Securing Revocable Iris and Retinal Templates using Combined User and Soft Biometric based Password Hardened Multimodal Fuzzy Vault

V. S. Meenakshi[1] and Dr G. Padmavathi[2]

[1] Department of Computer Applications, S.N.R. Sons College
Coimbatore, Tamilnadu, India

[2] Department of Computer Science, Avinashilingam Deeemed University for Women
Coimbatore, Tamilnadu, India

Abstract

Biometric systems are subjected to a variety of attacks. Stored biometric template attack is very severe compared to all other attacks. Providing security to biometric templates is an important issue in building a reliable personal identification system. Multi biometric systems are more resistive towards spoof attacks compared to unibiometric counterpart. Soft biometric are ancillary information about a person. This work provides security and revocability to iris and retinal templates using combined user and soft biometric based password hardened multimodal biometric fuzzy vault. Password hardening provides security and revocability to biometric templates. Eye biometrics namely iris and retina have certain merits compared to fingerprint. Iris and retina capturing cameras can be mounted on a single device to improve user convenience. Security of the vault is measured in terms of min-entropy.

Keywords: Biometric template security, min-entropy, fuzzy vault, retina, iris, revocability, Soft Biometrics

1. Introduction

1.1 Merits of eye biometrics - Iris and Retina

Iris is the colored ring surrounding the pupil of the eye. Retinal scan capture the pattern of blood vessels in the eye. Retina and iris as biometric have certain merits compared to other biometrics. They are very difficult to spoof. More over retinal patterns do not change with age. When a person is dead then the lens will not converge the image that fall on the retina. Retina and iris are internal organs and is less susceptible to either intentional or unintentional modification unlike fingerprint. Retina is located deep within ones eyes and is highly unlikely to be altered by any environmental or temporal conditions. Both are highly secure and use a stable physiological trait. They are very difficult to spoof. Iris and retinal texture

are different for right and left eye. They are unique even for identical twins. Retina is best suitable for high security systems.

1.2 Soft Biometrics

Soft biometrics provides ancillary information about a person (gender, ethnicity, age, height, weight, eye color etc). They lack distinctiveness or permanence. Hence Soft biometrics alone is not enough to differentiate two individuals. Anyhow when combined with primary biometrics (Fingerprint, Iris, Retina etc) soft biometrics gives better results

1.3 Operation of Fuzzy Vault

Fuzzy vault is a cryptographic construct proposed by Juels and Sudan [1,2]. 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.

1.4 Limitation of Fuzzy Vault Scheme

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

1. Compromised vault cannot be revoked and it is prone to cross- matching of templates across various databases.
2. It is easy for an attacker to develop attacks based on statistical analysis of the points in the vault.
3. Attacker can substitute few points from his own biometric feature. Therefore the vault authenticates both the genuine user and the imposter using the same biometric identity.
4. Original template of the genuine user is temporarily exposed and the attacker can glean the template.

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

1.5 Steps in Combined Password Hardened Fuzzy Vault

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 the biometric template and the combined password at the same time. The proposed method constructs a fuzzy vault using the feature points extracted from iris and retina. The iris and retinal multimodal biometric fuzzy vault is then hardened using the password.

Steps in hardening scheme:

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

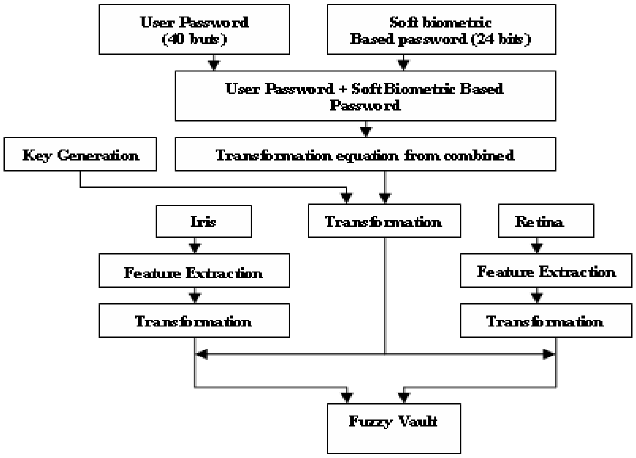


Fig. 1 Steps in combined password hardened fuzzy vault

Figure 1 depicts the steps involved in the construction of the combined user and soft biometric based password hardened multimodal biometric fuzzy vault.

The organization of the paper is as follows: Chapter II elaborates the background study. Section III explains the proposed combined password hardened multimodal biometric fuzzy vault. Section IV discusses the experimental results and the security analysis. Section V concludes of the proposed work.

2. Related Work

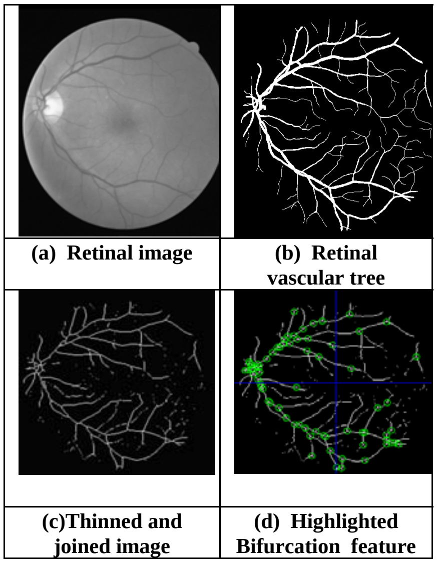
Karthick Nandakumar et al [5] used the idea of password transformation for fingerprint and generated transformed templates. In his work those transformed templates are protected using fuzzy vault cryptographic construct in which password acts an additional layer of security. Iris based hard fuzzy vault proposed by Srinivasa Reddy [3] followed the same idea of [5] to generate revocable iris templates and secured them using password hardened fuzzy vault. The basic idea of generating cancelable iris is based on the idea derived from the work done by karthick Nandakumar et al [5,6,7] and Srinivasa Reddy[3]. Sharat Chikkarur[8] work on fingerprint provided a general understanding on feature extraction steps,

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 method for extracting the minutiae feature point from the Iris. The same idea is used but with combined user and soft biometric password. Soft biometrics ideas derived from [16, 17, 18, 19] are used for constructing soft biometric passwords.

3. Proposed Method

3.1 Extraction of Bifurcation Feature point from Retina

Thinning and joining morphological operation is performed on the Retinal texture. The proposed work uses the idea of Li Chen [15] for extracting the bifurcation structure from retina.



(a) Retinal image

(b) Retinal vascular tree

(c)Thinned and joined image

(d) Highlighted Bifurcation feature

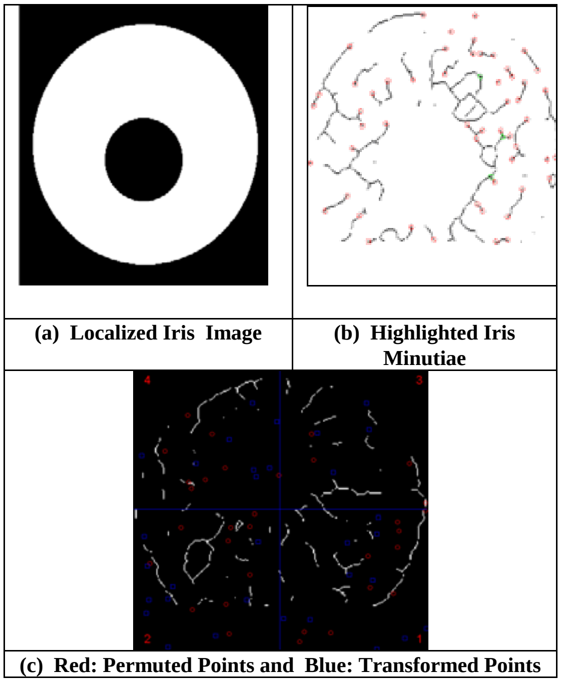
Fig 2 Retina Feature Point Extraction

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 feature points are transformed based on the soft biometric password.

Fig.2(a) shows the retina image Fig. 2(b) shows the retinal vascular tree and Fig.2(c) shows the vascular pattern after thinning and joining operation. Fig 2(d) highlights the retinal template with bifurcation points.

3.2 Feature point Extraction of Minutiae from Iris

The idea proposed by Srinivasa Reddy [3] is utilized to extract the minutiae feature points from the iris texture. 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.



(a) Localized Iris Image

(b) Highlighted Iris Minutiae

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

Fig 3. Iris Minutiae Extraction and Password Transformation

Finally the following sequence of morphological operations is performed on the enhanced iris structure.
(i) closing-by-tophat (ii) opening (iii) thresholding

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. 3(a) shows the localized iris image, Fig. 3(b) exhibits the iris image with the minutiae patterns and Fig 3(c) shows the permuted and transformed points.

3.3 Iris and Retinal Minutiae Feature Point Transformation

The Iris texture and the retinal vascular tree containing the highlighted minutiae feature points are subjected to simple permutation and translation. This results in the original minutiae points being transformed into new points. The user password is restricted to the size of 5 characters. The length of the user password is 40 bits.
The soft biometric [16, 17.18] password is generated by combining height, eye color, and gender. The combination of these three factors results in 24 bit soft biometric password (8 bit each). Therefore the length of the combined password is 64 bits. These 64 bits are divided into 4 blocks of each 16 bits in length. The feature points highlighted in Iris texture and the retinal structure are divided into 4 quadrants. One password block is assigned to each quadrant. Permutation is applied in such a way that the relation position of the minutiae 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 represents the amount of translation in the horizontal and vertical directions, respectively. The new feature points are obtained by the following transformation.

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

where $\mathbf{X_u}$ and $\mathbf{X'_u}$ is the horizontal distance before and after transformation respectively. Similarly $\mathbf{Y_v}$ and $\mathbf{Y'_v}$ is the vertical distance before and after transformation respectively.

3.4 Fuzzy Vault Encoding

The combined transformed features from iris and retina are encoded in the fuzzy vault. Password acts as an extra layer of security to the vault. It resists an imposter from modifying the vault. 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

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

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.

3.5 Fuzzy Vault Decoding

In the authentication phase, the encrypted vault and combined feature point are decrypted by the combined password. Password based transformation is applied to the query feature points and the vault is unlocked. From the query templates of the iris 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 not zero, query image does not match template image and the secret data decodes in not correct. If the remainder is zero, query image matches with the template image, and the secret decoded is correct.

3.6 Parameters used in implementation

The parameters used in this implementation are shown in Table 1. 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 1: Parameters of the combined Retina and Iris Vault.

Parameter	Iris	Retina	Total
No. of. Genuine points(r)	28	30	58
No. of Chaff points(c)	280	300	580
Total no. of points (t = r + c)	308	330	638

4. Experimental Results and Analysis

The Iris and retinal template are transformed for three different user passwords to check for revocability.

Consider a 5 character user password ‘FUZZY’, whose ASCII value is given by or 40 bits. Soft biometric password component is 155BM (24 bits). Soft biometric password and User Password are combined to form the transformation password as ‘155BMFUZZY’ (64 bits) whose ASCII values are (155, 66, 77, 70, 85, 90, 90, 89,) . These 64 bits are divided into four blocks of 16 bits each. Each 16 bit is divided into 7 bits and 9 bits for transformation in horizontal and vertical direction.

The feature point transformation is done with other two user passwords and soft biometric password combinations namely ‘170GFTOKEN’ and ‘146AM VAULT’ whose ASCII codes are (170, 71, 70, 84, 79, 75, 69, 78,) and (146, 65, 77, 86, 65, 85, 76, 84,) respectively. For the same original iris and retinal template different transformed templates are obtained when password is changed. Fig 4(a), Fig 4(b) and Fig 4(c) shows the transformed iris feature points and Fig 5(b), Fig 5(c) and Fig 5(d) shows the transformed retinal templates for three different passwords. This property of password transformation facilitates revocability. Different password can be utilized for generating different Iris templates.

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 Nanda Kumar [7] the min-entropy of the feature template M_T given the vault V can be calculated as

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

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)
n = degree of the polynomial

Table II shows the possible eye colors and Table III shows the structure of the sample combined user and soft biometric passwords.

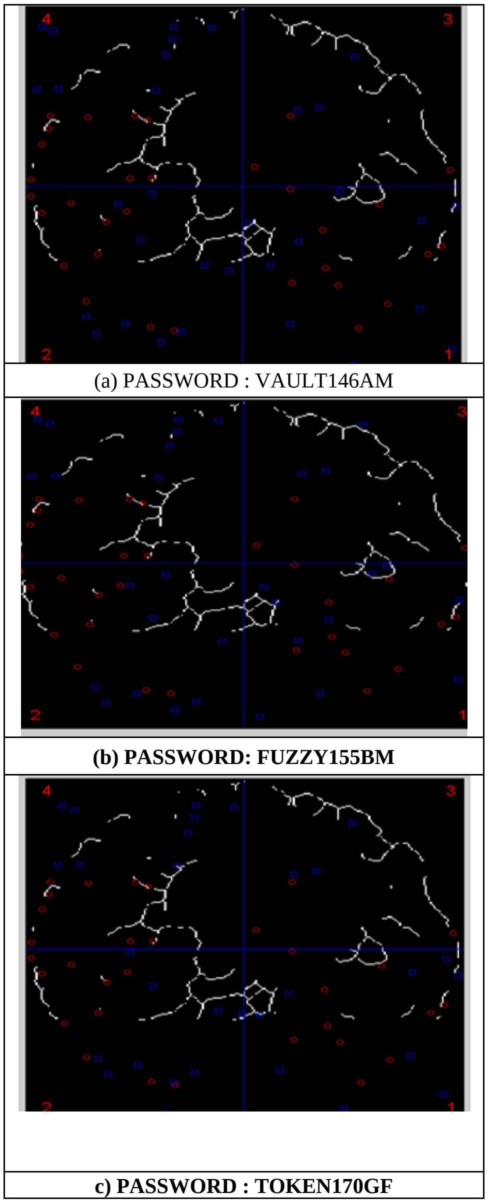
Table II: Eye Color and Character Code Representation

Eye Color	Character Code Used
Amber	A
Blue	E
Brown	B
Gray	G
Green	N
Hazel	H
Purple/violet	P

The security of the iris and retina vault is tabulated in Table. IV. 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 combined password hardened iris fuzzy vault is shown in Table IV.

Providing security [9, 10, 11, 12] to biometric template is very crucial due to the severe attacks targeted against biometric systems. This work attempts to provide multibiometric template security utilizing a hybrid template protection mechanism against stored biometric template attacks. Stored biometric template attack is the worst of all other attacks in a biometric system.



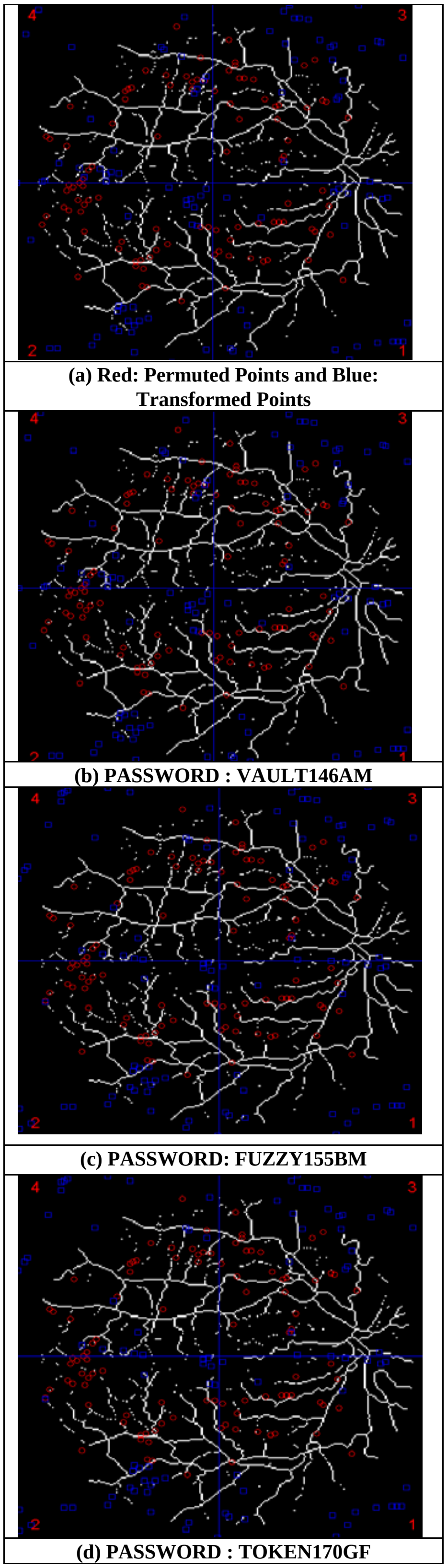
(a) PASSWORD : VAULT146AM

(b) PASSWORD: FUZZY155BM

c) PASSWORD : TOKEN170GF

Fig 4. Transformed Iris Features for Three Different Soft Biometric Passwords

The hardened retina based fuzzy vault is implemented in [21]. The multimodal fuzzy vault for fingerprint and iris was presented in [22]. The primitive idea of combined user and soft biometric password for iris is shown in [23]. The proposed work is an attempt to mix the ideas of soft biometrics and multibiometrics [13, 14] in providing stored biometric template security.



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

(b) PASSWORD : VAULT146AM

(c) PASSWORD: FUZZY155BM

(d) PASSWORD : TOKEN170GF

Fig 5. Transformed Retinal Features for Three Different Soft Biometric Passwords

Table III Showing the Structure of Sample Passwords

User password (5 character) (40 Bits)	**Soft Biometric Password (24 bits)**			**Combined Password (64 bits)**
	Height (0 – 255) (8 bit)	**Iris color (1 character) (8 bit)**	**Gender (M/F) (1 character) (8 bit)**	
FUZZY	155	B	M	FUZZY155BM
TOKEN	170	G	F	TOKEN170GF
VAULT	146	A	M	VAULT146AM

Table IV Security Analysis of Combined User and Soft Biometric based Password Hardened Multimodal Fuzzy Vault

Vault Type	**Degree of polynomial**	**Min-entropy of the vault (in security bits**	**Total no: of combinations tried**	**Combinations Required to decode the vault**	**No: of Evaluations To be performed to decode the vault**	**Min-entropy + guessing entropy of the password (in security bit)**
Iris	8	33	6.1088×10^{16}	6.9069×10^{6}	8.8445×10^{9}	51 to 63
Retina	8	33	1.1457×10^{17}	1.4307×10^{7}	8.0079×10^{9}	51 to 63
Combined Iris and Retina	13	51	1.8395×10^{28}	1.0143×10^{13}	1.8136×10^{15}	68 to 81

5. Conclusions

To resist against identity theft and security attacks it is very important to have a reliable identity management system. Biometrics play vital role in human authentication. However, biometric based authentication systems are vulnerable to a variety of attacks. Template attacks are more serious compared to other attacks. Single template protection scheme is not sufficient to resist the attacks. Hybrid scheme provide better security than their single counterpart. Fuzzy vault, which is a crypto biometric scheme, is modified by adding password hardening idea (salting) to impart more resistance towards attacks. Multi biometric fuzzy vaults can be implemented and again can be salted using passwords for achieving more security in terms of min-entropy. The only disadvantage of biometrics authentication as compared to traditional password based authentication is non revocability. Retina has certain advantage as compared to other biometrics and it is suitable for high security applications. Soft biometrics is ancillary information about a person, when combined with user password gives better results. It is very difficult for an attacker to gain both the biometric features, soft biometric components and user password at the same time. The user password can be changed for generating revocable biometric templates. In this implementation password acts as an additional layer of security. It is not possible for an attacker to gain the password and the fuzzy vault at the same time. Still better stable soft biometric components can be explored for better performance. This is an attempt to mix the ideas of password hardening, soft biometrics and multimodal biometrics for template security. Instead of using soft biometrics like height and weight which are prone to frequent changes, biometrics like fingerprint type and eye color can be used.

Acknowledgments

A public version of the DRIVE: Digital Retinal Images for Vessel Extraction is available from http://www.isi.uu.n/Research/Databases/DRIVE
A public version of the CUHK Iris Database is available from http://www2.acae.cuhk.edu.hk.

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] 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] 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] 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] Anil K. Jain, Sarat C. Dass, and Karthik Nandakumar, " Soft Biometric Traits for Personal Recognition Systems Proceedings of International Conference on Biometric Authentication", LNCS 3072, pp. 731- 738, Hong Kong, July 2004

[17] Anil K. Jain, Karthik Nandakumar, Xiaoguang Lu, and Unsang Park,"Integrating Faces, Fingerprints, and Soft Biometric Traits for User Recognition", Proceedings of Biometric Authentication Workshop, LNCS 3087, pp. 259-269, Prague, May 2004

[18] Anil K. Jain, Sarat C. Dass and Karthik Nandakumar, " Can soft biometric traits assist user recognition?", Proceedings of SPIE Vol. 5404, pp. 561-572, 2004.

[19] Anil K. Jain and Unsang Park," Facial Marks: Soft Biometric For Face Recognition", IEEE International Conference on Image Processing (ICIP), Cairo, Nov. 2009.

[20] Jung-Eun Lee, Anil K. Jain and Rong Jin, "Scars, Marks And Tattoos (Smt): Soft Biometric For Suspect And Victim Identification", Biometrics Symposium 2008

[21] V.S.Meenakshi, G.Padmavathi, "Security analysis of Password Hardened Retina based Fuzzy Vault", International Conference on Advances in Recent Technologies in Communication and Computing 2009, Kottayam, Kerala, India October 27-October 28 ISBN: 978-0-7695-3845-7, http://doi.ieeecomputersociety.org/10.1109/ARTCom 2009.101

[22] V.S.Meenakshi, G.Padmavathi, "Security analysis of Password Hardened Multimodal Biometric Fuzzy Vault", World Academy of Science, Engineering and Technology 56 2009, www.waset.org/journals/waset/v56/v56- 61.pdf

[23] V.S.Meenakshi, G.Padmavathi "Securing Iris Templates using Combined User and Soft Biometric based Password Hardened Fuzzy Vault" International Journal of Computer Science and Information Security, IJCSIS, Vol. 7, No. 2, pp. 001-008, ISSN 19475500 February 2010, USA

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 Associate Professor in the Department of Computer Applications, SNR Sons College, and Coimbatore. She has 17 years of teaching experience. She has presented nearly 15 papers in various national and international conferences. Her research interests are Biometrics, Biometric Template Security and Network Security.

Dr. Padmavathi Ganapathi is the Professor and Head of the Department of Computer Science, Avinashilingam University for Women, Coimbatore. She has 22 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 100 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.