryptology Eurocrypt, 2000 pp. 139-155.

[5] J. Brainard, A. Juels, B. Kaliski, and M. Szydlo, "A New Two – Server Approach for Authentication with Short Secrets," Proc. USENIX Security Symp., 2003.

[6] Y.J. Yang, F. Bao, and R.H. Deng, "A New Architecture for Authentication and Key Exchange Using Password for Federated Enterprises, " Proc. 20th Federation for Information Processing Int'l Information Security Conference. (SEC '05), 2005.

[7] 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.

[8] D. Zhang and W. Shu, "Two novel characteristics in palm-print verification: Datum point invariance and line feature matching," *Pattern Recognition*, vol. 32, pp. 691–702, 1999.

[9] Wai-Kin Kong, "Palmprint Texture Analysis Based on Low-Resolution Images for Personal Authentication, Proceedings of the 16th International Conference on Pattern Recognition (ICPR'02) IEEE, 2002.

[10] David zhang, "Palmprint Idetification using Feature-level Fusion", Pattern Recognition society, Published by Elseiver Ltd, 2005.

[11] A. Jagadeesan, 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.

[12] 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.

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

[14] 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.

[15] D. Boneh,"The Decision Diffie-Hellman Problem", Proc. Third Int'l Algorithmic Number Theory Symp., pp. 48-63, 1998.