©2010 International Journal of Computer Applications (0975 - 8887)
Volume 1 – No. 29

Retina and Iris Based Multimodal Biometric Fuzzy Vault

V.S.Meenakshi
Department of Computer Applications,.
S.N.R. Sons College,Coimbatore,Tamilnadu
India

Dr. G. Padmavathi
Department of Computer Science,,
Avinashilingam University for women,
India

ABSTRACT

Biometric authentication technology is gaining much importance as it serves as a powerful alternative for traditional password based authentication. In the current scenario securing the biometric template against attack is an important issue. Fuzzy vault is a proven biometric crypto system that is used to protect biometric templates and secret data. Multi biometric systems are more secure compared to their single biometric counterparts. In this work, fuzzy vault framework is used to secure both retina and iris template. Retina and iris can be used in high security applications like access control, military applications, border security control. The proposed multimodal fuzzy vault is constructed with feature points extracted from retina and iris. Combination of retina and iris enhances the user convenience as they can be captured from the user by the same device. This work measures the security of the resultant vault by using min-entropy.

Keywords

Biometrics, Multi Biometrics, Fuzzy Vault, Multi Biometric Fuzzy Vault, Biometric Template Security, Min-Entropy, Crypto Biometric Systems

1. INTRODUCTION

The biometric cryptography system utilizes the advantages of both biometrics and cryptography for ensuring high security. Biometrics and cryptography can be combined in two methods namely Biometric based key release and Biometric based key generation.

Biometric based key release method involves the separation of biometric matching from cryptography. If the biometric templates are matched successfully then cryptography key is released, eg. smart card. In this example biometrics play the role of a wrapper.

In biometric based key generation method, biometrics and cryptography are combined together at a much higher level. Here the secret key is extracted from the combined key and biometric template. The fuzzy vault is a biometric based key generation cryptographic construct.

A. *Fuzzy vault*

Fuzzy vault is a cryptographic construct proposed by Juels and Sudan[2]. This construct is more suitable for applications where biometric authentication and cryptography are combined together. Fuzzy vault framework thus utilizes the advantages of both cryptography and biometrics. Fuzzy vault eliminates the key management problem as compared to other practical cryptosystems

In fuzzy vault framework the secret key S is locked by G, where G is an unordered set from the biometric sample. A polynomial P is constructed by encoding the secret S. This polynomial is evaluated by all the elements of the unordered set G.

A vault V is constructed by the union of unordered set G and chaff point set **C** which is not in G**.**

$$V = G \cup C$$

The union of the chaff point set hides the genuine point set from the attacker. Hiding of the genuine point set secures the secret data S and user biometric template T.

The vault is unlocked with the query template T**'.** T**'** is represented by another unordered set U**'**. The user has to separate sufficient number of points from the vault V by comparing U**'** with V. By using error correction method the polynomial P can be successfully reconstructed if U**'** overlaps with U and secret S gets decoded**.** If there is not substantial overlapping between U and U**'** secret key S is not decoded. This construct is called fuzzy because the vault will get decoded even for very near values of U and U**'** and the secret key S can be retrieved. Therefore fuzzy vault construct become more suitable for biometric data which show inherent fuzziness hence the name fuzzy vault as proposed by Sudan[2].

The security of the fuzzy vault depends on the infeasibility of the polynomial reconstruction problem. The vault performance can be improved by adding more number of chaff points C to the vault.

1.1 B. Advantages of retina

Retinal scan captures the pattern of blood vessels in the eye. Retina as a biometric has certain merits compared to other biometrics. It is highly secure and uses a stable physiological trait. Retina is very difficult to spoof. Retinal patterns are different for right and left eye. They are unique even for identical twins. More over, retinal patterns do not change with age. Unlike other biometric traits, the image will not fall on the retina for dead person. Retina is located deep within ones eyes and is highly unlikely to be altered by any environmental or temporal conditions. Therefore retina is best suited biometric for high security systems. In this work, retina and iris features are combined together to construct the vault. Both retina and iris can be captured using the same device to enhance user convenience.

B. Multimodal Fuzzy Vault

Multimodal fuzzy vault performs well compared to the traditional unibiometric systems [5]. Multibiometrics provides better recognition accuracy, enhances very high security, flexibility and user convenience [14,15]. It can be used in applications like financial transactions, for securing secret cryptographic keys, email communications etc.

Biometrics templates are not revocable when compromised like passwords [13]. A template represents a set of salient features that summarizes the biometric data of an individual. A compromised template would mean the loss of a user's identity [10, 11]. A potential abuse of biometric identifiers is cross-matching [12]. Therefore biometric template security is very crucial to protect user privacy. It is very difficult for an attacker to compromise multibiometric modalities.

The proposed multimodal fuzzy vault contains point set from two different biometric modalities say Fingerprint and Iris namely K_f and K_i. Then chaff points are added to the vault to conceal the genuine points.

$$V = (K_f \cup K_i \cup C)$$

The chaff points are generated in such a way that they do not lie on K_f and K_i.

In this proposed vault the secret **S** is locked by two unordered sets U_f and U_I.

The organization of the paper is as follows: Chapter 2 elaborates on background study of the construction and operation of fuzzy vault. Section 3 explains the proposed operations and implementation of the multimodal biometric fuzzy vault. Section 4 discusses the experimental results and the security analysis of the vaults. Section 5 concludes the outcome of the proposed vault.

The following Table1 shows the notations used.

Table1. Notations Used.

Notations	Meaning
S	Secret Key
SC	Secret Key + Cyclic Redundancy Code (CRC)
G	Genuine set
C	Chaff set
VS	List Scrambled Vault
SC*	SC Generated after Decoding
Q	Query Template

2. BACKGROUND

Umut uludag et al [1] used the concept of fuzzy vault to protect a secret S of 128 bits length. The x and y coordinate of the fingerprint minutiae are used as the locking/unlocking unit u (x|y) of the vault. The secret key S (128 bits) is added with its CRC code (16 bit) to obtain SC (144 bits). SC is divided into 16 bit segments to obtain the polynomial coefficients. Two sets namely the Genuine set (G) and chaff set (C) are generated.

$$G = [(u_1, p(u_1)), (u_2, p(u_2)), \ldots\ldots (u_N, p(u_N))].$$
$$C = [(c_1, d_1), (c_2, d_2) \ldots\ldots (c_m, d_m)].$$
$$c_i \neq u_i, (j = 1,2,\ldots\ldots M, i = 1,2,\ldots\ldots N)$$
$$d_i \neq P(c_i), j = 1,2,\ldots\ldots M.$$
$$VS = \text{Listscrambled}(G \cup C)$$

During decoding, query minutiae set (Q) is compared with the vault to isolate the genuine point set. These points are used to reconstruct the polynomial. The coefficients are mapped back and SC* is obtained. SC* is divided by the CRC primitive polynomial. If the Remainder is not zero, Query template (Q) does not matches and the secret decoded is not correct. If the Remainder is zero, Query Template (Q) matches and the Secret(S) is decoded successfully.

The security of the fuzzy vault depends on the infeasibility of the polynomial reconstruction and the number of chaff points. Using this construct 128 bit secret data like Advanced Encryption Standard (AES) key can be protected.

Karthick Nandakumar et al [5] implemented the finger print fuzzy vault in which minutiae orientation attributes (helper data) can also be considered along with location. This facilitates to add more chaff points whose location is near but with a different direction that of the true minutiae. The work of Karthick Nandakumar [5]

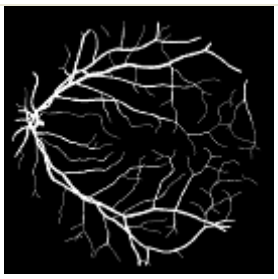
concluded that the performance of the fuzzy vault can be further improved by using multiple biometric sources (multiple fingerprint) or multiple modalities (fingerprint and Iris).

Iris based hard fuzzy vault proposed by Srinivasa Reddy [3] applies a sequence of morphological operations to extract minutiae points from the iris texture. This idea is utilized in the proposed multi biometric fuzzy vault for extracting the locking/unlocking unit from the iris.

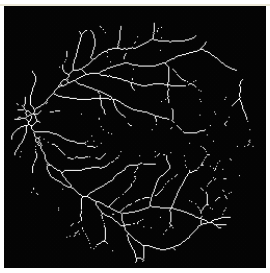
3. PROPOSED METHOD

The proposed work constructs three different fuzzy vaults. Two unibiometrics fuzzy vaults are constructed using the features extracted from retina and iris separately. Then a combined multimodal fuzzy vault is constructed with feature points from both retina and iris.

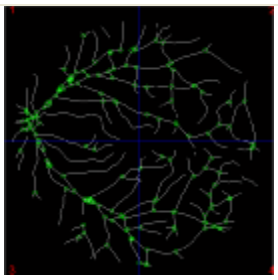
(a) Retinal image



(b) Retinal vascular tree



(c) Thinned and joined image.



(d)Highlighted Bifurcation feature

Fig 1. Retina Feature Extraction

The proposed work is carried out in the following steps.

1. Feature extraction from retinal template.
2. Implementation of unibiometric retina based fuzzy vault.
3. Feature extraction from iris template.
4. Implementation of unibiometric iris fuzzy vault.
5. Implementation of multimodal biometric fuzzy vault using the features extracted from both retina and iris.

Implementation of the vault includes the encoding and decoding operations. This work extents the idea of Umut uludag [1] for encoding and decoding the fuzzy vault.

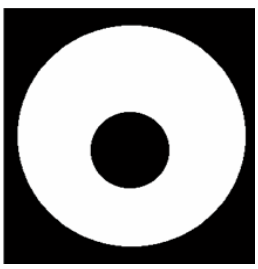
The basic idea of the proposed multi biometric fuzzy vault is derived from the work done by Umut uludag [1]. To identify the bifurcation feature point on the retinal texture the method proposed by Li chen[16] is utilized. The work done by Srinivasa Reddy [3] is utilized for extracting feature points from iris texture by performing sequence of morphological operations.

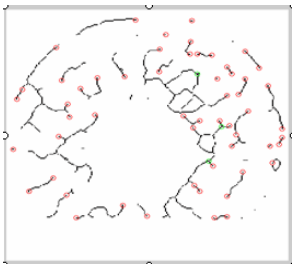
A. Feature Extraction from retina and Iris

The proposed work uses the idea of Li Chen [16] for extracting the bifurcation structure from retina. Thinning and joining morphological operations are performed on the retinal texture. These operations highlight the retinal vascular patterns. Then the bifurcation feature points are extracted from the vascular patterns. The (x, y) co-ordinates of the bifurcation feature points acts as lock/unlock data for the vault. Fig.1 (a) shows the retinal image, Fig.1 (b) shows the retinal vascular tree, Fig.1 c) shows the vascular pattern after thinning and joining operation and Fig 1(d) highlights the retinal template with bifurcation points. A unibiometric iris fuzzy vault is constructed from the bifurcation features extracted from retinal template.

The following operations are applied to the iris images to extract lock/unlock data. Canny edge detection is applied on iris image to deduct iris. Hough transformation is applied first to iris/sclera boundary and then to iris/pupil boundary. Then thresholding is done to isolate eyelashes. Histogram equalization is performed on iris to enhance the contrast. Finally the following sequences of morphological operations are performed on the enhanced iris structure.

(i) closing-by-tophat
(ii) opening
(iii) thresholding





. (a) Localized Iris Minutiae (b) Highlighted Iris Minutiae

Fig 2. Iris Feature Extraction

Finally thinning is done to get structures as a collection of pixels. Now the (x, y) coordinates of the nodes and end points of the iris minutiae are extracted. Fig. 2(a) shows the localized iris image and Fig. 2(b) exhibits the iris image with the minutiae patterns. A unibiometric iris fuzzy vault is constructed from the features extracted from iris template.

B. Implementation of Multimodal biometric fuzzy vault.

The proposed system is implemented in Matlab 7.0. Retinal samples are taken from DRIVE database. The retinal images taken from the DRIVE data base are resized to the standard 256 x 256 format.

Iris samples are taken from CUHK Iris Image Dataset [10]. Both the images are resized to 256 x 256 grey scale images by bilinear interpolation for further processing. Two independent fuzzy vaults are constructed from retina and iris features.

The method proposed by Umut uludag is enhanced for multibiometric vault and the proposed encoding shown in a Fig[3] and decoding Fig. [4].

a. Encoding

The minutiae points from retina and iris are combined together. Secret message is generated as a 128 bit

random stream. The primitive polynomial considered for CRC generation is

$$g_{crc}(a) = a^{16} + a^{15} + a^2 + 1$$

The 16 bit CRC is appended to S to get 144 bit SC.

In the combined set the minutiae points whose Euclidian distance is less than D are removed. 16 bit lock/unlock unit 'u' is obtained by concatenating x and y (each 8 bits) coordinates. The 'u' values are sorted and first N of them are selected. The Secret (SC) is divided into 9 non overlapping segments of 16 bits each. Each segment is converted to its decimal equivalent to account for the polynomial coefficients (C_8, C_7 …C_0). All operations takes place in Galois Field GF(2^{16}) .

The projection of 'u' on polynomial 'p' is found. Now the Genuine points set G is (u_i, $P(u_i)$). 200 random chaff points are generated. Both the genuine and chaff point sets are combined to become the vault. The vault is List scrambled.

b. Decoding

From the query templates of the retina and iris, unlocking points (N in number) are extracted. The unlocking set is found as in encoding. This set is compared with the vault to separate the genuine point set for polynomial reconstruction. From this set all combinations are tried to decode the polynomial. Langrangian interpolation is used for polynomial reconstruction. For a specific combination polynomial gets decoded.

In order to decode the polynomial of degree 8 a minimum of at least 9 points are required. If the combination set contains less then 9 points, polynomial cannot be reconstructed. Now the coefficients and CRC are appended to arrive at SC*. Then SC* is divided by the CRC primitive polynomial. If the remainder is zero, query image does not match template image and the secret data cannot be extracted. If the remainder is not zero, query image matches with the template image and the correct secret data can be extracted. In this case SC* is divided into two parts as the 128 bit secret data and 16 bit CRC code

4. RESULTS AND SECURITY ANALYSIS

The proposed method implements three different fuzzy vaults for retina, iris and combined retina and iris features. The security of the fuzzy vault is measured by min-entropy which is expressed in terms of security bits. . According to NandaKumar [8] the min-entropy of the minutiae template M^T given the vault V can be calculated as

$$H_{\infty}(M^T \mid V) = -\log_2 \left(\frac{\binom{r}{n+1}}{\binom{r+c}{n+1}} \right) \quad \ldots\ldots\ldots\ldots (1)$$

Where

r = number of genuine points in the vault

c = number of chaff points in the vault

t = the total number of points in the vault (r + c)

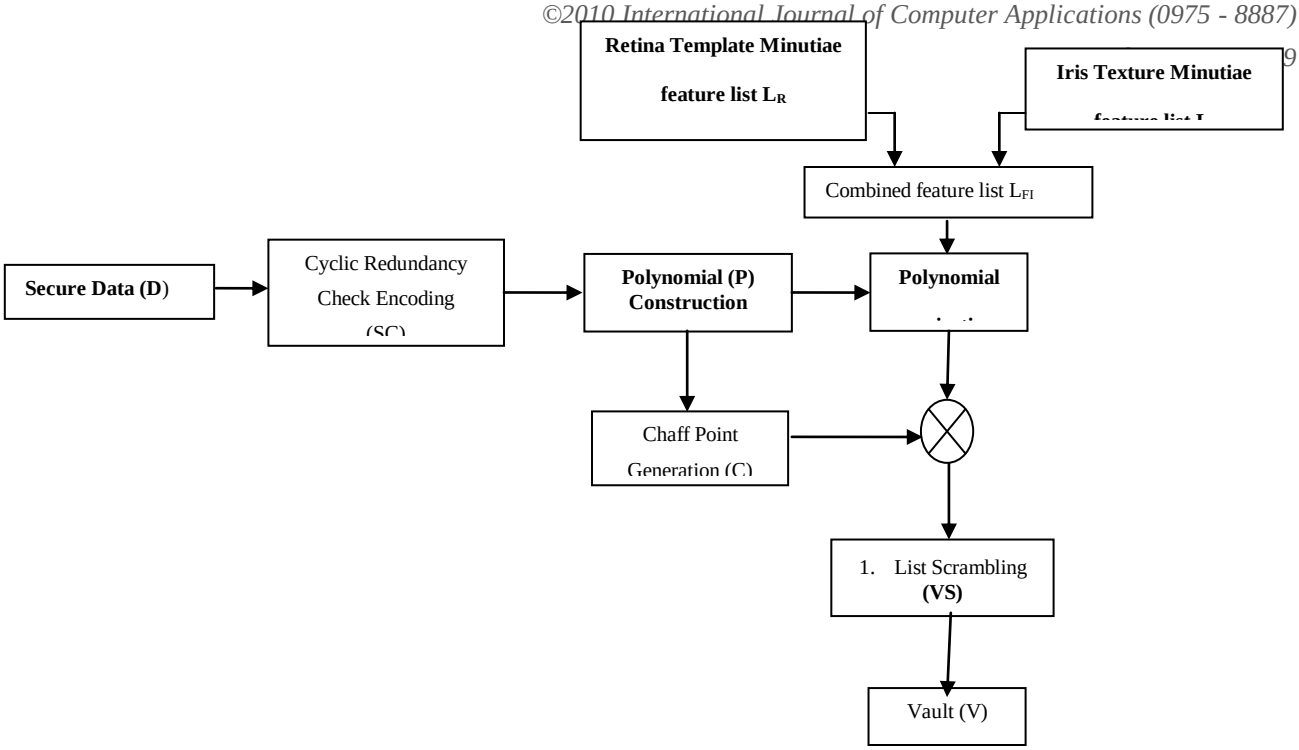


Fig. 3 Multi Biometric Fuzzy vault: Encoding

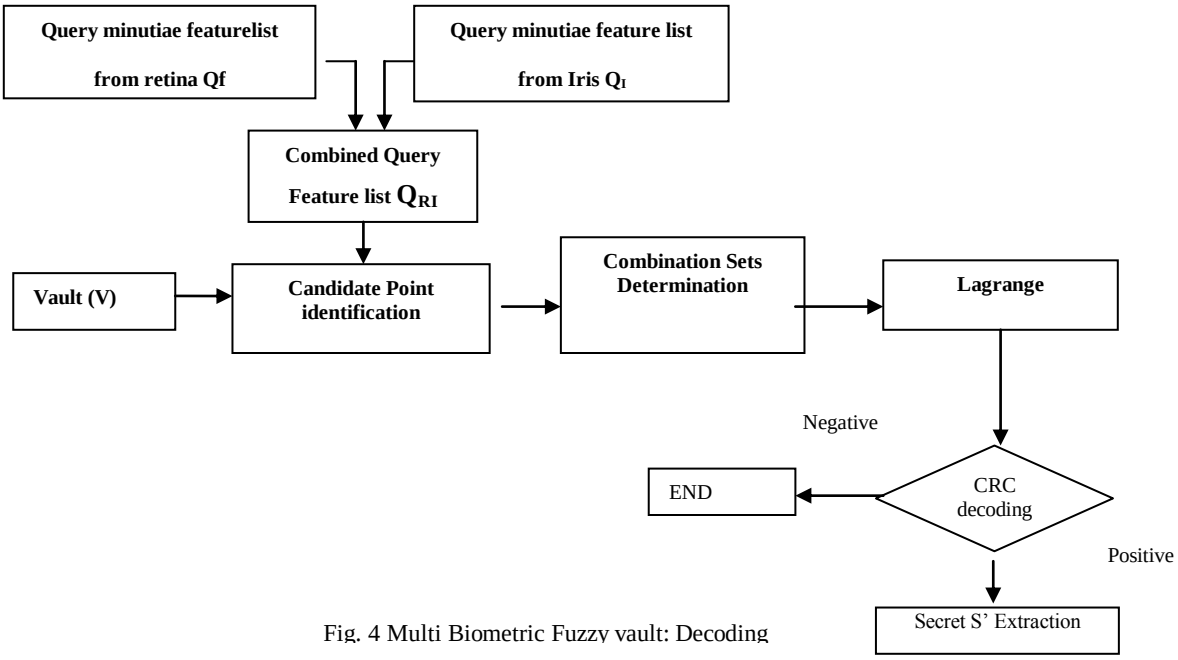


Fig. 4 Multi Biometric Fuzzy vault: Decoding

The parameters for the retina, iris and combined vault implementation are shown in table 1, table 3 and table 5. In the above constructed retina and iris fuzzy vault an adversary has to guess (n+1) points combinations simultaneously to decode the vault. The size of the secret key and the degree of the polynomials are increased and the security is calculated for the individuals vault.

Using Equation (1), the min-entropy in terms of security bits for the retina, iris and combined fuzzy vault are calculated for different polynomial degrees. The results are shown in table 2, table 4 and table 6.

Polynomial with lesser degrees can be easily reconstructed by the attacker and the vault gets decoded. Polynomials with larger degrees require a lot of computational effort. The min-entropy in terms of the security bits for retina and iris fuzzy vault for polynomial degree 11 are 44 bits and 45 bits respectively. In the combined vault for polynomial degree 13 the security increases to 50 bits. Therefore the multimodal fuzzy vault is more secure compared to the individual fuzzy vault. The combined vault contains the larger number of points from both the vaults. Hence it is evaluated for polynomial of degree 13.

The security of the fuzzy vault increases as the degree of the polynomial is increased. However it requires a lot of computation for higher degree polynomials which makes the system slow. The security increases as the number of chaff points in the vault increases but at the cost of increased memory consumption. Number of chaff points added is 10 times that of the genuine points to have larger combinations for achieving higher security.

Table 1 Parameters for retina fuzzy vault implementation

No. of. Genuine points(r)	30
No. of Chaff points(c)	300
Total no. of points (t = r + c)	330

Table 2 Min-entropy for retina fuzzy vault for different degree of the polynomial(n)

Degree of polynomial (n)	Min-entropy in terms of security bits
6	25
7	29
8	32
9	36
10	40
11	44

Table 3 Parameters for iris fuzzy vault implementation

No. of. Genuine points(r)	28
No. of Chaff points(c)	280
Total no. of points (t = r + c)	308

Table 4 Min-entropy for iris fuzzy vault for different degree of the polynomial(n)

Degree of polynomial (n)	Min-entropy in terms of security bits
6	25
7	29
8	33
9	37
10	41
11	45

Table 5 Parameters for multimodal retina and iris fuzzy vault implementation

No. of. Genuine points(r)	58
No. of Chaff points(c)	580
Total no. of points (t = r + c)	638

Table 6 Min-entropy for multimodal retina and iris fuzzy vault

Degree of polynomial (n)	Min-entropy in terms of security bits
13	50

In the case of the unimodal retina fuzzy vault of polynomial degree 11, if the adversary uses brute force attack, the attacker has to try a total of (330, 12) = 2.8440 x 10^{21} combination of 12 elements each. Only (30, 12) = 8.6493 x 10^{7} of these combinations are required to decode the vault. Hence for an attacker to decode the vault it takes Combination of (330, 12) / Combination (30, 12) = 3.2881 x 10^{13} evaluations.

In the case of the unimodal iris fuzzy vault of polynomial degree 11, the attacker has to try a total of (308,12) = 1.2247 x 10^{21} combination of 12 elements each. Only (28, 12) = 3.0422 x 10^{7} of these combinations are required to decode the vault. Hence for an attacker to

decode the vault it takes Combination of (308, 12) / Combination (28, 12) = 4.0257×10^{13} evaluations.

In the case of the multimodal vault of polynomial degree 13, the attacker has to try a total of (638,14)= 1.8395×10^{28} combination of 14 elements each. Only (58, 14) = 1.0143×10^{13} of these combinations are required to decode the vault. Hence for an attacker to decode the vault it takes Combination of (638, 14) / Combination (58, 14) = 1.8136×10^{15} evaluations.

The number of combinations for the attacker to try is comparatively larger for multimodal fuzzy vault. Therefore it is highly secure compared to its unimodal counterparts.

5. CONCLUSION

Multi biometric fuzzy vault is more secure compared to the single biometric fuzzy vault as an attacker cannot compromise it easily. The ideas of password hardening, helper data, and non-invertible transformation can still improve the security of the fuzzy vault. The idea of fuzzy vault secures the biometric template as well as the secret data at the same time. In the above study single template and query minutiae are used for encoding and decoding. This work can be further extended to measure other performance parameters like False Acceptance Rate (FAR), False Rejection Rate (FRR) of the vault. A compromised stored template cannot be revoked like passwords. Hence cancelable biometric templates can be generated by applying transformation functions. Different transformation functions can be applied to generate cancelable biometric templates for different applications. The ideas of other template protection schemes can be mixed with fuzzy vault to get a better hybrid method. This work uses two biometric that can be captured by the same capturing device and facilitates user convenience. More over iris and retina are less susceptible to environmental changes as compared to fingerprint. Therefore such system can be deployed in high security applications.

Acknowledgement

A public version of the CUHK Iris Database is available from http://www2.acae.cuhk.edu.hk.

A public version of the DRIVE: Digital Retinal Images for Vessel Extraction is available from http://www.isi.uu.n/Research/Databases/DRIVE

References

[1] Umat uludag, sharath pankanti, Anil. K.Jain "Fuzzy vault for fingerprints", Proceedings of International conference on Audio video based person authentication, 2005.

[2] A. Juels and M.Sudan, "A fuzzy vault scheme", Proceedings of IEEE International symposium Information Theory, 2002.

[3] E.Srinivasa Reddy, I. Ramesh Babu, "Performance of Iris Based Hard Fuzzy Vault", Proceedings of IEEE 8th International conference on computers and Information technology workshops, 2008

[4] U.Uludag, S. Pankanti, S.Prabhakar, and A.K.Jain, "Biometric Cryptosystems: issues and challenges, Proceedings of the IEEE ,June 2004.

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

[6] Karthick Nandakumar, Sharath Pankanti, Anil K. Jain, "Fingerprint-based Fuzzy Vault Implementation and Performance", IEEE Transacations on Information Forensics and Security, December 2007.

[7] K.NandaKumar, "Multibiometric Systems: Fusion Strategies and Template Security", PhD Thesis, Department of Computer Science and Engineering, Michigan State University, January 2008.

[8] Sharat Chikkarur, Chaohang Wu, Venu Govindaraju, "A systematic Approach for feature Extraction in Fingerprint images", Center for Unified Biometrics and Sensors(CUBS), university at Buffalo, NY,USA.

[9] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, June 2006.

[10] A. K. Jain, A. Ross, and U. Uludag, "Biometric Template Security: Challenges and Solutions," in Proceedings of European Signal Processing Conference (EUSIPCO), Antalya, Turkey, September 2005.

[11] Anil K.Jain, Karthik Nanda Kumar and Abhishek Nagar, "Biometric Template Security" EURASIP Journal on Advance in Signal Processing, special issue on Biometrics, January 2008.

[12] Ratha, N.K., J.H. Connell, and R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, vol. 40, no. 3.

[13] Jain, Anil K. Jain and Arun Ross, "Multibiometric systems," Communications of the ACM," January 2004, Volume 47, Number 1 (2004).

[14] A.K. Jain and A. Ross, "Learning User-specific parameters in a Multibiometric System", Proc. IEEE International Conference on Image Processing(ICIP),

Rochester, New York, September 22 – 25, 2002, pp. 57 – 60.

[15] Li Chen, IEEE Member, Xiao-Long zhang, "Feature-based image registration using bifurcation structures", Matlab Central

[16] N.K.Radha, S.Chikkerur, J.H.Connell, and R.M. Bolle,

Generating Cancelable Fingerprint Templates, IEEE Trans, PAMI, 29(4):561-572,April 2007.

[17] J.Feng , Combining Minutiae Descriptors for fingerprint matching, Pattern Recognition, 41(1):342 - 352,2008.