# Performance of Iris Based Hard Fuzzy Vault

**E. Srinivasa Reddy[1], I. Ramesh Babu[2]**

[1]Research Scholar, [2] Professor
Department of Computer Science and Engineering, Acharya Nagarjuna University, Guntur, A.P., India

**Summary**

Blend of cryptography and biometrics results an emerging architecture known as Crypto-biometrics which produces high level security. Fuzzy vault is a cryptographic construction used to store iris biometric templates which are binded by a random key extracted from same iris textures. Though the fuzzy vault provides better security, it is affected by cross matching, non uniform nature of biometric data. To overcome these limitations, we propose a scheme that hardens both fuzzy vault and secret key using password. By using password an additional layer of security is embedded to achieve high level security.

***Key words:***
*Crypto-biometric, fuzzy vault, hardening, morphological operations, chaff point.*

## 1. Introduction

Independently both biometrics and cryptography play a vital role in the field of security. A blend of these two technologies [1] can produce a high level security system, known as biometric crypto system that assists the cryptography system to encrypt and decrypt the messages using bio templates.

There are two ways to merge these two technologies,

1. Biometric based key release: Cryptographic key generation is decoupled with biometric matching. If a biometric match is done, key is released e.g., smart card.
2. Biometric key generation: Here both biometrics and cryptography are combined together. No separate matching operation is needed to extract the key.

But when combining these two technologies, there is a large gap regarding exact presentation of data by the bio templates used for generation of keys. Digital signatures require crisp keys, but due to noise bio templates produce only fuzzy data. Also biometric data are not secret. Even knowledge from biometric systems is exact, transmission channels may introduce noise which leads to fuzziness. Also fuzziness can come from the variability of biometric data. Same biometric template is analyzed during different acquisitions; extracted biometric data will vary and cause fuzziness. This gap can be easily filled up by iris textures as bio metric templates. They are less prone to noise when compared to other bio templates and also their unique texture give rise to high level security.

Current cryptographic algorithms require their keys to be very long and random for higher security, that is, 128 bits for Advanced Encryption Standards [2]. These keys are stored in smart cards and can be used during encryption/decryption procedures by using proper authentication. There are two major problems with these keys: One is their randomness. The randomness provided by current mathematical algorithms is not sufficient to support the users for commercial applications. The second is authentication. Most of the authentication mechanisms use passwords to release the correct decrypting key, but these mechanisms are unable to provide non-repudiation.

Considering all the above issues it is felt that, cryptographic systems must accept some fuzziness regarding witness i.e., it must be decrypted by a key that is nearer to encryption key. A fuzzy extractor addresses both error tolerance and non uniformity. Fuzzy vault is such a construction used to store the secret key based on iris bio templates.

### Fuzzy Vault

Fuzzy vault [3] is a cryptographic frame work designed using biometric features which are represented as an unorder set of genuine points (i.e., minutiae in iris pseudo textures) and chaff points. Polynomial reconstruction problem which is a special case of Reed-Solomon list decoding problem is the basis for the security provided by this fuzzy vault. One of the major of fuzzy vault is dealing the intra class variations in the biometric data and working with unordered sets.

If a user wishes to hide a secret key S (e.g., digital signature obtained from his biometric template) using his biometric sample which is represented as unorder set U. A polynomial P is generated by encoding S and evaluated by using all elements of U. Further random chaff points which are not on the polynomial are added to

Manuscript received January 5, 2008
Manuscript revised January 20, 2008

constitute the vault V. The chaff points conceal the genuine points lying on P from an attacker. Since the points lying on P encode the complete information about the template U and secret key S, concealing these points secures both template and the secret key simultaneously.

While decoding the secret key S can be retrieved from the vault by providing query template. Let the query template is represented by another unordered set U'. If U' overlaps substantially with U, then the user can identify many points in V that lie on P. If sufficient number of points on P can be identified, an error correction scheme can be applied to exactly reconstruct P and thereby decode the secret keys. If U' does not overlap substantially with U, it is infeasible to reconstruct P and the authentication is unsuccessful. Since the secret key can be retrieved from the vault even when U and U' are not exactly same but very near, this scheme is referred to as a fuzzy vault.

a) Performance of Fuzzy Vault:

The performance of the vault depends on three parameters, they are g,c,d. The parameter g denotes the number of points in the vault that lie on the polynomial P and it depends on the number of features that can be extracted from the template. The parameter c represents the number of chaff points that are added and this parameter influences the security of the vault. If no chaff points are added, the vault reveals the information about the template and the secret key. As number of chaff points increases, degree of security increases. Parameter d denotes the degree of polynomial and it controls the tolerance of the system to errors in bio data.

b) Polynomial Interpolation:

To unlock the vault and retrieve the secret key a subset of g points from V which is known as unlocking set is selected from a query template U'. The simple mechanism for recovering the polynomial is a brute force search. The second method is Reed-Solomon decoding algorithm suggested by Juels and Sudan. There are two main RS decoding algorithms: Berlekamp Massey [4] requires more than $\frac{g+d}{2}$ points for unlocking while Guruswami-Sudan [18] requires only √gd points. Both the algorithms has same unlocking complexity. If the number of discrepancies in the bio data |U-U'| is less than $\frac{g-d}{2}$ a valid polynomial P can be found and secret key S can be successfully retrieved.

The ideal Galois field for the vault is given by $F_{p^2}$ , where p is prime. For a reasonable vault parameters, there exists a δ with d<= δ<=g such that the expected number of spurious degree d polynomials interpolated by more than δ points will yield a unique result, namely the vault is secret [16].

Where the value of δ satisfying the above requirement is given by

$$\delta = \left[ \frac{\log \frac{1}{3} p^{2d}}{\log \frac{d p^{2}}{t}} \right]$$

If the vault size is small, approximately δ = d+1.

**Limitations of Fuzzy Vault**

Fuzzy vault scheme proposed in the previous chapter has following limitations [5]

1. If the same biometric data is used for constructing different vaults with different polynomials and random chaff points, the genuine points can be easily identified by correlating the abscissa values from different vaults. Thus if a vault is compromised, a new vault cannot be created from the same biometric data binding with a different key.
2. Since the number of chaff points in the vault is much larger than the number of genuine points, it is possible for an attacker to substitute few points using his own features. Therefore the vault can be authenticated by both original user and also attacker using same identity. This increase false accept ratio.
3. The non uniformity nature of the biometric features can be exploited by the attacker and can develop attacks based on statistical analysis of points in the vault.
4. As a genuine user is being authenticated, his original template is exposed temporarily, which may be gleaned by an attacker.

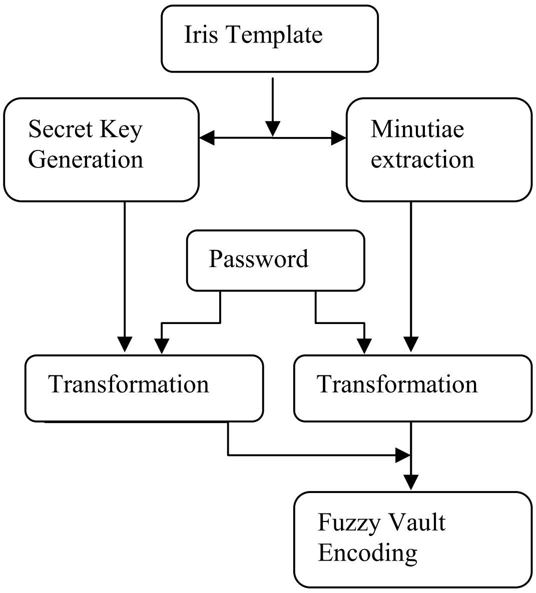
**Hardening the Fuzzy Vault**

To overcome the above limitations, the fuzzy vault is hardened by using user's password. Password is an additional layer of authentication provided and the security provided by the basic fuzzy vault is not affected even if the password is compromised. This scheme

This study has been implemented on windows platform using MATLAB software at Computer Science Laboratory, Acharya Nagarjuna University, India.

provides high level security until the password is secure. If password is compromised, it is same as that of ordinary fuzzy vault. The same password is also used to harden the secret key extracted from same template.

The hardening scheme consists of following steps, a random transformation function derived from the user password is applied to the biometric template. The transformed template is then secured using the fuzzy vault frame wok. Finally the vault is encrypted using a key derived from the password.



The remainder of the paper is organized as follows: Section-2 focuses on background and survey of related work. Section-3 gives a brief outline of proposed method. Section-4 describes feature extraction techniques, where as Section-5 describes implementation of proposed algorithm. Setion-6 gives results and Section-7 brings out conclusions.

## 2. Background

Many approaches are in existence to protect the biometric templates..

(a) Using Encryption Techniques:

The biometric template can be encrypted using any one of the advanced cryptographic algorithms. This does not affect accuracy in any degree but the template is exposed every time during authentication and it can be easily stolen by attacker.

(b) Using Non invertible transform functions:

This method was proposed by Ratha, N.,[6], using one way function to transform the biometric features. The transformation occurs in the same feature space and matcher need not be redesigned. But the algorithm leads to increase in the FRR.

( c) Using Secure Sketch:

Dodis. Y [7] proposed a method to derive a sketch from the biometric template. The sketch is secure because the template can be reconstructed only if a matching biometric query is presented. This method is more tolerant to intra user variations in biometric data. Also it can be used for securing external data such as cryptographic keys. But at the same time non uniform nature of the biometric data reduces the degree of security.

(d) Generating key from Biometric data:

Monrose, F., [8] proposed generating cryptographic key directly from the biometric features. It is more efficient and scalable approach. But the tolerance to intra user variations is limited resulting in high FRR.

(e) Using Salting:

Tech. A.B.J.,[9] method involves in adding user specific external randomness to the biometric features. This increases the entropy of biometric features resulting in low FAR. At the same time if user compromises at his random information then the entropy gain decreases.

(f) Using Error correcting Codes:

Feng hao [10] method shows how to generate keys robustly from iris biometric measurements, using associated error correction data that can be changed to yield different keys. It can produce different keys for different application, so that an attack on one does not given an attack on all. It supports revocation and FRR is less than half a percent. Since passwords can be easily compromised by using social engineering techniques, security level falls. Also template can be exposed and it can be used in other applications.

## 3. Proposed Method

The proposed work has three stages. In the first stage the biometric template is undergone random transformation using the password. This enhances the privacy because it enables the creation of revocable templates and prevents cross matching of templates across different applications. The transformed template is also statistically more similar to uniform distribution and similarity between transformed templates decreases.

In the second stage the transformed template is protected using fuzzy vault. Password based transformation alone is no sufficient to ensure the security of the biometric template. Thus fuzzy vault is used to secure the template. The key used in constructing the fuzzy vault that secures the transformed template is also derived from the iris textures and transformed using same password. Finally vault is encrypted using the key derived from the password.

## 4. Extraction of Minutiae and Secret Key

### Iris Localization and normalization

We use the iris image data base from CASIA Iris image Database [CAS03a] and MMU Iris Database [MMU04a]. CASIA Iris Image Data base contributes a total number of 756 iris image which were taken in two different time frames. Each of the iris images is 8-bit gray scale with resolution 320 X 280. MMU data base contributes a total number of 450 iris images which were captured by LG Iris Access®2200.

Canny edge detection is performed both in vertical direction and horizontal directions as suggested by Wildes et a [11]. The iris images in CASIA database has iris radius 80 to 150 and pupil radius from 30 to 75 pixels, which were found manually and given to the Hough transform. If we apply Hough transform first for iris/sclera boundary and then to iris/pupil boundary then the results are accurate. The output of this step results in storing the radius and x, y parameters of inner and outer circles.

Canny edge detection is used to create edges in horizontal direction and then Hough transform is implemented on it. If the maximum Hough space is less than the threshold it represents non occlusion of eyelids. For isolating eyelashes it is easier by using thresholding, since they are darker when compared with other elements in eye. The eye images collected from the above database are of gray scale and their contrast is enhanced using histogram equalization.

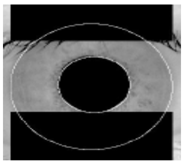


Figure 1 Localized iris image

Daugman [12] suggested normal Cartesian to polar transformation that maps each pixel in the iris area into a pair of polar coordinates$(r,\theta)$, where r and $\theta$ are on the intervals of [0 1] and [0 2∏ ] .

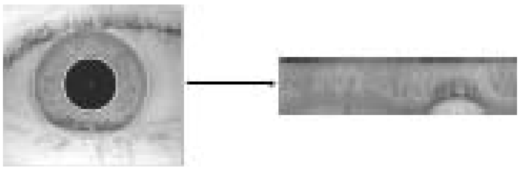


Figure 2 Normalized Iris

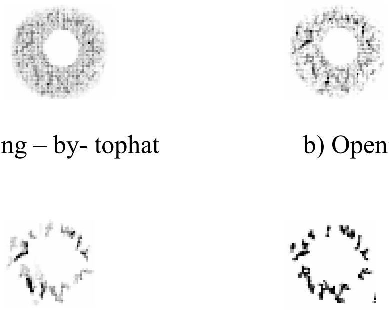
### Generation of Secret Key

A typical iris exhibits rich texture information in the immediate vicinity of the pupil which tapers away in intensity as one move away from the pupil. Similarly there is a chance of having noise in iris patterns at top an bottom rows even after preprocessing. Also the iris pixels near the pupil have more variations than those of farther from the pupil. Thus after leaving 3 rows of patterns both at bottom and top, remaining rows are sued to extract the key.

### Extraction of Lock/Unlock Data

On the highlighted iris structures as a whole, the following sequence of morphological operations [13] is used to extract the pseudo structures.

Close – by - reconstruction top-hat (figure 3(a)) opening (figure 3(b)), area opening to remove structures in according to its size resulting image with structures disposed in layers (figure 3 (c)) and thresholding is applied to obtain binary image.



(a) Closing – by- tophat b) Opening

c) Thresholded images

Figure 3 Morphological operations on Iris Textures

For appropriate representation of structures, thinning is used so that every structure presents itself as an agglomerate of pixels as shown in figure 4.

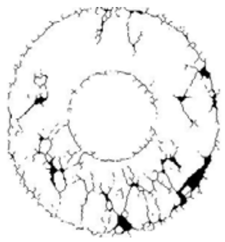
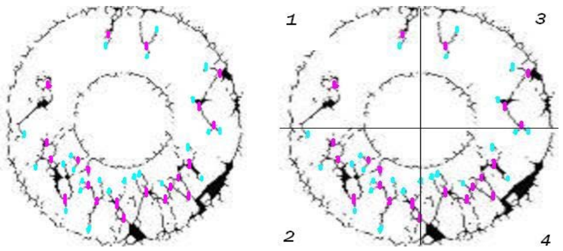


Figure 4 Iris textures after thinning operation

From the above iris rim containing iris pseudo textures, the polar coordinates of minutiae (nodes and end points of iris textures) are extracted by resizing the image into a standard format of 256 x 256 as shown in figure 5.



(a) (b)

Figure 5 Minutiae representation a) Nodes are shown in pink dots and end points are shown in blue dots b) Iris rim divided into 4 quadrants

## 5. Implementation

The implementation stage carries three operations, one is transformation, second one is encoding and finally decoding.

(a) Transformation:

Simple operations such as translation and permutation are used to transform the original minutiae features into new minutiae. The password given by the user is limited to 8 characters so that its length is 64 bits, which is divided into 4 blocks of each 16bits length.

Similarly iris circular rim containing minutiae is divided into 4 quadrants as shown in figure 6(a) and for each quadrant one password block is assigned. The 4 quadrants are permuted such that relative positions of the minutiae within each quadrant are not changed as shown in figure 6(b).

Each password block is divided into two components $T_r$ of 7 bits and $T_\theta$ of 9 bits length. Where $T_r$ is the translation in radial direction and $T_\theta$ is in angular direction. These translation values are added to original values modulo the appropriate range

$$Q_r^{'} = (Q_r + T_r)\,\mathrm{mod}(2^{\wedge}7)$$

$$Q_\theta^{'} = (Q_\theta + T_\theta)\,\mathrm{mod}(2^{\wedge}9)$$

where $Q_r^{'}$ is the radial value after transformation and $Q_r$ is before transformation. Similarly $Q_\theta^{'}$ and $Q_\theta$ are angular values after and before transformation respectively.

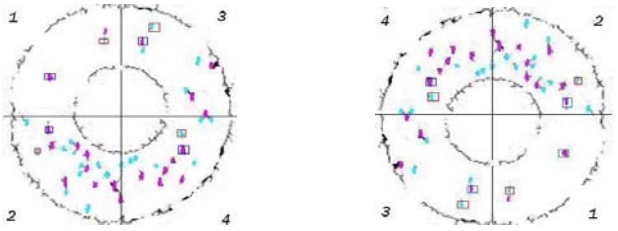


Figure 6 a) Minutiae before permutation b) Minutiae after permutation

(b) Encoding:

The transformed minutiae are encoded in the vault using the same procedure that is described earlier section. This layer of encryption prevents an imposter without knowledge of the password from modifying the vault.

(c ) Decoding:

During authentication phase, the encrypted vault and the minutiae data are decrypted using the password given by the user. The template and query data sets are aligned and the password based transformation is applied to these query minutiae and used for unlocking the vault.

**Parameters used in implementation**

The parameter used in our implementation is shown in Table 1. The choice of the polynomial degree depends upon the size of secret key. For a degree d=8, the secure key size is 128 bits. Since the number of minutiae varies for different users, using a fixed value of genuine points for all users may reduce accuracy. This can be overcome by using more number of chaff points, approximately 10 times the number of genuine points in the vault.

| Parameter | Size |
|---|---|
| Number of genuine points, g | 18-20 |
| Degree of polynomial, d | 6-8 |
| Total number of points in the vault, t | 120-220 |
| Number of chaff points, c | 100-200 |

Table 1 Parameters used for Fuzzy vault implementation

## 1. 6. Results and Analysis

The polar indices $Q_r$ (radial value) and $Q_\theta$ (angular value) of nodes and end points are used for projections of the polynomial. Nodes and end points are shown in the Figure 6 which was obtained after a sequence of morphological operations.

| Quadrant | Iris Feature | Distance $Q_r$ (7-bits) | Orientation $Q_\theta$ (9-bits) | Minutiae value (16-bits) |
|---|---|---|---|---|
| I | Node | 97 | 77 | 1100001<br>001001101 |
|  | End point | 108 | 71 | 1101100<br>001000111 |
| II | Node | 90 | 150 | 1011010<br>010010110 |
|  | End point | 90 | 103 | 1011010<br>001100111 |
| III | Node | 83 | 250 | 1010011<br>011111010 |
|  | End point | 62 | 247 | 0111110<br>011110111 |
| IV | Node | 98 | 312 | 1100010<br>100111000 |
|  | End point | 53 | 288 | 0110101<br>100100000 |

Table 2 Some of the minutiae used to lock the Vault

Using these indices, genuine points are generated to which chaff points are added later to form the vault. The ratio of chaff points and original points is taken as 10:1 so that the combinations are large in giving high security. During decoding 20 query points are selected on the average. Out of 100 iris templates, 92 are successful in unlocking the vault. Hence False Rejection Rate (FRR) of the system is 0.08 that is genuine acceptance ratio is 92% which is considerably higher than the other biometric templates such as finger prints which is79% [14].

Consider a user password **'template'** of 8 characters (whose ASCII value is given by 116, 101, 109, 112, 108, 97, 116, 101) or 64 bits which are divided into 4, 16 bit codes used for transformation of minutiae in each quadrant. In each 16 bit code first 7 bits are used to transform the distance and remaining 9 bits for orientation.

| Quadrant | Minutiae before transformation | | Transformation code from password | | Minutiae after Transformation | |
|---|---|---|---|---|---|---|
| | Distance $Q_r$ | Orientation $Q_\theta$ | $T_r$ | $T_\theta$ | Distance $Q_r'$ | Orientation $Q_\theta'$ |
| I | 97 | 77 | 58 | 101 | 27 | 178 |
|  | 108 | 71 | 58 | 101 | 38 | 172 |
| II | 90 | 150 | 54 | 368 | 16 | 6 |
|  | 90 | 103 | 54 | 368 | 16 | 215 |
| III | 83 | 250 | 54 | 97 | 9 | 91 |
|  | 62 | 247 | 54 | 97 | 52 | 88 |
| IV | 98 | 312 | 58 | 101 | 28 | 157 |
|  | 53 | 288 | 58 | 101 | 47 | 133 |

Table 3 Minutiae after Transformation

If the number of minutiae in the given template is less than required number of genuine points required then it is said to be failure to capture (FTCR). The range of the genuine minutiae is not fixed and ranges from 10-20 times that of genuine points in the vault Table shows that there is a small decrease in the GAR for all values of d after hardening. This is due to misclassification of a few minutiae at the boundaries of quadrants. At the same time FAR is zero for all values of d. This is due to the transformation of minutiae using password which makes the distribution of minutiae more random and reduces the similarity between minutiae.

| Degree of Polynomial, d | Without Hardening | | With Hardening | |
|---|---|---|---|---|
| | GAR (%) | FAR (%) | GAR (%) | FAR (%) |
| 4 | 87.2 | 0.26 | 84 | 0 |
| 5 | 90.1 | 0.16 | 87 | 0 |
| 6 | 91.4 | 0.11 | 89.7 | 0 |
| 7 | 92.2 | 0.07 | 90.4 | 0 |
| 8 | 92.0 | 0.03 | 90.2 | 0 |

Table 4GAR and FAR before and after hardening

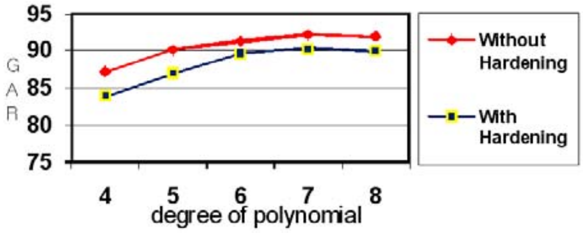


Figure 7GAR vs degree of polynomial before and after hardening

The performance of the approach is measured in terms of FRR/GAR and FAR with respect to degree of polynomial. As the degree of polynomial d increase the FRR must increase, but it has a slight decrement when compared to that of without hardening. This is due to misclassification of minutiae present near the boundaries. FAR is zero for all d. This is due to random distribution of minutiae which reduces similarity between different user sets.

## 7. Conclusion

Hardening the fuzzy vault system has tow layers of security, namely password and biometric. When an imposter gains access to the password, he can at most generate the decryption key to decrypt the vault. But to successfully authenticate he must decode the vault by identifying genuine minutiae points. This is very hard for computation. If he used brute force technique, the vault has 220 points, hence there are a total of C(220,9) = 2.8 x $10^{15}$ combinations with 9 elements. Only C(20,9) = 167960 of these are used to open the vault. Therefore, it takes C(220,9)/C(20,9) = 1.67 x $10^{10}$ evaluations for an attacker to open the vault. A better transformation technique can be proposed by introducing non-invertible transforms for hardening.

## References

[1] J.Daugman, "Combining Cryptography and Biometrics," Technical Report No.640, University of Cambridge Computer Laboratory, 2000.

[2] NIST, Advanced Encryption Standard (AES), 2001. http://csrc.nist.gov/publications/fips/fips-197.pdf

[3] A. Juels and M. Sudan, "A Fuzzy Vault Scheme",Proceedings of IEEE International Symposium Information Theory, pp.408, 2002.

[4] Massey J L, "Shift register synthesis and BCH decoding," IEEE Transactions on Information Theory, Vol. 15, 1969.

[5] Karthik Nandakumar, Abhishek Nagar and Anil K. Jain, "Hardening Fingerprint Fuzzy Vault using Password", International Conference on Biometrics, pp.927-938, 2007.

[6] Ratha N K, Connell J H, and Bolle R M, "An Analysis of Minutiae Matching Strength," Proceedings of Audio and Video Based Biometric Person Authentication, Sweden, 2001.

[7] Dodis Yevgeniy, Reyzin Leonid, and Smith Adam, "Fuzzy Extractors: How to generate Strong Keys from Biometrics and other Noisy Data", Proceedings of International Conference on Theory and Applications of Cryptographic Techniques, pp. 523-540, 2004.

[8] F. Monrose, M. Rieter, Q. Li. S. Wetzel," Password hardening using key board dynamics", Proceedings of ACM conference on Computer and Communications security, pp.73-82, 1999.

[9] Tech A B J, Goh A and Ngo D C L., " Random Multispace Quantization as an Analytic Mechanism for Bio Hashing of Biometric and Random Identity Inputs", IEEE Transactions on Pattern Analysis and Machine Intelligence, 2006.

[10] Feng Hao, Ross Anderson, and Daugman J, "Combining Cryptography with Biometrics Effectively", Technical report, No. 640, University of Cambridge, 2005.

[11] R. Wildes, "Iris Recognition: An Emerging Biometric Technology", Proceedings of the IEEE, vol. 85, pp 1348-1363, 1999.

[12] J. Daugman, "How iris recognition Works," in IEEE Transactions on Circuits and Systems for video Technology, vol.14, no.1, pp21-30, January 2004.

[13] H. Heijmans, Morphological Image Operators, Academy Press, 1994.

[14] Uludag U, Pankanti S, and Anil Jain K " Fuzzy Vault for Finger prints", Proceedings of International Conference on Audio Video Based Person Authentication, pp. 310-319, 2005.

[15] Joaqum Mira Jr., Joceli Mayer," Image Feature Extraction for application of Biometric Identification of Iris-A morphological approach", proceedings of the XVI Brazilian Symposium on Computer Graphics and Image Processing, 2003.

## Authors

**Srinivas R.E.** received the B.Tech degree in Electronics & Communication Engienering from Nagarjuna University, India in 1988, M.S. degree from Birla Institute of Technology and Scince, India in 1997, M.Tech degree in Computer Science from Visveswaraiah Technological University, India in 2000 and submitted his Ph.D in computer science in Nagarjuna Univeristy under the guidance of Dr. I. Ramesh Babu. He is the member of IEEE and presented 9 papers in international conferences and one journal paper. His research interests includes image processing, biometrics and pattern recognition

**Ramesh Babu.I** received the B.Tech degree in Electronics & Communication Engineering from Mysore University, India in 1981, M.Tech degree in Computer Engineering from Andhra University, India in 1984 and Ph.D degree in computer Science & Engineering from Nagarjuna University, India in 1994. He is currently working as Head & Professor in the department of computer science, Nagarjuna University. Also he is the senate member of the same University from 2006. His areas of interest are image processing & its applications, and he is currently supervising 10 ph.D students who are working in different areas of image processing. He is the senior member of IEEE, and published 35 papers in international conferences and journals.