Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature

A. Jagadeesan[1], T.Thillaikkarasi[2], Dr.K.Duraiswamy[3]
Senior Lecturer/EIE[1], Senior Lecturer/EEE[2], Dean/Academic[3]
[1&2]Bannari Amman Institute of Technology Sathyamangalam-638 401, Tamil Nadu, India
[3]K.S.Rangasamy College of Technology, Tiruchengode – 637 209, Tamil Nadu, India

ABSTRACT

Human users find difficult to remember long cryptographic keys. Therefore, researchers, for a long time period, have been investigating ways to use biometric features of the user rather than memorable password or passphrase, in an attempt to produce tough and repeatable cryptographic keys. Our goal is to integrate the volatility of the user's biometric features into the generated key, so as to construct the key unpredictable to a hacker who is deficient of important knowledge about the user's biometrics. In our earlier research, we have incorporated multiple biometric modalities into the cryptographic key generation to provide better security. In this paper, we propose an efficient approach based on multimodal biometrics (Iris and fingerprint) for generating a secure cryptographic key, where the security is further enhanced with the difficulty of factoring large numbers. At first, the features, minutiae points and texture properties are extracted from the fingerprint and iris images respectively. Then, the extracted features are fused at the feature level to obtain the multi-biometric template. Finally, a multi-biometric template is used for generating a 256-bit cryptographic key. For experimentation, we have used the fingerprint images obtained from publicly available sources and the iris images from CASIA Iris Database. The experimental results have showed that the generated 256-bit cryptographic key is capable of providing better user authentication and better security.

Keywords: Biometrics, Multi-modal, Fingerprint, Minutiae points, Iris, Rubber Sheet Model, Fusion, Cryptographic key, Chinese Academy of Sciences Institute of Automation (CASIA) iris database.

1. Introduction

In the wake of heightened regarding security and swift progression in networking, communication and mobility, there are rapid demand in reliable user authentication techniques [1]. Majority of the authentication systems found today are of not very flexible (can be broken or stolen) to attacks, rather it can control access to computer systems or secured locations utilizing passwords. Thus, in most of the application areas [23], biometrics has emerged practically as a better alternative to conventional identification methods in recent. Biometrics which deals with the science of recognizing a person on the basis her/his physiological or behavioral traits has started to achieve acquiescence as a genuine method for identifying an person`s identity [1]. Biometric technologies have confirmed its importance in the fields such as security, access control and monitoring applications. Technologies are always innovative and seem to be fast growing [2]. Besides conventional authentication methods, biometric systems provides various advantages that are numbered below 1) Using direct covert observation, a biometric information can't be attained 2) reproduction and sharing is impracticable 3) By easing the necessity to keep in mind lengthy and random passwords, it augments user expediency, 4) It safeguards against negation by the user. Unlike passwords, biometrics also bestows the similar level of security to every user and is extremely immune to brute force attacks [3]. The important biometric characteristics currently in use includes fingerprint, DNA, iris pattern, retina, ear, face, thermogram, gait, hand geometry, palm-vein pattern, keystroke dynamics, smell, signature, and voice [16, 17].

Practical problems like noisy sensor data, non-universality and/or lack of distinctiveness of the biometric trait, unacceptable error rates, and spoof attacks [4] affects biometric systems which utilizes a single trait for recognition (i.e., unimodal biometric systems). This can be surmounted via multimodal biometric systems (a probable improvement of biometrics technology) and this is achieved by strengthening the proof attained from diverse sources [5] [6]. Multimodal biometric system utilizes a minimum of two and more than two single modalities. Some examples are face, gait, Iris and fingerprint, to enhance the recognition accuracy of conventional unimodal methods. By bestowing supplementary useful information to the classifier, multiple biometric modalities have shown decreased error rates. Diverse characteristics can be utilized by an individual system or independent systems which can function separately and their decisions may be combined [7]. In disparity to unimodal biometric authentication, the security and efficiency can be increased using the multimodal-based authentication and therefore for an opponent to spoof the system would be of very complex owing to a pair of distinct biometrics traits [15].

In recent decades, multimodal biometrics fusion techniques have attained much focus of interest as additional information among diverse modalities that could enhance the recognition performance. Majority of the works have focused on multimodal biometrics [8-10]. It is broadly categorized into three major levels:(i) fusion at the feature level (ii) fusion at the match level and finally (iii) fusion at the decision level [6] [11]. Fusion at the feature level entails the integration of feature sets related to multiple modalities. Integration at this level is expected to bestow fine recognition output, in view of the fact that the feature set comprises richer information about the raw biometric data than the match score or the final decision. In practice, to accomplish fusion at this level is complicated process due to the following reasons: (i) the feature sets of multiple modalities is highly incompatible (e.g., minutiae set of fingerprints and eigen-coefficients of face); (ii) Scarcity of knowledge about the relationship between the feature spaces of different biometric systems; and (iii) joining two feature vectors may lead to a feature vector with very large dimensionality that results in the `curse of dimensionality' problem [12].

A recent progress in biometrics is biometric cryptosystems [13] which is nothing but the combination of both cryptography and biometrics that benefits from the strengths of both fields. The main advantage of utilizing cryptography is its availability for high and adjustable security levels; on the other hand biometrics brings in non-repudiation and eradicates the necessity to memorize passwords or to carry tokens etc [14]. Of late, amongst the researchers and experimenters, a massive reputation has been attained for the enhanced performance of cryptographic key generated from biometrics in terms of security [18] and by abolishing the requirement for key storage using passwords, researchers in the recent past have endeavored towards merging biometrics with cryptography so as to increase overall security [19-22]. Still, the attackers grasp the possibility of sneaking through cryptographic attacks in spite of its high infeasibility to break cryptographic keys generated from biometrics. One proficient solution with added security to accomplish incredible security against cryptographic attacks will be the incorporation of multimodal biometrics within cryptographic key generation.

In our earlier research [27], we developed an approach for cryptographic key generation from multimodal biometric template. In this paper, we develop the secure cryptographic key generation approach depending on the problem of factoring the large number. Initially, the minutiae points are extracted from the fingerprint image. The extraction process utilized the subsequent steps such as Image enhancement based on local statistics using neighborhood operations, ROI extraction, Estimation of orientation field and morphological thinnig process. On the other hand, the texture features are extracted from the iris image utilizing the following steps namely, segmentation, estimation of iris boundary and Normalization. Then, the extracted features are used to perform the fusion process, in which we make use of feature level fusion technique. Fusion process consists of intermediate steps such as shuffling, joining based on exponential operation and combining with the help of prime multiplication. The multimodal biometric template is obtained from the fusion process and thereby, a user-specific secure cryptographic key is generated.

The rest of the paper is structured as follows. A brief review of the researches related to the proposed approach is given in Section II. The proposed approach for generation of multimodal-based cryptographic key is given in Section III. The experimental results of the proposed approach are presented in Section IV. Finally, the conclusions are given in Section V.

2. Review of Related Literature

A copious number of researches are available in the literature for generating cryptographic keys from biometric modalities and multimodal biometrics based user authentication. Recently, among researchers, a great deal of attention have been received on developing approaches for cryptographic key generation from biometric features and authenticating users by combining multiple biometric modalities. A concise review of few recent researches is presented here.

Feng Hao et al. [31] have presented a biometric based cryptographic key generation method utilizing the iris feature. From legitimate iris codes, a recurring binary string termed as biometric key was created which is more reliable. Auxiliary error-correction data, that does not unvei006C the key and can be accumulated in a tamper-resistant token, like a smart card was used to create the key from a subject's iris image. The regeneration of the key orbits on two factors: the iris biometric and the token. They evaluated the method utilizing iris samples taken from 70 different eyes, with 10 samples from each eye. They produced an error-free key which were created reliably from a legitimate iris codes and hence achieved a 99.5 percentage rate. They produced up to 140 bits of biometric key that is adequate for a 128-bit AES. B. Chen and V. Chandran [21] have presented a technique that produces deterministic bit-sequences from the output of a repetitive one-way transform via entropy based feature extraction process coupled with Reed-Solomon error correcting codes. The technique was evaluated by means of a 3D face data and was thus confirmed to be reliable in key generations of suitable length for 128-bit Advanced Encryption Standard (AES).

Beng.A et al. [33] have presented a biometric-key generation scheme based on a randomized biometric helper. The technique consists of a code redundancy construction and a randomized feature discretization process. The first one permitted the minimization of the errors as well as even more; on the other hand the later one controlled the intra-class variations of biometric data to the minimum level. The randomized biometric helper proved that a biometric-key was easy to be invalidated as soon as the key get conciliated. The subset of the Facial Recognition Technology (FERET) database helps to evaluate the projected technique in the context of face data. The straight generation of the biometric keys from live biometrics, under definite conditions, by partitioning feature space into subspaces and partitioning subspaces into cells, where each cell subspace gives to the overall key generated has been presented by Sanaul Hoque et al. [32]. On contrary to both genuine samples and attempted imitations, still they investigated the presented technique on real biometric data. The reliability in the probable realistic scenarios of this technique has been confirmed through experimental results.

Gang Zheng et al. [30] have depicted a lattice mapping based fuzzy commitment method for cryptographic key generation from biometric data. This technique obscured the original biometric data and also produced high entropy keys. In spite the stored information in the system being naked to an attacker, the technique makes it highly unfeasible to recover the biometric data. Simulated results have confirmed that its authentication accuracy was equal to that of the k-nearest neighbor classification. To select subspace, a Geometry Preserving Projections (GPP) method has been presented by Tianhao Zhang et al. [10]. It is proficient of differentiating various classes and preserving the intra-modal geometry of samples among an indistinguishable class. With GPP, classification can be processed by projecting all raw biometric data from various identities and modalities onto a unified subspace. In addition to these, after having a unified transformation matrix to project various modalities, the training stage was being done. For each recognition tasks, the effectiveness of the presented GPP has been proved using experimentation.

Donald E. Maurer and John P. Baker et al. [28] have described fusion architecture on the basis of Bayesian belief networks. The proposed technique utilized the graphical structure of Bayes nets to define and certainly model statistical dependencies among significant variables: per sample measurements such as, match scores and consequent quality estimates and global decision variables. These statistical dependencies are structured as conditional distributions that are modeled as Gaussian, gamma, log-normal or beta. Every model is obtained by its mean and variance, there by significantly reducing training data requirements. Additionally, by conditioning decision variables on quality and match score on contrary to reject them out of hand, they retrieved the information from lower quality measurements. Another significant feature of the technique was, a global quality measure anticipated to be utilized as a confidence estimate supporting decision making.

Muhammad Khurram Khana and Jiashu Zhanga [15] have proposed an efficient multimodal face and fingerprint biometrics authentication system on space-limited tokens, e.g. smart cards, driver license, and RFID card. Fingerprint templates were encrypted and encoded/embedded within face images by which the characteristics do not get distorted radically through the process of encoding and decoding. Experimental and simulation results showed that the presented technique was an inexpensive substitute to the multimodal biometrics authentication on space-limited tokens devoid of downgrading the entire decoding and matching performance of the biometrics system. Yan Yan and Yu-Jin Zhang [11] have bestowed a class-dependence feature analysis technique on the basis of Correlation Filter Bank (CFB) technique for an efficient multimodal biometrics fusion at the feature level. In CFB, an unconstrained correlation filter trained for a specific modality is being outputted by optimizing the entire original correlation. Therefore the discrepancy among modalities has are taken into account as well as the valuable information in different modalities is completely utilized. Prior investigational result on the fusion of face and palmprint biometrics confirmed the benefit of the technique.

M. Nageshkumar et al. [24] have presented an authentication method utilizing two features i.e. face and palmprint for multimodal biometric system identification. The robustness of the person authentication has been enhanced by the combination of both palmprint and face features. The final evaluation was made by fusion at matching score level architecture where features vectors were created autonomously for query measures and afterwards these are assessed to the enrolment template, which were stored during database preparation. Multimodal biometric system was stretched out via fusion of face and palmprint recognition.

3. An Effective Approach for Generation of Security-Enhanced Cryptographic Key from Multi-Modal Biometrics

Multimodal biometric authentication has lately evolved as an interesting research area. In addition to these it is more consistent as well highly proficient than knowledge-based (e.g. Password) and token-based (e.g. Key) techniques [24]. Multiple biometric traits are successfully utilized by quite a few researchers to attain user authentication [10, 11, 15 and 28]. Security-conscious customers have set stringent performance requirements and thereby multimodal biometrics was expected to convene this requirement. The following are very few good advantages of multimodal biometrics 1) improved accuracy 2) in case if sufficient data is not extracted from a given biometric sample, it can serve as a secondary means of enrollment as well as verification or identification and 3) the capability to identify endeavors to spoof biometric systems via non-live data sources particularly fake fingers. The preference of the biometric traits to be combined and the application area both serves as the major constraints to find out the efficacy of the multimodal biometrics. The various biometric traits comprises of fingerprint, face, iris, voice, hand geometry, palmprint and more. In the proposed approach, for cryptographic key generation, fingerprint and iris features are combined. Since it is intricate for an intruder to spool multiple biometric traits concurrently, there are possibilities to bestow prominent security with the utilization of multimodal biometrics for key generation. The necessity to memorize or carry lengthy passwords or keys is averted by the integration of biometrics within the cryptography. The steps involved in the proposed approach based on multimodal biometrics for cryptographic key generation are,

1) Extraction of minutiae points from fingerprint
2) Extraction of features from iris
3) Feature level fusion of fingerprint and iris features
4) Cryptographic key generation from fused features

3.1 Extraction of Minutiae Points from Fingerprint

This sub-section describes the method of extracting the minutiae points from the fingerprint image. We prefer fingerprint biometrics primarily for the following significant characteristics namely uniqueness and permanence (capability to sustain with no changes till its lifetime). A fingerprint can be described as a pattern of ridges and valleys present on the surface of a fingertip. The minutiae points such as (1) ridge endings (terminals of ridge lines) and (2) ridge bifurcations (fork-like structures) are formed by the ridges of the finger [26]. The important features of fingerprint are of those minutiae points. The steps used in the proposed approach for minutiae extraction are as follows,

1. Image enhancement based on local statistics using neighborhood operations
2. ROI extraction
3. Estimation of orientation field
4. Minutiae extraction

3.1.1 Image enhancement based on local statistics using neighborhood operations

To enhance the fingerprint image, we utilize the method based on local statistics. This method makes use of sliding neighborhood operations for image enhancement where, the non-linear filter is used for performing the Sliding Neighborhood Operation. At first, the input image is processed with a sliding blocks. For each sliding block, the centre pixel of the sliding block is updated with the local response of the corresponding sliding block (L_R) when, condition 1, 2 and 3 are satisfied. Condition 1: $M_b \le K_M * M_F$ Condition 2: $V_b \ge K_V * V_F$ Condition 3: $V_b \le K_V' * V_F$. Otherwise, the local response is equivalent to the centre pixel value of the sliding block (F_b). The local response of the sliding block is calcultated based on the following equation,

Local response, $L_R = E \times F_b$

Where, E → Enhancement Threshold

F_b →Central pixel value of the sliding block

M_b →Mean of the block

V_b → Variance of the block

M_F →Mean of the fingerprint image

V_F →Variance of the fingerprint image

K_M →Mean Threshold

K_V' & K_V →Variance Thresholds

Finally, we obtain the enhanced fingerprint image, where the visual quality of the image is considerably improved so that the recognition of ridges can be easily achieved.

3.1.2. ROI Extraction

The next step is to find the region of interest in the enhanced fingerprint image. In the fingerprint image, the region of interest (ROI) is the area of an image, which is importance for extraction of minutiae points. At first, the fingerprint image is divided into non-overlapping blocks of size 16x16. Then, the gradient of each block is computed. The standard deviation (SD) of gradients in X and Y direction are calculated and summed. The block is filled with ones only if the resultant value exceeds the threshold value, else the block is filled it with zeros.

3.1.3 Estimation of orientation field

The most common technique to estimate the orientation field of the fingerprint image is gradient based methods. In gradient based methods, at first, the gradient vectors are computed for a fingerprint image by obtaining the partial derivatives of gray intensity at every pixel. It is feasible to indicate a gradient vector as $[g_x, g_y]^T$ in Cartesian coordinates. In a fingerprint image, the gradient vectors, constantly point to the directions of the peak variation of gray intensity that are perpendicular to the edges of ridge lines. A collection of two-dimensional orientation fields is known as fingerprint orientation map. The magnitudes of these fields can be neglected. Hardly the angle information alone is focused since it captures the dominant ridge direction in each regular spaced grid. An orientation map is generally symbolized as a matrix θ_{xy} , where $\theta_{xy} \in [0,\pi]$ [40].

3.1.4. Minutiae extraction

The enhanced fingerprint image is then used for the process of minutiae point extraction. To perform the extraction process, we first apply the binarization and morphological operations to the enhanced fingerprint image. Binarization is the process of converting a grey level image into a binary image. Morphological operations are used to remove unnecessary spurs, bridges and line breaks are removed. The ridge thinning algorithm is used for removing the redundant pixels till the ridges become one pixel wide. The Ridge thinning algorithm used for Minutiae points' extraction in the proposed approach has been employed by the authors of [36]. After that, minutiae points are extracted from the thinned fingerprint image. The major minutia features of fingerprint ridges are: ridge ending (the abrupt end of a ridge), bifurcation (a single ridge that divides into two ridges). The process of extraction of minutiae points such as ridge ending and bifurcation is described as:

(1) Normalize the fingerprint image resulted from ROI extraction (F_D) to the size of the thinned fingerprint image.

(2) Compute the Euclidean distance transform of the fingerprint image, F_D.

(3) For every pixel ($p(i)$) except the boundary pixel in the thinned fingerprint image, neighbor pixels, $p_1, p_2,..., p_8$ are identified.

Where, $p_1, p_2,..., p_8$ are the values of the eight neighbors of $p(i)$, starting with the east neighbor and numbered in counter-clockwise order.

(4) Calculate the value $Q(i)$ for every pixel $p(i)$.

$$Q(i) = 0.5 * \left[(p_8 - p_1) + \sum_{i=1}^{7} (p_i - p_{i+1}) \right]$$

(5) The point is said to be a ridge ending points, when $Q(i) = 1$ and $F_D(i) > 6$.

(6) The point is said to be a bifurcation points, when $Q(i) \geq 3$ and $F_D(i) > 6$.

The identified ridge ending and bifurcation points are known as minutiae points that are unique features found within the fingerprint patterns. These points are then used for generating the secured cryptographic key generation.

3.2 Extraction of Features from Iris

The method of extracting features from the iris image is discussed in this sub-section. Iris recognition has been renowned as a successful means for providing user authentication. A unique significant characteristic of the iris is that, no two irises are similar, even for identical twins, among the human population [37]. An annular part between the pupil (generally, appearing black in an image) 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 [38]. 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. In general, the development of iris segmentation is comprises of two steps 1) Estimation of iris boundary and 2) Noise removal.

3.2.1.1 Estimation Of Iris Boundary

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.

- *Canny edge detection*

John F. Canny developed the canny edge detection operator in 1986. To find an extensive range of edges in images, it utilizes a multi-stage algorithm. Canny edge detection begins by means of linear filtering to calculate the gradient of the image intensity distribution function and stops with thinning and thresholding to achieve a binary map of edges. A important feature of the Canny operator is its optimality in managing noisy images as the method to link between strong and weak edges of the image by relating the weak edges in the output only if they are connected to strong edges. Consequently, the edges will perhaps be the actual ones. Hence compared to other edge detection methods, the canny operator is less fooled by spurious noise [39].

- *Hough Transform*

The traditional Hough transform was regarded with the identification of lines in the image, after that, the Hough transform has been enhanced to find positions of arbitrary shapes, usually circles or ellipses. For the parameters of circles passing through every edge point, votes are being casted in Hough space, from the obtained edge map. These parameters are the centre coordinates x and y, and the radius r that are capable to describe every circle in accordance with the following equation

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

A peak point in the Hough space will correspond to the radius and centre coordinates of the circle finitely described by the edge points.

3.2.1.2 Isolation of Eyelids and Eyelashes

Generally, the eyelids and eyelashes occlude the upper and lower parts of the iris region. Besides, specular reflections can happen inside the iris region corrupting the iris pattern. The elimination of such noises is also indispensable for attaining consistent iris information.

- Eyelids are isolated by fitting a line to the eyelids utilizing the linear Hough transform. A second horizontal line is then drawn that bisects with the first line at the iris edge which is closest to the pupil; the second horizontal line permits utmost isolation of eyelid region

- Compared with the surrounding eyelid region, the eyelashes seem to be quite dark. As a result, thresholding is utilized to isolate eyelashes.

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 is utilized for the transformation process.

3.2.2.1 Daugman's Rubber Sheet Model

Normalization process includes unwrapping the iris and transforming it into its polar equivalent. It is performed utilizing Daugman's Rubber sheet model [35] and is depicted in the following figure,

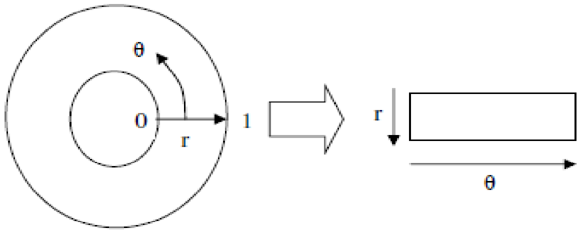


Fig 1: Daugman's Rubber Sheet Model

On polar axes, for each pixel in the iris, its equivalent position is found out. The process consists of two resolutions: (i) Radial resolution and (ii) 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.

$$I[x(r,\theta), y(r,\theta)] \to I(r,\theta)$$

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 the preceding equations

$$x(r,\theta) = (1-r)x_p(\theta) + x_i(\theta)$$

$$y(r,\theta) = (1-r)y_p(\theta) + y_i(\theta)$$

$$x_p(\theta) = x_{p0}(\theta) + r_p Cos(\theta)$$

$$y_p(\theta) = y_{p0}(\theta) + r_p Sin(\theta)$$

$$x_i(\theta) = x_{i0}(\theta) + r_i Cos(\theta)$$

$$y_i(\theta) = y_{i0}(\theta) + r_i Sin(\theta)$$

where, (x_p, y_p) and (x_i, y_i) are the coordinates on the pupil and iris boundaries along the θ direction. (x_{p0}, y_{p0}), (x_{i0}, y_{i0}) are the coordinates of pupil and iris centers [39].

3.2.2.2 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,

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

Where f_0 indicates the centre frequency, and σ provides the bandwidth of the filter [34]. The Log-Gabor filter generates the biometric feature (texture properties) of the iris.

3.3. Feature Level Fusion of Fingerprint and Iris Features

At present, we have two sets of features. They are as follows 1) Fingerprint features and 2) Iris features. The two sets of features are fused to obtain a multimodal biometric template that can carry out biometric authentication.

Feature Representation: Fingerprint - Each minutiae points extracted from a fingerprint image is denoted as (x , y) coordinates. In this, we store those extracted minutiae points in two different vectors: Vector M_1 comprises every x co-ordinate values and vector M_2 comprises every y co-ordinate values.

$$M_1 = x_1\ \ x_2\ \ x_3 \ldots x_n\ ;\ |M_1| = \text{n}$$

$$M_2 = y_1\ \ y_2\ \ \text{y}_3 \ldots y_n\ ;\ |M_2| = \text{n}$$

Iris - The texture properties obtained from the log-gabor filter are complex numbers $(a + ib)$. Equivalent to fingerprint representation, we also store the iris texture features in two various vectors: Vector C_1 includes the real part of the complex numbers and vector C_2 includes the imaginary part of the complex numbers.

$$C_1 = a_1 \; a_2 \; a_3 \ldots \; a_m \; ; \; |C_1| = m$$

$$C_2 = b_1 \; b_2 \; b_3 \ldots \; b_m \; ; \; |C_2| = m$$

The four vectors namely M_1, M_2, C_1 and C_2 are fed as input to the fusion process (multimodal biometric generation). The multimodal biometric template is obtained from the output of the fusion process. The procedures for fusion of biometric feature vectors are given as below.

3.3.1. Shuffling of individual feature vectors

The foremost step in the fusion process is the randomly permutation of the individual feature vectors M_1, M_2, C_1 and C_2. Shuffling of vector M_1 includes the process as listed below,

i. A random vector R of size M_1 is generated. The random vector R is regulated by the seed value.

ii. For shuffling the i^{th} component of fingerprint feature vector M_1,

   a) Multiply the i^{th} component of the random vector R with a large integer value.

   b) Divide the product value attained with the size of the fingerprint feature vector M_1 and takes the remainder from it.

   c) The remainder value is the index say 'j' to be interchanged with. The components in the i^{th} and j^{th} indexes are interchanged.

iii. Step (ii) is iterated for all component of M_1. The randomly permutated vector M_1 is indicated as P_1.

The aforementioned process is iterated for all other vectors M_2, C_1 and C_2 with P_1 P_2 and P_3 as random vectors correspondingly, where P_2 is shuffled M_2 and P_3 is shuffled C_1. At the end of shuffling process, four vectors P_1, P_2, P_3 and P_4 are generated.

3.3.2. Joining of shuffled feature vectors

The next step is to join the randomly permutated vectors P_1, P_2, P_3 and P_4. Here, we join the randomly permutated fingerprints P_1 and P_2 with the randomly permutated iris features P_3 and P_4 respectively. The steps involved in the joining of the vectors P_1 and P_3 are given as follows:

(i) A vector V_1 is created and its components are filled with P_1 repeatedly.

(ii) For every component $P_3^{(i)}$,

(a) Exponentiation, a mathematical operation, written as $P_3(i)^{V_1(i)}$, involving two numbers, the base $P_3(i)$ and the exponent $V_1^{(i)}$ is performed.

(b) The resultant value is put into a vector $J_1^{(i)}$, when the resultant exceeds the threshold level.

(c) Otherwise, exponentiation $P_3(i)^{V_1(i)^{V_1(i+1)}}$ is performed and this procedure (taking exponentiation) is repeated until it reaches the value, which is above the threshold value.

The above process is carried out between shuffled vectors P_2 and P_4 to form vector J_2. Thus, the joining process results with two vectors J_1 and J_2.

3.3.3. Combining of joined feature vectors

The last step in generating the multimodal biometric template T_B is combining of two vectors J_1 and J_2. The combining of the vectors J_1 and J_2 is carried out as follows.

(i) For combining i^{th} component of J_1 and J_2,

(a) Take the next highest prime number for the i^{th} component of both the vectors (J_1 and J_2).

(b) Multiply the two prime numbers $J_1(i)$ and $J_2(i)$.

(c) Store the resultant in the i^{th} component of the vector T_B.

(ii) Step (i) is iterated for all component of J_1 and J_2. The combined vector T_B serves as multimodal biometric template.

Security analysis: Prime numbers are a basic constituent in public-key cryptography. "Prime Factorization" is very important for the researchers who are trying to generate a secure cryptographic key and it describes the procedure of finding the prime numbers that is multiplied together to get the large number. RSA [41], [29], [25], which is a well-known algorithm for public-key cryptography explain the hardness of obtaining the prime factors of the large number. We make use of the mathematical problem that is difficult to solve, such as factoring large number into primes, for enhancing the security of the cryptographic key. The proposed cryptographic key generation technique relies on the difficulty of factoring the large numbers.

3.4 Cryptographic Key Generation from the Fused Features

The generation of the k-bit cryptographic key from multimodal biometric template T_B is the last step of the proposed approach. The template vector T_B is represented as,

$$T_B = [t_1 \;\; \mathrm{t}_2 \; \mathrm{t}_3 \cdots \; \mathrm{t}_{\mathrm{d}}]$$

The vector T_B is then normalized to k components appropriate for generating the k-bit key. The normalization employed in the proposed approach is given as,

$$N = \begin{cases} [t_1 \;\; t_2 \;\; \cdots \;\; t_k] & ;if \;\; |T_B| > k \\ [t_1 \;\; t_2 \;\; \cdots \;\; t_d] << \mathrm{t_i};\ \mathrm{d}+1 \geq \mathrm{i} \geq \mathrm{k} & ;if \;\; |T_B| < k \end{cases}$$

$$\text{Where, } \mathrm{t_i} = \frac{1}{d}\sum_{j=1}^{d} t_j$$

Finally, the key K_B is generated from the vector N ,

$$K_B << \begin{cases} 1 & \text{if} \quad \mathrm{N_i} \geq N_{avg} \\ 0 & \text{if} \quad \mathrm{N_i} < N_{avg} \end{cases} \quad ; \quad i = 1,2,3\ldots,k$$

$$\text{Where, } N_{avg} = \frac{1}{k}\sum_{i=1}^{k} N_i$$

4. EXPERIMENTAL RESULTS

In this section, we have presented the experimental results of the proposed approach, which is implemented in Matlab (Matlab7.4). For experimentation, we have used the fingerprint images from publicly available databases and the iris images from CASIA Iris Image Database collected by Institute of Automation, Chinese Academy of Science. We have tested the proposed approach with different sets of input images (fingerprint images and iris images) and the results are shown in figure 4, 5, 6 and 7 for four sets of input images (shown in figure 2 and 3). For every input fingerprint images, the intermediate results of the proposed approach such as fingerprint image after enhancement, ROI extracted image, fingerprint image with minutiae points are given. 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. Then, we present the 256 bit cryptographic key generated from the fingerprint and iris images using the proposed approach.

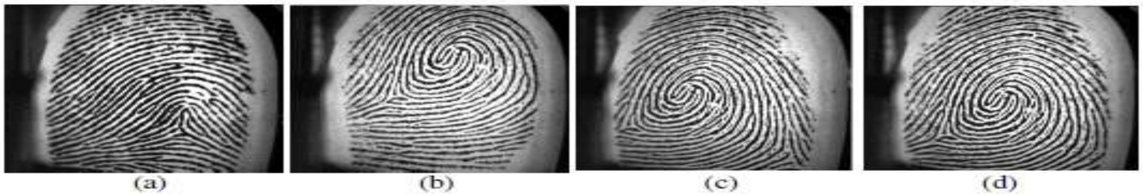


Fig 2: Input fingerprint images

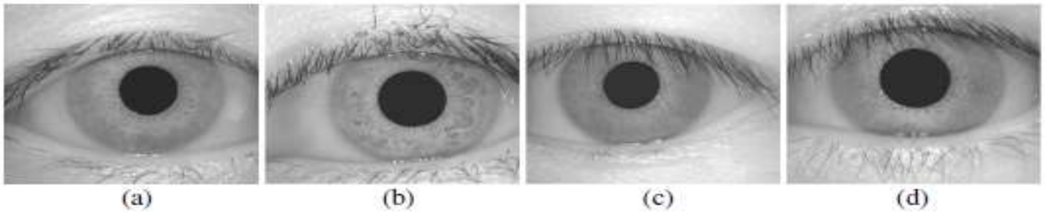


Fig 3: Input iris images

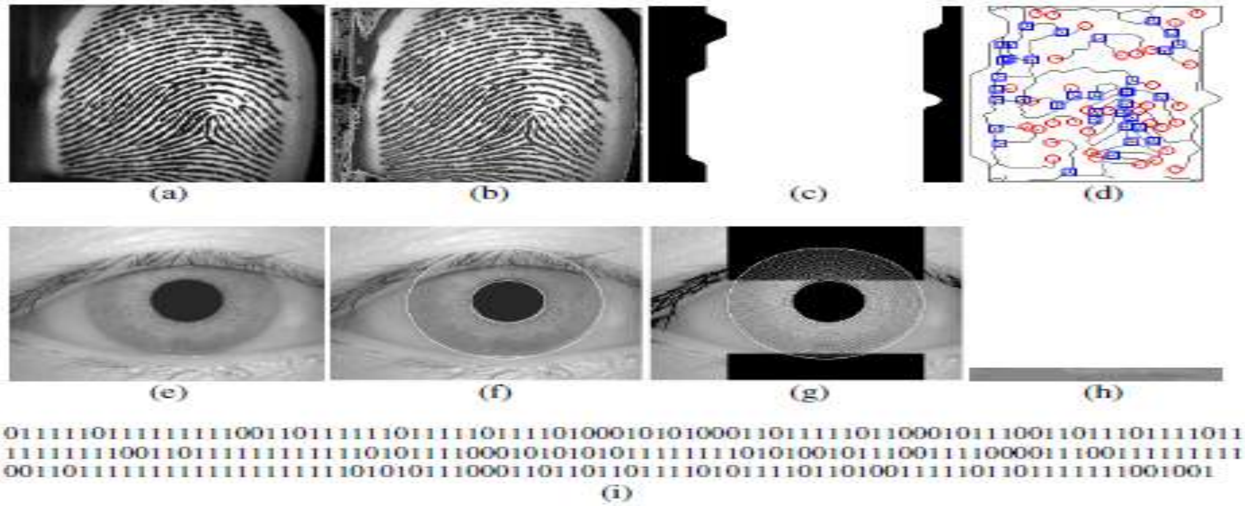
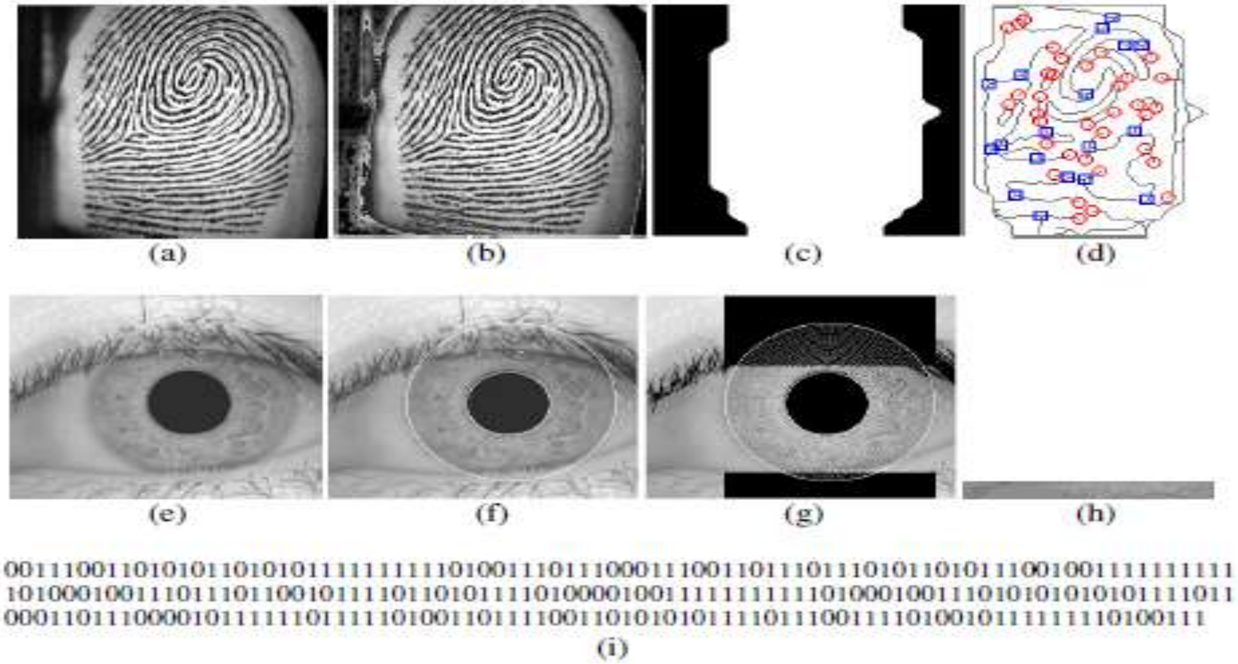
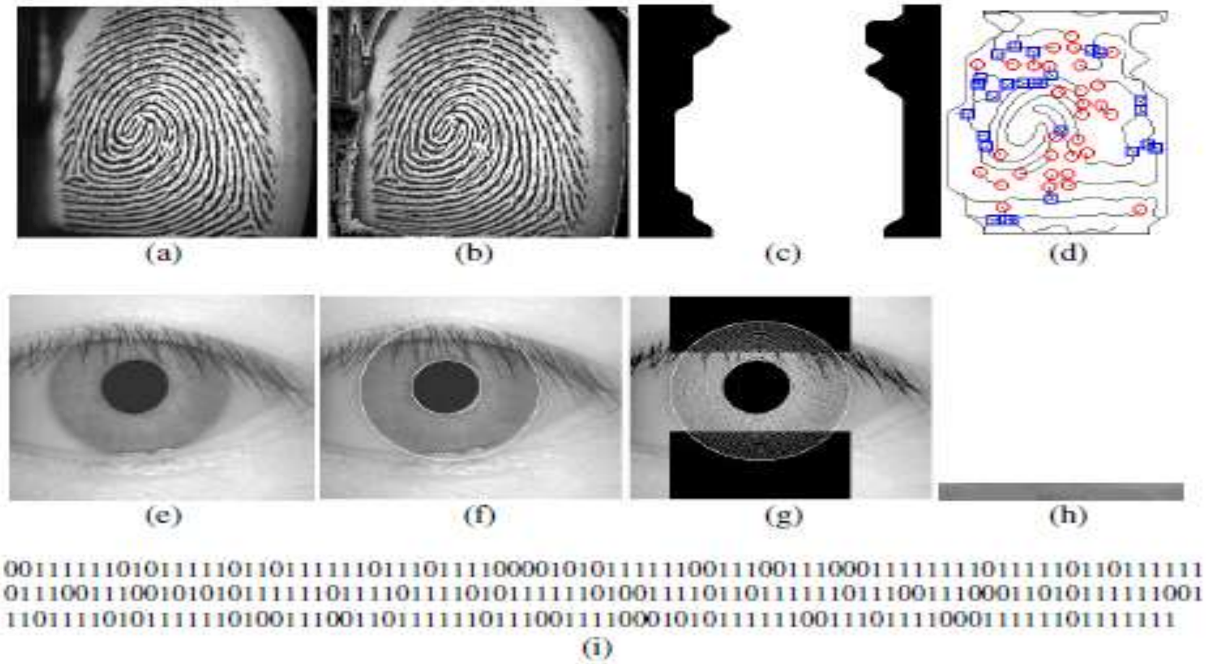


Fig 4: (a) Input fingerprint image (shown in fig 2.a) (b) Enhanced fingerprint image (c) ROI extraction (d) Fingerprint image with minutiae points (e) Input iris image (shown in fig 3.a) (f) Located pupil and iris boundary (g) Detected top and bottom eyelid region (h) Normalized iris images (i) Generated 256 bit key



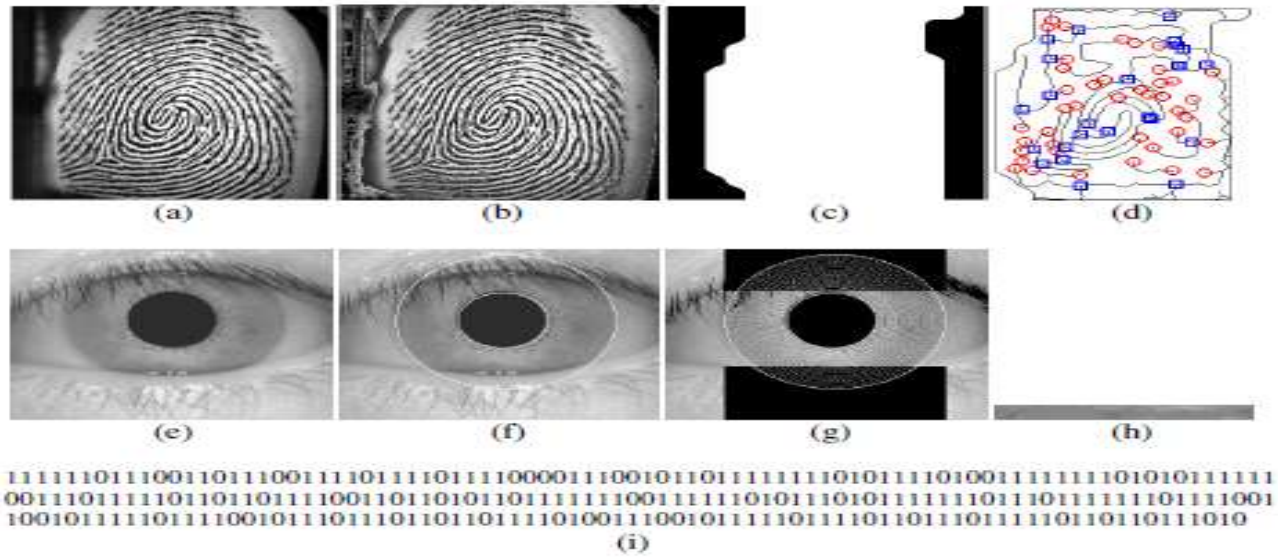
```
0011100110101011010101111111111110100111011100011100110111011101011010111001001111111111
1010001001110111011001011110110101111010000100111111111110100010011101010101010101111011
0001101110000101111110111110100110111100110101010111101110011110100101111111110100111
```

Fig 5: (a) Input fingerprint image (shown in fig 2.b) (b) Enhanced fingerprint image (c) ROI extraction (d) Fingerprint image with minutiae points (e) Input iris image (shown in fig 3.b) (f) Located pupil and iris boundary (g) Detected top and bottom eyelid region (h) Normalized iris image (i) Generated 256 bit key



```
0011111010111110110111111011101111000010101111110011100111000111111110111110110111111
0111001110010101011111101111010111111010011110110111111011100111000110101111111001
1101111010111111010011100110111111011100111100010101111110011101111000111111011111111
```

Fig 6: (a) Input fingerprint image (shown in fig 2.c) (b) Enhanced fingerprint image (c) ROI extraction (d) Fingerprint image with minutiae points (e) Input iris image (shown in fig 3.c) (f) Located pupil and iris boundary (g) Detected top and bottom eyelid region (h) Normalized iris images (i) Generated 256 bit key



```
1111110111001101110011110111101111000011100101101111111101011110100111111110101011111
0011101111101101101111001101101011011111111001111110101110101111111011101111111101111001
100101111101111001011101110110110111101001110010111110111101101110111110110110111010
```

Fig 7: (a) Input fingerprint image (shown in fig 2.d) (b) Enhanced fingerprint image (c) ROI extraction (d) Fingerprint image with minutiae points (e) Input iris image (shown in fig 3.d) (f) Located pupil and iris boundary (g) Detected top and bottom eyelid region (h) Normalized iris images (i) Generated 256 bit key.

5. CONCLUSION

In this paper, we have generated a 256-bit cryptographic key by incorporating the features of the fingerprint and iris. We have enhanced the security of the proposed approach by incorporating the complexity of factoring the large number. 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 multi-biometric template and subsequently generated a 256-bit secure cryptographic key from the multi-biometric template. For experimentation, we have employed the fingerprint images obtained from publicly available sources and the iris images from CASIA Iris Database. The experimental results have demonstrated the security of the proposed approach to produce user-specific cryptographic key is enhanced.

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] Richard A. Wasniowski, "Using Data Fusion for Biometric Verification", in Proceedings of World Academy of Science, Engineering and Technology, vol. 5, April 2005.

[3] Parvathi Ambalakat, "Security of Biometric Authentication Systems", in proceedings of 21st Computer Science Seminar, 2005.

[4] 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.

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

[6] Anil Jain, Karthik Nandakumar and Arun Ross, "Score normalization in multimodal biometric systems", Pattern Recognition, vol. 38, pp. 2270 – 2285, 2005.

[7] Eren Camlikaya, Alisher Kholmatov and Berrin Yanikoglu, "Multi-biometric Templates Using Fingerprint and Voice", Biometric technology for human identification, Vol. 6944, no5, pp: 1-9, Orlando FL, 2008.

[8] R. Wang and B. Bhanu, "Performance prediction for multimodal biometrics", In Proceedings of the IEEE International Conference on Pattern Recognition, pp. 586-589, 2006.

[9] X. Jing, Y. Yao, D. Zhang, J. Yang, and M. Li. "Face and palm print pixel level fusion and Kernel DCV-RBF classifier for small sample biometric recognition", Pattern Recognition, vol. 40, no.11, pp. 3209-3224, 2007.

[10] T. Zhang, X. Li, D. Tao, and J. Yang, "Multi-modal biometrics using geometry preserving projections", Pattern Recognition, vol. 41, no. 3, pp. 805-813, 2008.

[11] Yan Yan and Yu-Jin Zhang, "Multimodal Biometrics Fusion Using Correlation Filter Bank", in proceedings of 19th International Conference on Pattern Recognition, pp. 1-4, Tampa, FL, 2008.

[12] Arun Ross and Rohin Govindarajan, "Feature Level Fusion in Biometric Systems", in proceedings of Biometric Consortium Conference (BCC), September 2004.

[13] Umut Uludag, Sharath Pankanti, Salil Prabhakar, Anil K.Jain, "Biometric Cryptosystems Issues and Challenges", in Proceedings of the IEEE, vol. 92, pp. 948-960, 2004.

[14] P.Arul, Dr.A.Shanmugam, "Generate a Key for AES Using Biometric for VOIP Network Security", Journal of Theoretical and Applied Information Technology, vol. 5, no.2, 2009.

[15] Muhammad Khurram Khan and Jiashu Zhang, "Multimodal face and fingerprint biometrics authentication on space-limited tokens", Neurocomputing, vol. 71, pp. 3026-3031, August 2008.

[16] Kornelije Rabuzin and Miroslav Baca and Mirko Malekovic, "A Multimodal Biometric System Implemented within an Active Database Management System", Journal of software, vol. 2, no. 4, October 2007.

[17] M Baca and K. Rabuzin, “Biometrics in Network Security”, in Proceedings of the XXVIII International Convention MIPRO 2005, pp. 205-210 , Rijeka,2005.

[18] N. Lalithamani and K.P. Soman, "Irrevocable Cryptographic Key Generation from Cancelable Fingerprint Templates: An Enhanced and Effective Scheme", European Journal of Scientific Research, vol.31, no.3, pp.372-387, 2009.

[19] A. Goh and D.C.L. Ngo, “Computation of cryptographic keys from face biometrics”, International Federation for Information Processing 2003, Springer-Verlag, LNCS 2828, pp. 1–13, 2003.

[20] F. Hao, C.W. Chan, “Private Key generation from on-line handwritten signatures”, Information Management & Computer Security, vol. 10, no. 2, pp. 159–164, 2002.

[21] Chen, B. and Chandran, V., "Biometric Based Cryptographic Key Generation from Faces", in proceedings of 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp. 394 - 401, December 2007.

[22] N. Lalithamani and Dr. K.P. Soman, “An Effective Scheme for Generating Irrevocable Cryptographic Key from Cancelable Fingerprint Templates”, International Journal of Computer Science and Network Security, vol. 9, no.3, March 2009.

[23] Jang-Hee Yoo, Jong-Gook Ko, Sung-Uk Jung, Yun-Su Chung, Ki-Hyun Kim, Ki-Young Moon, and Kyoil Chung, "Design of an Embedded Multimodal Biometric System", ETRI-Information Security Research Division, 2007.

[24] Nageshkumar.M, Mahesh.PK and M.N. Shanmukha Swamy, “An Efficient Secure Multimodal Biometric Fusion Using Palmprint and Face Image”, IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[25] R. L. Rivest, A. Shamir and L. Adleman , "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol. 21, no. 2, pp. 120 - 126, February 1978.

[26] Yi Wang , Jiankun Hu and Fengling Han, "Enhanced gradient-based algorithm for the estimation of fingerprint orientation fields", Applied Mathematics and Computation, vol. 185, pp.823–833, 2007.

[27] A. Jagadeesan, K.Duraiswamy, “Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris”, International Journal of Computer Science and Information Security, IJCSIS, vol. 7, no. 2, pp. 28-37, February 2010.

[28] Donald E. Maurer and John P. Baker, "Fusing multimodal biometrics with quality estimates via a Bayesian belief network", Pattern Recognition, vol. 41 , no. 3, pp. 821-832, March 2008.

[29] “RSA” from http://en.wikipedia.org/wiki/RSA

[30] Gang Zheng, Wanqing Li and Ce Zhan, "Cryptographic Key Generation from Biometric Data Using Lattice Mapping", in Proceedings of the 18th International Conference on Pattern Recognition, vol.4, pp. 513 - 516, 2006.

[31] Feng Hao, Ross Anderson and John Daugman, "Combining Crypto with Biometrics Effectively", IEEE Transactions on Computers, vol. 55, no. 9, pp. 1081 - 1088, September 2006.

[32] Sanaul Hoque , Michael Fairhurst and Gareth Howells, "Evaluating Biometric Encryption Key Generation Using Handwritten Signatures", in Proceedings of the 2008 Bio-inspired, Learning and Intelligent Systems for Security, pp.17-22, 2008.

[33] Beng.A, Jin Teoh and Kar-Ann Toh, "Secure biometric-key generation with biometric helper”, in proceedings of 3rd IEEE Conference on Industrial Electronics and Applications, pp.2145-2150, Singapore, June 2008.

[34] David J. Field, "Relations between the statistics of natural images and the response properties of cortical cells", Journal of the Optical Society of America,vol. 4, no. 12, 1987.

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

[36] L. Lam, S. W. Lee, and C. Y. Suen, “Thinning Methodologies-A Comprehensive Survey”, IEEE Transactions on Pattern analysis and machine intelligence, vol. 14, no. 9, 1992.

[37] 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.

[38] 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.

[39] 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.

[40] Yi Wang, Jiankun Hu, Heiko Schroder, “A Gradient Based Weighted Averaging Method for Estimation of Fingerprint Orientation Fields”, pp.29, Digital Image Computing: Techniques and Applications (DICTA'05), 2005.

[41] “RSA Factoring Challenge” from http://en.wikipedia.org/wiki/RSA_Factoring_Challenge.

Authors Detail:

Mr.A.Jagadeesan was born in Coimbatore, India on June 14, 1979. He graduated from Bannari Amman Institute of Technology in 2000 with a degree in Electrical and Electronics Engineering. He completed his Master of Technology in Bio-medical Signal Processing and Instrumentation from SASTRA University in 2002. Thereafter he joined as a Lecturer in K.S.Rangasamy College of Technology till 2007. Now he is working as a Senior Lecturer in Bannari Amman Institute of Technology. He is a research scholar in the Department of Information and Communication Engineering in Anna University, Chennai. His area of interest includes Biometrics, Digital Image Processing, Embedded Systems and Computer Networks. He is a life member in ISTE and BMESI. He is also a member of Association of Computers, Electronics and Electrical Engineers (ACEEE) and International Association of Engineers (IAENG).

Mrs.Thillaikkarasi.T was born in Salem, India on May 18, 1981. She graduated from Adhiyamaan college of Engineering in 2002 with a degree in Electrical and Electronics Engineering. Thereafter she joined as a Lecturer in K.S.Rangasamy College of Technology and completed her Master of Engineering in Power Electronics and Drives from K.S.Rangasamy College of Technology in 2007. Now she is working as a Senior Lecturer in Bannari Amman Institute of Technology. She is a research scholar in the Department of Computer Science and Engineering in Anna University, Coimbatore. Her area of interest includes Multiprocessor based Embedded Systems, Computer Networks and Application specific SoC’s. She is a life member in ISTE.

Dr. K.Duraiswamy received his B.E. degree in Electrical and Electronics Engineering from P.S.G. College of Technology, Coimbatore in 1965 and M.Sc. (Engg) from P.S.G. College of Technology, Coimbatore in 1968 and Ph.D. from Anna University in 1986. From 1965 to 1966 he was in Electricity Board. From 1968 to 1970 he was working in ACCET, Karaikudi. From 1970 to 1983, he was working in Government College of Engineering Salem. From 1983 to 1995, he was with Government College of Technology, Coimbatore as Professor. From 1995 to 2005 he was working as Principal at K.S.Rangasamy College of Technology, Tiruchengode and presently he is serving as Dean of KSRCT. He is interested in Digital Image Processing, Computer Architecture and Compiler Design. He received 7 years Long Service Gold Medal for NCC. He is a life member in ISTE, Senior member in IEEE and a member of CSI.