International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:3, No:8, 2009

Security Analysis of Password Hardened Multimodal Biometric Fuzzy Vault

V. S. Meenakshi, and G. Padmavathi

***Abstract*—**Biometric techniques are gaining importance for personal authentication and identification as compared to the traditional authentication methods. Biometric templates are vulnerable to variety of attacks due to their inherent nature. When a person's biometric is compromised his identity is lost. In contrast to password, biometric is not revocable. Therefore, providing security to the stored biometric template is very crucial. Crypto biometric systems are authentication systems, which blends the idea of cryptography and biometrics. Fuzzy vault is a proven crypto biometric construct which is used to secure the biometric templates. However fuzzy vault suffer from certain limitations like non-revocability, cross matching. Security of the fuzzy vault is affected by the non-uniform nature of the biometric data. Fuzzy vault when hardened with password overcomes these limitations. Password provides an additional layer of security and enhances user privacy. Retina has certain advantages over other biometric traits. Retinal scans are used in high-end security applications like access control to areas or rooms in military installations, power plants, and other high risk security areas. This work applies the idea of fuzzy vault for retinal biometric template. Multimodal biometric system performance is well compared to single modal biometric systems. The proposed multi modal biometric fuzzy vault includes combined feature points from retina and fingerprint. The combined vault is hardened with user password for achieving high level of security. The security of the combined vault is measured using min-entropy. The proposed password hardened multi biometric fuzzy vault is robust towards stored biometric template attacks.

***Keywords*—**Biometric Template Security, Crypto Biometric Systems, Hardening Fuzzy Vault, Min-Entropy.

I. Introduction

THE biometric crypto system utilizes the advantages of both biometrics and cryptography for ensuring high security. Some of the applications include financial transactions, border security and military applications. 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. Here biometric plays the role of a wrapper.

In biometric based key generation method, biometrics and cryptography are combined together at a much higher level. In this method the secret key is extracted from the combined key and biometric template. A fuzzy vault is a biometric based key generation cryptographic construct. This work focuses on the mixing of two different biometric modalities for constructing the multimodal fuzzy vault. Fingerprint and retina are utilized to construct the multimodal biometric vault.

V. S. Meenakshi is with the Dept. of Computer Application, SNR Sons College, Coimbatore.Tamil Nadu, India (e-mail: meenasri70@yahoo.com).

Padmavathi Ganapathi, Head of the Dept of Computer Science, Avinashilingam University for Women, Coimbatore (e-mail: mail_padma@yahoo.com).

A. 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.

B. Construction of 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 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.

C. 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 [13, 14]. It can be used in applications like financial transactions, for securing secret cryptographic keys, email communications etc.

Biometric templates are not revocable when compromised like passwords [12]. A template represents a set of salient features that summarizes the biometric data (signal) of an individual. A compromised template would mean the loss of a user's identity [9,10]. A potential abuse of biometric identifiers is cross-matching [11]. Therefore biometric template security is very crucial to protect user privacy. It is very difficult for an attacker to compromise multi biometric modalities.

The proposed multimodal fuzzy vault contains point set from two different biometric modalities say fingerprint and retina namely K_f and K_r. Then Chaff points are added to the vault to conceal the genuine points.

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

The Chaff points are generated in such a way that they do not lie on K_f and K_r. In this proposed vault the secret **S** is locked by two unordered sets U_f and U_r.

Table I shows the notations used.

TABLE I
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

D. Limitation of Fuzzy Vault Scheme

Fuzzy vault being a proven scheme has its own limitations [5].

(i) If the vault is compromised, the same biometric data cannot be used to construct a new vault. Fuzzy vault cannot be revoked. Fuzzy vault is prone to cross-matching of templates across various databases.

(ii) Due to the non-uniform nature of the biometric features it is easy for an attacker to develop attacks based on statistical analysis of the points in the vault.

(iii) The vault contains more chaff points than the genuine points. This facilitates the attacker to substitute few points from his own biometric feature. Therefore the vault authenticates both the genuine user and the imposter using the same biometric identity. As a consequence, the false acceptance ratio of the system increases.

(iv) Original template of the genuine user is temporarily exposed. During this exposure the attacker can glean the template.

To overcome the limitations of fuzzy vault, password is used as an additional authentication factor. The proposed multimodal fuzzy vault is hardened by password. This enhances the user-privacy and adds an additional level of security.

E. Fuzzy Vault Hardening

The hardened fuzzy vault overcomes the limitations of non-revocability and cross-matching by introducing an additional layer of security by password. If the password is compromised the basic security and privacy provided by the fuzzy vault is not affected. However, a compromised password makes the security level same as that of a fuzzy vault. Therefore, security of the password is crucial. It is very difficult for an attacker to compromise both the biometric template at the same time. The proposed method constructs a multimodal biometric fuzzy vault using the feature points extracted from retina and fingerprint. The multimodal biometric fuzzy vault is then hardened using the password.

Steps in hardening scheme:

1. A random transformation function is derived from the user password.
2. The password transformed function is applied to the retina template.
3. The password transformed function is applied to the fingerprint template.
4. Fuzzy vault frame work is constructed to secure the transformed templates by using the feature points from both the retina and fingerprint.
5. The key derived from the same password is used to encrypt the vault.

Fig. 1 depicts the steps involved in the construction of the multi biometric fuzzy vault.

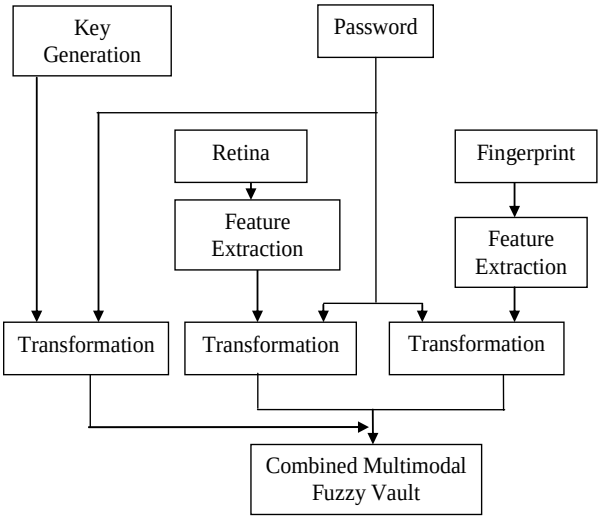


Fig. 1 Hardening Multi Biometric Fuzzy Vault

The organization of the paper is as follows: Section II elaborates the construction and operation of fuzzy vault. Section III explains the proposed password hardened multimodal biometric fuzzy vault. Section IV discusses the experimental results and the security analysis of the vault. Section V presents the conclusion.

II. Background

Umut uludag et al [1] uses the concept of fuzzy vault to protect a secret S of 128 bits length. The general notations used in the literature are shown in table I. The x and y coordinates 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.

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

During decoding process, 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 match and the secret decoded is not correct. If the Remainder is zero, Query Template (Q) matches and the Secret(S) is decoded successfully. The same idea is used for retina and the retinal bifurcation points acts as lock/unlock data.

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] show the password hardened fingerprint fuzzy vault in which password acts an additional layer of security. Srinivasa Reddy [3] followed the same idea of [5] to implement an iris based hardened fuzzy vault. The basic idea of hardening multimodal biometric fuzzy vault is derived from the work done by Karthick Nandakumar et al [5] and Srinivasa Reddy [3].

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 for extracting the locking/unlocking unit from the retina. To identify the bifurcation feature point on the retinal texture the method proposed by Li Chen[16] is utilized. Section 3 presents the proposed password hardened multimodal biometric fuzzy vault.

III. Proposed Method

The proposed work constructs the password hardened multimodal fuzzy vault in three steps. In the first step the retinal biometric template and fingerprint template are subjected to random transformation using password separately. This process enhances the user privacy and facilitates the generation of revocable templates that resists cross matching. This transformation reduces the similarity between the original and transformed template.

In the second step, multimodal fuzzy vault is constructed to secure the transformed templates. The key used in fuzzy vault construction is randomly generated and transformed using the same password. The key can also be generated from the retinal structure or from the fingerprint features for better security.

In the third step, the vault is encrypted by the key derived from the password. In this vault, password acts as an additional layer of security.

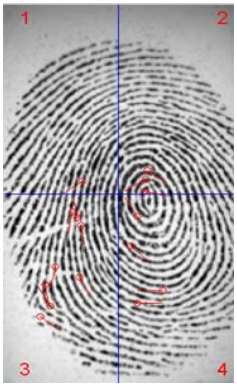
A. Extraction of Feature point from Fingerprint and Retina

The proposed work uses the algorithm of Sharat S.Chikkerur [8] for extracting the fingerprint minutiae. Fig. 2 (a) shows the original fingerprint template and Fig. 2 (b) shows the highlighted fingerprint template with minutiae points.

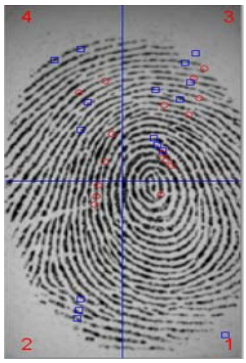
The proposed work uses the idea of Li Chen [16] for extracting the bifurcation structure from retina. Thinning and joining morphological operations are performed on the retinal texture. These operations highlight the retinal vascular patterns. Then the bifurcation feature points are extracted from the vascular patterns. The (x, y) co-ordinates of the fingerprint minutiae and bifurcation feature points of the retina act as lock/unlock data for the vault. Fig. 2(a) shows the fingerprint image and Fig. 2(b) shows the fingerprint template with highlighted minutiae points. Fig.3 (a) shows the retina image Fig. 3(b) shows the retinal vascular tree and Fig.3(c) shows the vascular pattern after thinning and joining

operation. Fig 3(d) highlights the retinal template with bifurcation points.

(a) Fingerprint Image



(b) Fingerprint Minutiae



(c) Red: Permuted Points and Blue: Transformed Points

Fig. 2 Fingerprint Minutiae Extraction and Password Transformation

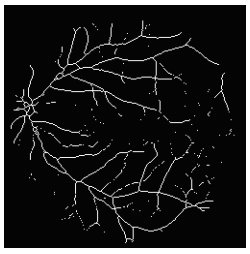
B. Implementation of Password Hardened Multi Modal Fuzzy Vault

The proposed system is implemented in Matlab 7.0. Fingerprint samples are taken from FVC2002 DB2 fingerprint database. Fingerprint images are resized to 256 X 136. Retina samples are taken from DRIVE database. The retinal images taken from the DRIVE data base are resized to the standard 256 x 256 format.

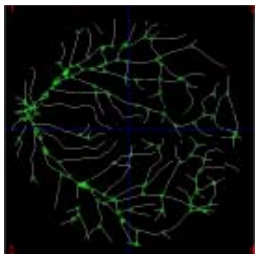
This implementation identifies the lock/unlock data by highlighting the fingerprint minutiae and retinal bifurcation structures. The (x, y) attributes, of the fingerprint minutiae and retina bifurcation structure, where 'x' and 'y' represents the row and column indices of the both the biometric images are found out. Permutation and Translation operations are applied on the minutiae point and bifurcation feature points by using the password separately. The transformed feature points are protected in the combined fuzzy vault. In this implementation 128 bit random key is generated. This key can also be generated from the retinal structure or fingerprint for added security. This key is transformed by the 64 bit user password and is used to encrypt the vault.

(a) Retinal image

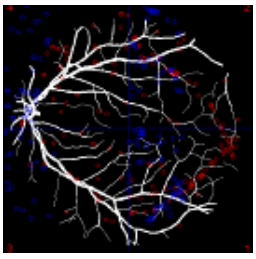
(b) Retinal vascular tree



(c) Thinned and joined image



(d)Highlighted Bifurcation feature



(e) Red: Permuted Points and Blue: Transformed Points

Fig. 3 Retina Feature Extraction

a. Feature Point Transformation

The fingerprint template and retinal vascular tree containing the highlighted bifurcation feature points are subjected to simple permutation and translation. Fig 2(b) shows the minutiae before transformation and Fig 2(c) shows the minutiae after transformation for fingerprint. Fig 3(d) shows the feature point before transformation and Fig. 3(e) shows the feature point after transformation for retina. This results in the original feature points being transformed into new points.

The user password is restricted to the size of 8 characters. Therefore, the length of the password is 64 bits. These 64 bits are divided into 4 blocks of each 16 bits in length.

The feature point highlighted in fingerprint template and retinal vascular tree is divided into 4 quadrants. One password block is assigned to each quadrant Permutation is applied in such a way that the relative position of the feature point does not change.

Each 16 bit password block is split into two components T_u of 7 bits and T_v of 9 bits in length. T_u and T_v represent the amount of translation in the horizontal and vertical directions, respectively.

The new feature points are obtained by the following transformation.

$$X'_u = (X_u + T_u) \bmod (2^{\wedge}7)$$
$$Y'_v = (Y_v + T_v) \bmod (2^{\wedge}9)$$

Where $\mathbf{X_u}$ and $\mathbf{X'_u}$ are the horizontal distance before and after transformation respectively. Similarly $\mathbf{Y_v}$ and $\mathbf{Y'_v}$ are the vertical distance before and after transformation respectively. This transformation is applied for both fingerprint and retina template.

b. Encoding

The transformed features are encoded in the multi biometric fuzzy vault. Password acts as an extra layer of security to the multi biometric vault. It resists an imposter from modifying the vault. The minutiae points from fingerprint and bifurcation points from retina are combined together. Secret message is generated as a 128 bit random stream. This secret message is transformed with the password. The 16 bit CRC is appended to transformed key S to get 144 bit SC. The primitive polynomial considered for CRC generation is

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

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, $P(u_i)$). Random chaff points are generated which are 10 times in number that of the genuine points. Both the genuine and chaff point sets are combined to construct the vault. The vault is List scrambled. The encoding operation is shown in Fig. 4.

c. Decoding

In the authentication phase, the encrypted vault and bifurcation feature point are decrypted by the user password. Password based transformation is applied to the query feature points and the vault is unlocked.

From the query templates of the fingerprint and retina, 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. Lagrangian interpolation is used for polynomial reconstruction. For a specific combination of feature points the 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.

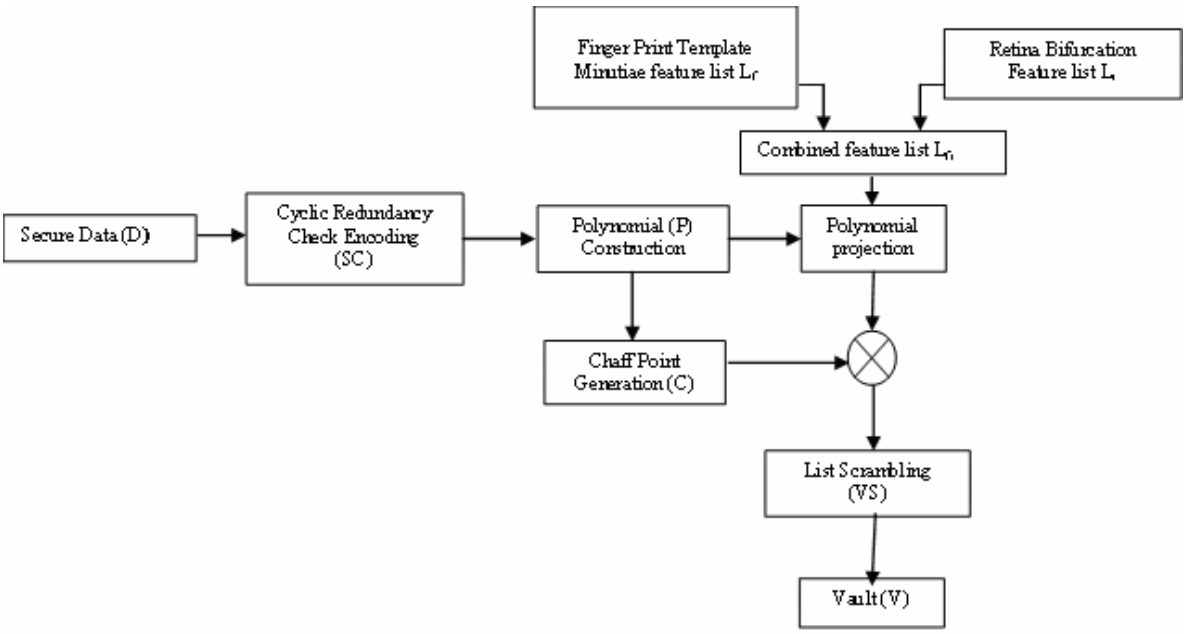


Fig. 4 Multi Biometric Fuzzy Vault: Encoding

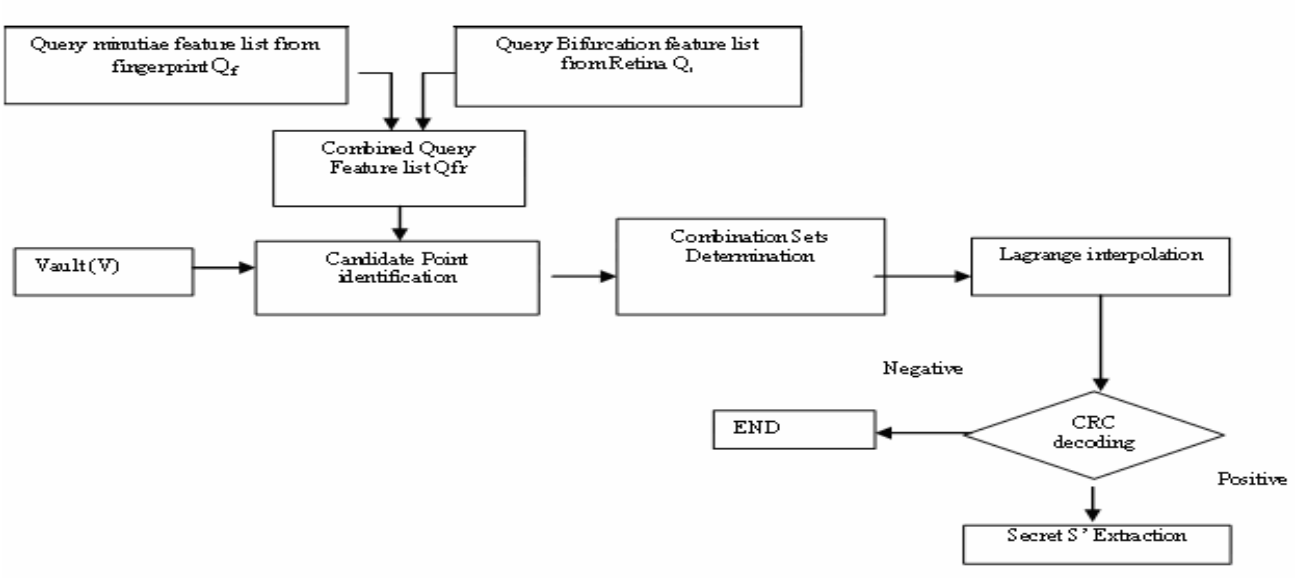


Fig. 5 Multi Biometric Fuzzy Vault: Decoding

Parameters used in Implementation

The parameters used in this implementation are shown in Table II. Chaff points hide the genuine points from the attacker. More chaff points makes the attacker to take much time to compromise the vault but consumes additional computation time. The chaff points added are 10 times in number that of the genuine points.

TABLE II
PARAMETERS FOR VAULT IMPLEMENTATION

Parameter	Fingerprint	Retina	Multimodal
No. of. Genuine points(r)	20	30	50
No. of Chaff points(c)	200	300	500
Total no. of points (t = r + c)	220	330	550

IV. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

The vertical and horizontal distances of the retinal bifurcation features and fingerprint minutiae are used for the polynomial projections. The retinal and finger print template is transformed for three different user passwords to check for revocability. Tables III and IV show the sample fingerprint minutiae point and the sample retinal bifurcation points from four quadrants after transformation using three different user passwords 'security', 'template' and 'quadrant' respectively. Fig. 6 and Fig. 7 illustrate the password transformations.

Consider a 8 character user password 'security', the ASCII value of which is given by (115, 111, 99, 117, 114, 105,116,121) or 64 bits. These 64 bits are divided into four blocks of 16 bits each and these are further divided into 7 bits and 9 bits for transformation in horizontal and vertical directions respectively. Fig. 6 and Fig. 7 illustrate the password transformations.

The feature point transformation is done with other two user passwords namely 'template' and 'quadrant' whose ASCII codes are (116, 101, 109, 112, 108, 97, 116 101) and (113, 117, 97, 100, 114, 97, 110, 116) respectively. For the same original template different transformed templates are obtained when password is changed. This property of hardened fuzzy vault facilitates revocability. Different passwords can be utilized for different applications to avoid cross matching.

In the proposed method the security of the fuzzy vault is measured by min-entropy which is expressed in terms of security bits. According to NandaKumar [7] the min-entropy of the feature template M^T given the vault V can be calculated as

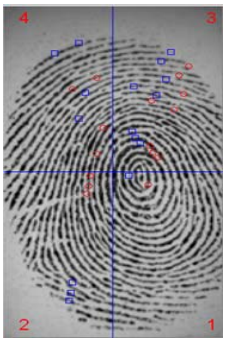
$$H_\infty(M^T \mid V) = -\log_2 \left(\frac{\binom{r}{n+1}}{\binom{r+c}{n+1}} \right) \quad (1)$$

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)
n = degree of the polynomial

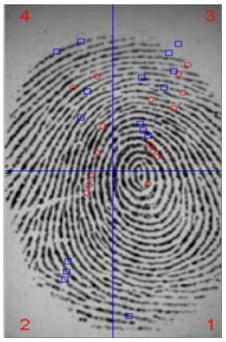
The security of the single modal fingerprint, retina and multi modal vault is tabulated in Table. V. In order to decode a polynomial of degree n , (n+1) points are required.

The security of the fuzzy vault can be increased by increasing the degree of the vault. Polynomial with lesser degree can be easily reconstructed by the attacker. Polynomial with higher degree increases security and requires lot of computational effort. This makes more memory consumption and makes the system slow. However they are hard to reconstruct.In the case of the vault with polynomial degree n,

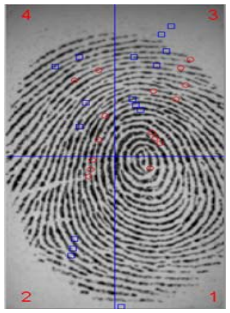
if the adversary uses brute force attack, the attacker has to try total of (t, n+ 1) combinations of n+ 1 element each. Only (r, n+1) combinations are required to decode the vault. Hence, for an attacker to decode the vault it takes C(t, n+1)/C(r, n+1) evaluations. The guessing entropy for an 8 ASCII character password falls in the range of 18 – 30 bits. Therefore, this entropy is added with the vault entropy. The security analysis of the password hardened multi biometric fuzzy vault is shown in Table V.



(a) Password 'security'



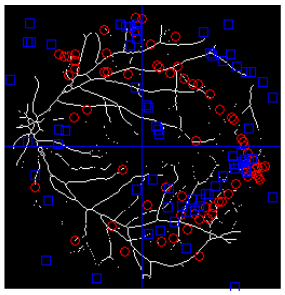
(b) Password 'template'



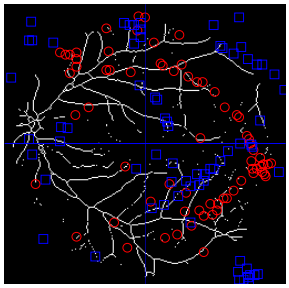
(c) Password 'quadrant'

Fig. 6 Transformed Fingerprint minutiae

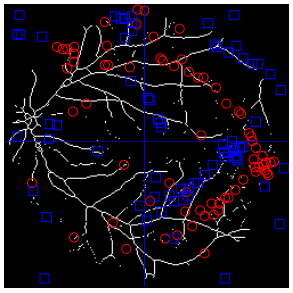
If the number of feature points is less than (n+1) then Failure to Capture Rate occurs. (FTCR). Multi modal biometric fuzzy vault minimizes the FTCR.



(a) Password 'security'



(b) Password 'template'



(c) Password 'quadrant'

Fig. 7 Transformed Retinal Features

V. Conclusion

Password hardening of the multi biometric fuzzy vault introduces two layers of security namely password and biometrics. Even if the attacker gains the password, he/she may not be able to access the genuine feature points. It is computational very hard for an attacker to identify the genuine feature points. When the attacker compromises both the biometrics and password simultaneously then he/she can capture the vault. This is not possible in real life situation. Hence the proposed password hardened multi biometric fuzzy vault is robust against stored biometric template attacks. The performance of the vault can be improved by the application non –invertible transformation and multiple biometric traits.

Acknowledgement

A public version of the FVC2002 fingerprint database is available from http://bias.csr.unibo.it/fvc2002/

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

TABLE III
FINGERPRINT MINUTIAE POINTS AFTER TRANSFORMATION

Quadrant and Password	Feature points before transformation		Transformation code from password		Feature point after transformation	
	Horizontal Distance (X_u)	Vertical Distance (Y_v)	T_u	T_v	Horizontal Distance (X_u)	Vertical Distance (Y_v)
I						
'security'	43	64	57	357	32	37
'template'			58	101	33	37
'quadrant'			56	373	31	53
II						
'security'	91	108	49	373	80	97
'template'			54	368	85	92
'quadrant'			48	356	79	80
III						
'security'	54	131	57	210	43	213
'template'			54	97	40	197
'quadrant'			57	194	43	197
IV						
'security'	91	138	116	121	78	131
'template'			58	101	78	239
'quadrant'			110	116	72	254

TABLE IV
RETINA BIFURCATION FEATURE POINTS AFTER TRANSFORMATION

Quadrant and Password	**Feature points before transformation**		**Transformation code from password**		**Feature point after transformation**	
	Horizontal Distance (X_u)	Vertical Distance (Y_v)	T_u	T_v	Horizontal Distance (X_u)	**Vertical Distance (Y_v)**
I						
'security'	122	12	57	357	51	113
'template'			58	101	52	113
'quadrant'			56	373	50	1
II						
'security'	159	29	49	373	208	18
'template'			54	368	213	13
'quadrant'			48	356	207	1
III						
'security'	110	149	57	210	39	231
'template'			54	97	36	215
'quadrant'			57	194	39	215
IV						
'security'	181	227	116	121	169	220
'template'			58	101	169	200
'quadrant'			110	116	163	215

TABLE V
SECURITY ANALYSIS OF THE PASSWORD HARDENED MULTIBIOMETRIC FUZZY VAULT

Vault Type	Degree of polynomial	Min-entropy of the vault (in security bits	Total no: of combinations	Combinations required	No: of Evaluations	Min-entropy + guessing entropy of the password (in security bit)
Fingerprint	8	34	2.8187×10^{15}	167960	1.6782×10^{10}	52 to 64
Retina	8	33	1.1457×10^{17}	14307150	8.0079×10^{9}	51 to 63
Combined Fingerprint and Retina	10	40	3.1559×10^{22}	3.7354×10^{10}	8.4487×10^{11}	58 to 70

REFERENCES

[1] Umat uludag, sharath pankanti, Anil. K.Jain "Fuzzy vault for fingerprints", Proceedings of International conference on Audio video based person authentication, july 20 – 22, pp. 310 – 319, 2005.
[2] A. Juels and M.Sudan, "A fuzzy vault scheme", Proceedings of IEEE International symposium Information Theory, pp. 408, 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, pp. 248 – 253, 2008
[4] U.Uludag, S. Pankanti, S.Prabhakar, and A.K.Jain, "Biometric Cryptosystems: issues and challenges, Proceedings of the IEEE 92(6): 948 - 960,June , 2004.
[5] Karthik Nandakumar, Abhishek Nagar and Anil K.Jain, "Hardening Fingerprint Fuzzy Vault using Password", International conference on Biometrics, pp. 927 – 938, 2007.
[6] Karthick Nandakumar, Sharath Pankanti, Anil K. Jain, "Fingerprint-based Fuzzy Vault Implementation and Performance", IEEE Transacations on Information Forensics and Security, 2(4):744 – 757, 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, pp. 614 – 634, 2001.
[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, pp. 57 – 60, September 22 – 25, 2002.
[15] Joes Staal, Associate Member, IEEE, Michael D. Abràmoff, Member, IEEE, Meindert Niemeijer, Max A. Viergever, Member, IEEE, and Bramvan Ginneken, Associate Member, IEEE, " Ridge-Based Vessel Segmentation in Color Images of the Retina", IEEE transactions on medical imaging, vol. 23, no. 4, April 2004.
[16] Li Chen, IEEE Member, Xiao-Long zhang, "Feature-based image registration using bifurcation structures", Matlab Central.

V. S. Meenakshi received her B.Sc (Physics) from Madurai Kamaraj University and MCA from Thiagarajar College of Engineering, Madurai in 1990 and 1993 respectively. And, she received her M.Phil degree in Computer Science from Manonmaniam Sundaranar University, Tirunelveli in 2003. She is pursuing her PhD at Avinashilingam University for Women. She is currently working as an Asst. Professor in the Department of Computer Applications, SNR Sons College, Coimbatore. She has 15 years of teaching experience. She has presented nearly 10 papers in various national and international conferences. Her research interests are Biometrics, Biometric Template Security and Network Security.

Padmavathi Ganapathi is the Professor and Head of the Department of Computer Science, Avinashilingam University for Women, Coimbatore. She has 21 years of teaching experience and one year Industrial experience. Her areas of interest include Network security and Cryptography and real time communication. She has more than 60 publications at national and International level. She is a life member of many professional organizations like CSI, ISTE, AACE, WSEAS, ISCA, and UWA. She is currently the Principal Investigator of 5 major projects under UGC and DRDO.