# Secure Biometric Key Generation Scheme for Cryptography using Combined Biometric Features of Fingerprint and Iris

**Mr.P.Balakumar[1]and Dr.R.Venkatesan[2]**

**[1] Associate Professor, Department of Computer Science and Engineering,
Selvam College of Technology, Namakkal, Tamilnadu, India**

**[2] Professor and Head, Department of Computer Science and Engineering,
PSG College of Technology, Coimbatore, Tamilnadu, India**

## Abstract

Exact and automatic recognition and authentication of users are a essential difficulty in all systems. Shared secrets like Personal Identification Numbers or Passwords and key devices such as Smart cards are not presently sufficient in few situations. What is required is a system that could authenticate that the person is actually the person. The biometrics is improving the capability to recognize the persons. The usage of biometrics system permits the recognition of a living person according to the physiological features or behavioral features to be recognized without human involvement. This leads to the world wide usage of biometrics to secure the system. The various biometrics used in securing system are fingerprint, iris, retina, etc. The construction of cryptographic key from biometrics is used generally to secure the system. The efficiency and the flexibility of the cryptographic make it suitable for securing purpose. In some times, biometrics can be stolen; this makes the attackers to access the system for any time. This problem is diminished in this paper by using two biometrics features. The biometrics used in this paper is fingerprint and iris. These two features are combined with the help of fusion algorithm. From the combined features, cryptographic key is generated. The experimental result shows that the proposed techniques results in better security than the existing techniques.

***Keywords*—**Biometrics, Cryptography Key Generation, Minutiae Points, Security Analysis

## 1. Introduction

Information security and privacy has become an important factor in the present world. Biometric recognition is one of the most important techniques for the security privacy due to its distinctive nature of biometric [5] traits such as fingerprints, iris and faces [7]. As a result, this technique is used with many other applications to enhance the security. Cryptographic techniques have gained its popularity due to its security purpose. In the cryptographic technique the original data is encoded by using any key so that it is not in a understandable format for the attacker. The original data can be obtained by decoding the encoded data using the same key. Thus the privacy is well protected in this cryptographic approach. Several cryptographic techniques like DES, AES and public key architectures like RSA are widely used for the authentication purpose.

The characteristic feature of cryptographic security is conditioned by an authentication step that depends on long pseudo-random keys (128 bits in symmetric encryption), which are very impossible to keep in mind. This feature of inability to remember cryptographic keys [8] has been restraining the security of systems for a long time. The inability of human users to remember powerful cryptographic keys has been a feature restraining the security of systems for decades.

It's the natural tendency of humans to set passwords [6, 13] that are usually recognized or deduced by any social engineering methods. Typically people usually store keys in a place that is insecure and can possibly be shared among users and therefore it is not capable of ensuring non-repudiation. Moreover it's a natural human tendency to use same keys or password for a variety of applications and as a result, if one system is hacked it is very easy to hack all the systems corresponding to that key. This practically reduces the security privacy and makes the work easy for the hacker. Cryptographic techniques when combined with the biometric approach are used to solve these problems and provide security. The cryptographic keys are produced from the biometric data and are used in the authentication checking.

Biometric technique [17] provides the distinct characteristics of a person which is always prevalent. A person's individuality can be differentiated from one or more behavioral or physiological features by this authentication technique. Various techniques that are under the biometric research include facial, palm prints, retinal and iris scans, and hand geometry, signature capture and vocal features.

Biometric cryptosystems is a new technique which combines biometrics and cryptography [2], and is popularly known as crypto-biometric systems. The integration of biometrics [16] and cryptography is broadly carried out in two distinct steps. In case of biometrics-based key generation, a biometric matching amid an input biometric signal and a registered template is utilized in the release of the secret key.

In biometrics resetting is very much complicated. One of the huge merits of the biometric data over time is its uniformity which is also the demerit at the same instant. In case of any conventional techniques, like credit card, it is possible to issue a new one, if it is lost. But it is impossible to substitute the biometric characteristics and it is fully evident since it is not feasible to provide a person with a fresh biometric feature once it is stolen.

This problem can be solved by the approach called cancellable biometric. This procedure uses a predefined transform and thus provides the intended and repeatable distortion of a biometric signal. This approach thus makes expose cross matching unachievable by facilitating the every incidence of enrollment to utilize a distinct transform. Furthermore, it is just enough to merely change the transform operation to produce a new variant for re-enrollment, if a variant of the transformed biometric data is comprised. Generally, the non-invertible transforms are utilized for distortion. Thus it is impossible for the hacker or the unauthenticated user to recover the original biometrics without knowing the transform method and the resulting transformed biometric data.

This paper uses two biometrics features to generate the cryptography key [3, 4]. The biometrics used in this paper is fingerprint [11] and iris [18]. These two biometrics features are combined using a technique called fusion. From these combined features, cryptography key is generated in this paper.

## 2. Related Works

The proposed work is inspired from a number of researches which are related to cryptography and cancellable biometric techniques. Goh and Ngo combined have proposed a new system based on face biometrics [5]. The work adopted the biometric locking approach of Soutar et al. Here the features are the Eigen-projections which are extracted from the face image, each of which is then mixed with a random string and quantized into a single bit.

Cancellable biometrics gives a better performance of security as it facilitates with more than one template for the same biometric data. Ang et al. [1] proposed the measurement of the success of a particular transformation and matching algorithm for fingerprints. A key-dependent cancellable template for the fingerprint was produced by employing a key dependant geometric transform on the obtained fingerprint features. Besides, the performance evaluation of an authentication system that utilizes the cancellable biometric is studied and it was found that the performance of the cancellable biometric was significant.

Hao et al. [10] presented a realistic and secure way to incorporate the iris biometric into cryptographic applications. They deliberated on the error patterns within iris codes and developed a two-layer error correction technique that merges Hadamard and Reed-Solomon codes. The key was produced from the iris image of the subject through the auxiliary error correction data that do not disclose the key and can be saved in a tamper-resistant token like a smart card. The evaluation of the methodology was performed with the aid of samples from 70 different eyes, 10 samples being obtained from every eye. It was established that an error-free key can be reproduced reliably from genuine iris codes with a success rate of 99.5 percent. It is possible to produce up to 140 bits of biometric key, more than adequate for 128-bit AES.

An on-line signature-based biometric authentication system, where non invertible transformations were applied to the acquired signature functions ruling out the possibility to derive the original biometrics from the stored templates at the same time maintaining the same recognition performances of an unprotected system was projected by Maiorana et al. Precisely the probability of producing cancellable templates from the same original data, thereby offering an appropriate solution to privacy concerns and security problems was intensely explored.

Teoh et al. [15] have presented a two-factor cancellable formulation that facilitates data distortion in a revocable yet non-reversible manner by first converting the raw biometric data into a fixed-length feature vector followed by the projection of the feature vector onto a sequence of random subspaces that were obtained from a user-specified Pseudorandom Number (PRN). The process was revocable making the replacement of biometrics seem as easy as replacing PRNs. This formulation was confirmed under numerous scenarios (normal, stolen PRN, and compromised biometrics scenarios) with the aid of 2400 Facial Recognition Technology face images.A cancellable biometric approach called PalmHashing was projected by T. Connie et al. [5] in order to address the non revocable biometric issue. This technique hashes palmprint templates with a set of pseudo-random keys to acquire a unique code known as the palmhash.

A fuzzy commitment method working on lattice mapping for cryptographic key generation from biometric data was proposed later. Despite providing high entropy keys as output the method as well obscures the original biometric data such that it becomes unfeasible to recover the biometric data besides the stored information in the system being open to an attacker. Results of simulation illustrated that the method's authentication accuracy was analogous to that of the renowned. For cancelable biometrics, the main scheme is to store an irreversibly transformed version of the biometric template which provides a high privacy and security level by allowing multiple templates to be associated with the dame biometric data [7].

Jo et al. [12] proposed a simple technique for the generation of digital signatures and cryptography communication with the aid of biometrics. The generation of the signature is necessary

in such a way that it becomes possible to verify the same with a cryptographic algorithm in existence like the RSA without altering its own security constraint and infrastructure.

## 3. Proposed Methodology

Biometric cryptosystems combines cryptography and biometrics to afford the advantages of both for security. This technique will provide the advantages like better and modifiable security levels which are the advantages of cryptography and advantages like eliminating the must to memorize passwords or to carry tokens etc which are the advantages of using biometrics. This paper combines the features of fingerprint and iris and with that combined feature, cryptography key is generated.

### 3.1. Feature Extraction from Fingerprint

Figure.1 represents a general procedure of extracting the minutiae points from fingerprint taken from the user.

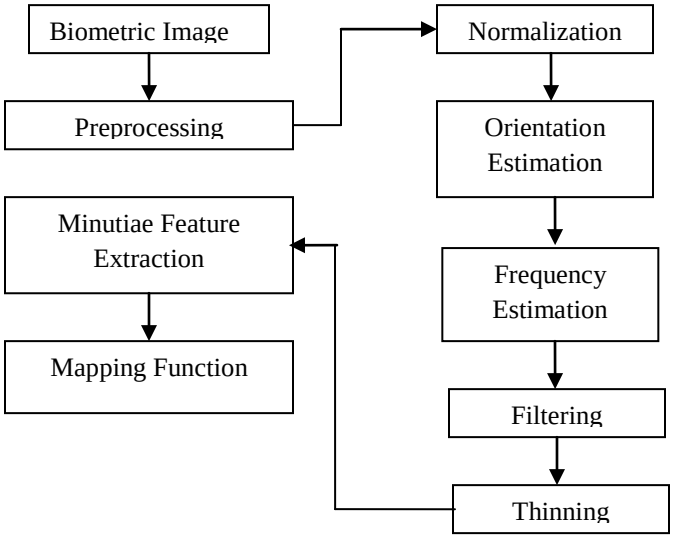



Figure 1. Steps Involved in Extracting Feature Point

*A. Fingerprint Enhancement*

This is usually required process in creating a security system with the help of biometrics. This process includes subsequent processing on the gathered fingerprint image. Fingerprint consists of sequence of ridges and furrows on the finger surface. This provides the individuality of the users fingerprint. No two fingerprints can have the similar existence of ridges and furrows. Minutiae points are local ridge features that appear at either a ridge bifurcation or a ridge ending. The ridges hold the information of features mandatory for minutiae extraction. Hence the clarity of the ridge occurrences in a fingerprint image must be very important. The gathered image is then enhanced with the help of image enhancement methods in order to diminish the noise in the image. The image enhancement methods used to enhance fingerprint image are normalization, orientation estimation, local frequency estimation, Gabor filtering, and thinning.

*1 Normalization*

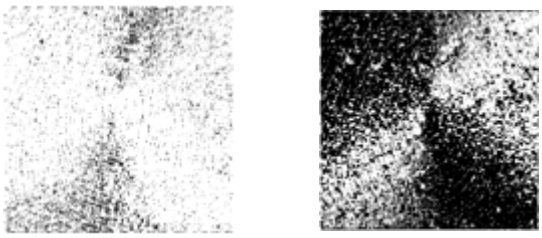
Normalization technique is nothing but the standardization of the intensity values in an image by altering the range of gray-level values with the intention that it occurs within a preferred range of values. Additionally the ridge structure in the fingerprint does not undergo any alterations in its structure because of this processing. This process is performed in order to standardize the dynamic levels of dissimilarity in gray-level values that assist the processing of subsequent image improvement processes. Figure 2 represents an image of the fingerprint before and after normalization.

(a) (b)

Figure 2. (a) Original Image (b) Image after normalization

*2 Orientation Estimation*

The orientation estimation is a necessary process in the improvement process as the successive Gabor filtering stage depends on the local orientation for the purpose of effectively improve the fingerprint image. Figure 3 (a) and 3 (b) indicates the outcome of orientation estimation and smoothed orientation estimation of the fingerprint image correspondingly. Other than the orientation image, another significant parameter that is utilized in the building of the Gabor filter is the local ridge frequency.



(a) (b)

Figure 3. (a) Orientation Image (b) Smoothened Orientation Image

*3 Gabor Filtering*

As the ridge orientation and ridge frequency parameters are determined, the even-symmetric Gabor filter [9] can be created with the help of those parameters. Gabor filters are engaged since they contain frequency-selective and orientation selective assets. These assets permit the filter to be adjusted to provide maximal response to ridges at a particular orientation and frequency in the fingerprint image. Hence, a appropriately adjusted Gabor filter can be utilized to successfully maintain the ridge structures during noise removal process. Figure 4 represents the outcome of applying Gabor filter to a fingerprint image.

Figure 4. Filtered Image

*4 Thinning*

The final image improvement pace normally performed before minutiae extraction is thinning [14]. Thinning is a morphological process that consecutively takes away the foreground pixels till they are one pixel apart. By applying the thinning technique to a fingerprint image maintains the connectivity of the ridge structures during the formation of a skeleton stage of the binary image. This skeleton image is subsequently utilized in the following extraction of minutiae. Figure 5 shows the results of thinning to a fingerprint image.

Figure 5. Thinned Image

*B. Minutiae Feature Extraction*

The next step is to obtain the minutiae from the thinned image. The most commonly used technique of minutiae extraction is the Crossing Number (CN) model. This process involves the utilization of the skeleton image in which the ridge flow pattern is eight-connected.

The minutiae are obtained by examining the local neighborhood of every ridge pixel in the image by means of a 3x3 window. The CN value is then calculated which is defined as partially the addition of the differences among the pairs of neighboring pixels in the eight-neighborhood. Figure 6 indicates the list of minutiae in a fingerprint image.

Figure 6. Minutiae extraction on a fingerprint image.

*C. Mapping Function*

The coordinate system utilized for the purpose articulating the minutiae point locations of a fingerprint is a Cartesian coordinate system. The X and Y coordinate of the minutiae points are in pixel units. Angles are represented in regular mathematical format, with zero degrees to the right and angles rising in the counter-clockwise direction. The obtained minutiae points are stored as below

$$F_1 = [x_1, x_2, \ldots x_n]$$

$$F_2 = [y_1, y_2, \ldots y_n]$$

**Feature Extraction from Iris**

*Iris Localization and Normalization:*

Canny edge detection is performed mutually in vertical direction and horizontal directions of the provided iris image. The radius of the iris image is determined and provided to the Hough transform. For better accuracy, the Hough transform is carried out initially for iris/sclera boundary and then for iris/pupil boundary. The outcome of this step results in storing the radius and x, y parameters of inner and outer circles.

Canny edge detection is utilized to build edges in horizontal direction and then Hough transform is applied on it. If the maximum Hough space is below the threshold then it indicates the non occlusion of eyelids. For isolating eyelashes it is very easy by utilizing thresholding. This is because they are darker while comparing with further elements in eye. The contrast of the eye image is improved with the help of histogram equalization.

Figure 7.Localized iris image

The normal Cartesian to polar transformation is recommended which maps all the pixel in the iris area into a pair of polar coordinates(r, θ), where r and θ represents the intervals of [0 1] and [0 2π ].

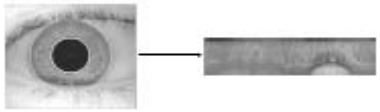
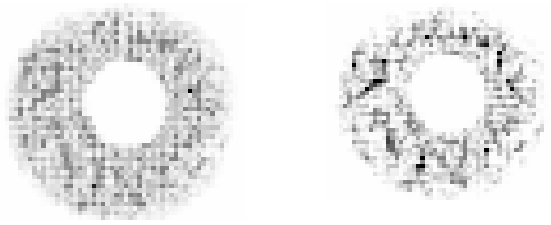


Figure 8. Normalized Iris

*D. Extraction of Lock/Unlock Data*

On the emphasized iris structures as a whole, the following order of morphological operations is utilized to mine the pseudo structures.

- Close - by - reconstruction top - hat (figure 9(a))
- Opening (figure 9(b)), area opening to remove structures in according to its size resulting image with structures disposed in layers (figure 9(c))
- Thresholding is applied to obtain binary image.



(a) Closing-by-tophat (b) Opening

(c) Thresholded images

Figure 9. Morphological operations on Iris Textures

For suitable depiction of structures, thinning is utilized so that it presents all the structure itself as an agglomerate of pixels. It is represented in figure 10.

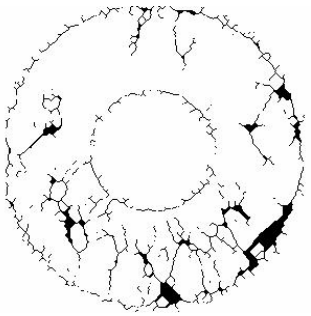


Figure 10. Iris textures after thinning operation

From the above iris rim containing iris pseudo textures, the polar coordinates of minutiae (nodes and end points of iris textures) are obtained by resizing the image into a standard format as represented in figure 11.

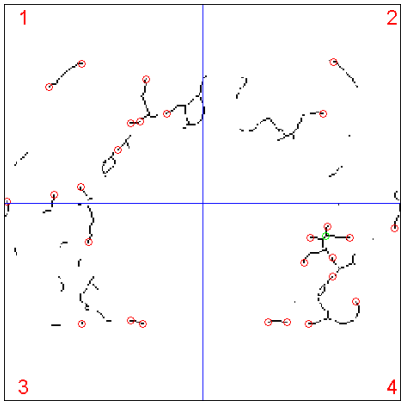



Figure 11. Minutiae representation of Nodes and end points are shown in circles.

These obtained Minutiae points are kept as

$$I_1 = [x_1, x_2, \ldots\ x_n]$$

$$I_2 = [y_1, y_2, \ldots\ y_n]$$

**Fusion of Biometric Features**

This phase will perform the fusion process for the gathered fingerprint and iris features. The input to the fusion process will be four vectors $F_1$, $F_2$, $I_1$ and $I_2$ which are obtained from fingerprint and iris. The steps involved in fusion of biometric feature vectors are as follows.

1. *Shuffling of Individual Feature Vectors*:

The initial step in the fusion process is the shuffling of all the individual feature vectors $F_1$, $F_2$, $I_1$ and $I_2$. The steps for performing shuffling of vector $F_1$ are as below,

i. A random vector R of size $F_1$ is created. The random vector R is controlled by the seed value.
ii. For shuffling the ith component of fingerprint feature vector $F_1$,
   a) The ith component of the random vector R is multiplied with a large integer value.
   b) The product value resulted is modulo operated with the size of the fingerprint feature vector $F_1$.
   c) The obtained value is the index say 'j' to be interchanged with. The components in the ith and jth indexes are interchanged.
iii. Step (ii) is repeated for all the component of F1. The shuffled vector F1 is indicated as S1.
This procedure is repeated for all other vectors F2, I1 and I2 and represent it as S1, S2 and S3 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 process is to concatenate the shuffled vectors process $S_1$, $S_2$, $S_3$ and $S_4$. In this process, the shuffled fingerprints $S_1$ and $S_2$ are concatenate with the shuffled iris features $S_3$ and $S_4$ correspondingly. The concatenation of the vectors $S_1$ and $S_3$ is performed as below:

i. A vector $M_1$ of size $|S_1| + |S_3|$ is generated and its initial $|S_3|$ values are filled with $S_3$.
ii. For all the components in $S_1$ ,
   a) The equivalent indexed component of $M_1$ say't' is selected.
   b) Logical right shift operation is performed in $M_1$ from index't'.
   c) The component of $S_1$ is inserted into the emptied tth index of $M_1$.
The above mentioned procedure is performed among shuffled vectors $S_2$ and $S_4$ to obtain a vector $M_2$. In this manner, the concatenation process yields two vectors $M_1$ and $M_2$.

3. *Merging of the Concatenated Feature Vectors*:

The final process in creating the biometric template $B_T$ is the merging of two vectors $M_1$ and $M_2$. The process for merging the concatenated feature vectors is provided below.

i. For all the 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 carried out among the components $M_{11}$ and $M_{21}$.
   c. The obtained binary value is then transformed back into decimal form.
ii. These decimal values are stored in the vector $B_T$ that serves biometric template.

### 3.2 Generation of Cryptographic Key from Fused Features

The final process of the proposed technique is the creation of the k-bit cryptographic key from the obtained biometric template $B_T$. The template vector $B_T$ can be indicated as,

$$B_T = [b_{T_1}\ b_{T_2}\ b_{T_3} \dots\ b_{T_h}]$$

The set of different components in the template vector $B_T$ are recognized and are stored in another vector $U_{BT}$.

$$U_{BT} = [u_1\ u_2\ u_3 \dots\ u_d]\ ;\ |U_{BT}| \leq |B_T|$$

The vector $U_{BT}$ is then resized to k components appropriate for creating the k-bit key. The resize procedure utilized in the proposed technique is

$$B = \begin{cases} [u_1\ u_1 \dots\ u_k], & if\ |U_{BT}| > k \\ [u_1\ u_1 \dots\ u_d] \ll u_i\ ; d+1 \geq i \geq k, & if\ |U_{BT}| < k \end{cases}$$

Where,

$$u_i = \frac{1}{d}\sum_{j=1}^{d} u_j$$

Finally, the key $K_B$ is created from the vector B,

$$K_B \ll B_i\ mod\ 2, i = 1,2,3, \dots k$$

This finally obtained key serves as an authentication key for the individual in the system. This key is definitely very difficult for the theft to generate. Therefore, a better secure system is created using the proposed technique. The evaluation for the proposed technique is provided in experimental result section.

## 4. Experimental Results

This section provides the evaluation of the proposed biometrics techniques. The fingerprint and iris are obtained from 100 persons are used for evaluation. Then the feature points are obtained from the gathered biometrics using the techniques presented in this paper. The biometrics features are obtained for fingerprint and iris separately. Then, these fingerprint features and iris features are combined using the technique fusion. The fusion process is carried out according the fusion method presented in this paper. Then the proposed system is evaluated using the parameters such as False Rejection Rate (FRR) and False Acceptance Rate (FAR)

Table 1: Average False Rejection Rate (FRR) (%) Comparison

| User | Fingerprint | Iris | Proposed |
|---|---|---|---|
| 1-10 | 92.9 | 89.5 | 85.6 |
| 11-20 | 92.1 | 89.6 | 84.6 |
| 21-30 | 93.6 | 89.9 | 85.1 |
| 31-40 | 94.5 | 92.1 | 86.2 |
| 41-50 | 92.8 | 90.6 | 86.7 |
| 51-60 | 89.6 | 87.6 | 84.2 |
| 61-70 | 90.6 | 89.4 | 83.5 |
| 71-80 | 92.7 | 90.9 | 84.1 |
| 81-90 | 91.1 | 90.1 | 85.6 |
| 91-100 | 91.6 | 89.2 | 85.1 |

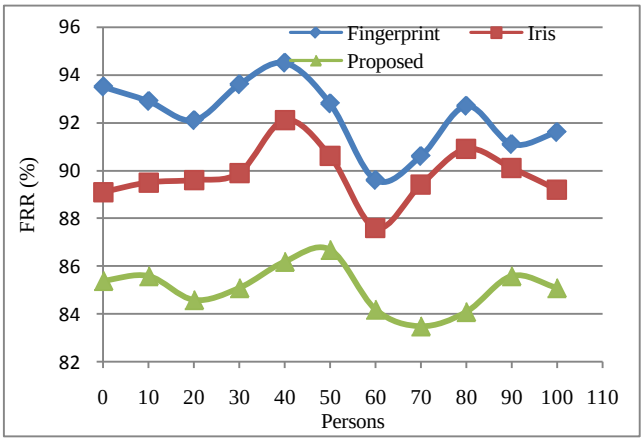



Figure 12. Resulted False Rejection Rate

Table 2 .False Acceptance Rate (FAR) (%) Comparison

| User | Fingerprint | Iris | Proposed |
|---|---|---|---|
| 1-10 | 0.45 | 0.39 | 0.11 |
| 11-20 | 0.42 | 0.38 | 0.12 |
| 21-30 | 0.43 | 0.39 | 0.09 |
| 31-40 | 0.39 | 0.38 | 0.11 |
| 41-50 | 0.38 | 0.37 | 0.08 |
| 51-60 | 0.39 | 0.37 | 0.08 |
| 61-70 | 0.44 | 0.41 | 0.09 |
| 71-80 | 0.41 | 0.38 | 1.02 |
| 81-90 | 0.39 | 0.37 | 1.12 |
| 91-100 | 0.40 | 0.39 | 0.98 |

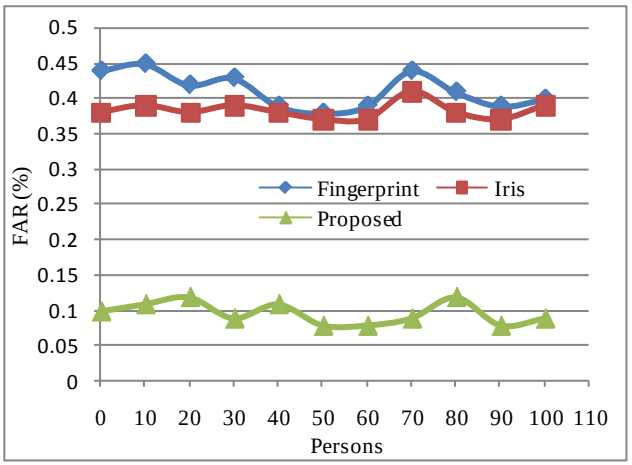



Figure 13. Resulted False Acceptance Rate

Table 1 and figure 12 shows the resulted False Rejection Rate (FRR) for the proposed and existing technique. From the result, it can be observed that the proposed technique results in lesser False Rejection Rate when compared to the existing technique. Table 2 and figure 13 shows the resulted False Acceptance Rate (FAR) for the proposed and existing technique. From the result, it can be observed that the proposed technique results in lesser False Acceptance Rate for all the persons, whereas the existing techniques results with higher percentage of False Acceptance Rate. From all the results obtained, it can be said that the proposed technique results in better security than the existing technique.

## 5. Conclusion

Securing the information system becomes most challenging task because of the increased number of theft. The conventional security system uses password or security key for authentication; but those password and security key can be easily stolen by the theft. To overcome these issues, biometrics of a person is used to secure the system. But, if the biometrics is stolen one time, it can be used by theft to access the system until it exists. This provides huge difficulty for the researchers to develop a new secure technique. One solution to this problem is usage of more than one biometrics for securing the system. This is because it is mostly impossible for the theft to steal more than one biometrics. This paper used fingerprint and iris biometrics to secure the system. The features obtained from these two biometrics are combined using fusion technique. From these fused features, cryptographic key is generated which is more secure than other techniques. The experimental result shows that the proposed security scheme results in better security than the existing techniques.

## References

[1] R. Ang, R. Safavi-Naini, L. McAven, “Cancellable key-based fingerprint templates," ACISP 2005, pp. 242-252.
[2] Announcing the Advanced Encryption Standard (AES), Federal Information, Processing Standards Publication 197, Nov. 26, 2001.
[3] Y. J. Chang, Z. Wende, and T. Chen, “Biometrics- based cryptographic key generation," IEEE International Conference on Multimedia and Expo, vol. 3, p. 2203-2206, 2004
[4] Chen, and V. Chandran, “Biometric Based Cryptographic Key Generation from Faces," Proceedings of the 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp. 394-401, 2007.
[5] T. Connie, A. Teoh, M. Goh, and D. Ngo, “ Palm hashing: A novel approach for cancellable biometrics," Information processing letters, vol. 93, no. 1, pp. 1-5, 2005.
[6] Feldmeier and P. Karn. “UNIX password security Ten years later," Advances in Cryptology Crytpo '89, LNCS 435, pp. 44-63, Springer-Verlag, 1990.
[7] Y. C. Feng, P. C. Yuen, and A. K. Jain, “A hybrid approach for face template protection," Proceedings of SPIE Conference of Biometric Technology for Human Identification, Orlando, USA, vol. 6944, pp. ca. 325, 2008.
[8] M. F. Santos, J. F. Aguilar, and J. O. Garcia, Cryptographic key generation using handwritten signature," Proceedings of SPIE, vol. 6202, pp. 225-231, Orlando, Fla, USA, Apr. 2006.
[9] Gabor Filter. (http://en.wikipedia.org/wiki/Gaborlter)
[10] F. Hao, R. Anderson, and J. Daugman, “Combining crypto with biometrics effectively," IEEE Transactions on Computers, vol. 55, pp. 1081-1088, 2006.
[11] L. C. Jain, U. Halici, I. Hayashi, S.B. Lee, and S.Tsutsui, “Intelligent Biometric Techniques in Fingerprint and Face Recognition”, CRC Press, 1999.
[12] J. G. Jo, J. W. Seo, and H. W. Lee, “Biometric digital signature key generation and cryptography communication based on fingerprint," First Annual International Workshop 2007, LNCS 4613, pp. 38-49, Springer Verlag, 2007.
[13] Klein, “Foiling the cracker: A survey of, and improvements to, password security," Proceedings of the 2nd USENIX Security Workshop, pp. 5-14, Aug. 1990.
[14] 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, pp. 879, Sep. 1992.
[15] B. Teoh, and C. T. Yuang, “Cancellable biometrics realization with multispace random projections," IEEE Transactions on Systems, vol. 37, no. 5, pp.1096-106, 2007.
[16] Alexander P. Pons, and Peter Polak, “Understanding user perspectives on biometric technology,” Communications of the ACM, vol. 51, no. 9, pp. 115-118, September 2008.
[17] N. K. Ratha, J. H. Connell, and R. M. Bolle “Enhancing security and privacy in biometrics based authentication systems”, IBM Systems Journal, vol. 40, pp. 614-634, 2001.
S. C. Chong, A. B. J. Teoh, and D. C. L. Ngo, “Iris Authentication Using Privatized Advanced Correlation Filter,” in ICB, pages 382–388, 2006

**P.Balakumar** received the B.E. and M.E. degrees in Computer Science and Engineering from PSG College of Technology, Coimbatore, in 1997 and Anna University, Chennai in 2004 respectively. During 1999-2001, he worked as Lecturer in PSG College of Technology in Coimbatore. Later during 2003-2008, he worked as Lecturer & Assistant Professor in AMS Engineering College, Namakkal.
He now with Selvam College of Technology, Namakkal, Tamilnadu, India as Associate Professor in Department of Computer Science and Engineering.

**Dr.R. Venkatesan** was born in Tamilnadu, India, in 1958. He received his B.E (Hons) degree from Madras University in 1980. He completed his Masters degree in Industrial Engineering from Madras University in 1982. He obtained his second Masters degree MS in Computer and Information Science from University of Michigan, USA in 1999. He was awarded with PhD from Anna University, Chennai in 2007. He is currently Professor and Head in the Department of Information Technology PSG College of Technology, Coimbatore, India. His research interests are in Simulation and Modeling, Software Engineering, Algorithm Design, Software Process Management.