

## The Role of ICT in our Daily Life Applications: Obstacles and Challenges

# Digital Security Using Multimodal Template Protection Schemes

Khaled Alfawaz

King Abdul-Aziz University, Jeddah Kingdom of Saudi Arabia

### ABSTRACT

The main issue of all the security and verification system is authentication and security by the user. This is needed to the enhancement of a mechanism which ensures users' privacy and security. This is a vast research area to develop security system in this field and different types of technologies have been proposed earlier. The conventional methods use tokens and passwords for providing security to the users and this system is compromised by hackers and also necessity to verification system design to ensure authentication and provide more security to the users. In recent years researchers have combined the key generation of cryptographic and biometrics method. The important features of biometrics are, it is a template which is not possible to revoke by an unauthorized person. The very familiar soft biometric features are the iris, retina, face, fingerprint, voice and so on. There is a cryptographic key generation technique Fuzzy Vault combine's soft biometrics. Providing more security to the users is necessary to avoid attacks. This technique gives an additional layer of security. Since this technique combines soft biometrics as well as cryptographic key generation which overcomes the limitation of biometric system when implemented individually. This paper proposes fuzzy vault scheme which uses retina as a soft biometric and gives best results when the performance is compared with other authentication system in ensuring the authentication.

**KEY WORDS:** SECURITY, BIOMETRICS, SOFT BIOMETRICS, NETWORK SECURITY, FINGER PRINT, RETINA

### INTRODUCTION

Soft biometric technology recognizes the persons with the help of biological or behavioral characteristics. The main advantages of soft biometric system are, it cannot be forgot or lost when compare with the conventional

system such as tokens and passwords. These new methods provide an innovative, also well suitable for the user information for identification and authentication. There are different stages for providing authentication to the users. The first step is enrollment of user. The process of this step is the user has to register their biometric

#### ARTICLE INFORMATION:


\*Corresponding Author: [kalfawaz@kau.edu.sa](mailto:kalfawaz@kau.edu.sa)

Received 3<sup>rd</sup> Nov, 2018

Accepted after revision 19<sup>th</sup> Dec, 2018

BBRC Print ISSN: 0974-6455

Online ISSN: 2321-4007 CODEN: USA BBRCBA

 Thomson Reuters ISI ESC / Clarivate Analytics USA and  
Crossref Indexed Journal

NAAS Journal Score 2018: 4.31 SJIF 2017: 4.196

© A Society of Science and Nature Publication, Bhopal India  
2018. All rights reserved.

Online Contents Available at: <http://www.bbrc.in/>

DOI: 10.21786/bbrc/12.1/15

features in different position for calculating in different measurement. The entire measurements are stored in a table after applied in some algorithm. Few of the biometric feature used for authentication is face, fingerprint, hand geometry, keystroke dynamics, hand vein, iris, retina, signature, voice, facial thermo gram, and DNA. The use of above mentioned biometrics is search the biometric templet from the table in a database and compare with the person who try to access the system. If the template matchers with the stored data and sensed data the system give the authentication to access it [1] [2] [3]. This system has both advantages and disadvantages. Once a biometric template of a user is stolen and the template not able to re-issue, destroy or update. Another disadvantage is one biometric system of a user can be used to access many systems, hence the attacker may easily access the system and utilize the data of the specific user. This is the major problem in the security.

As of late, novel cryptographic strategies, like fuzzy commitment and fuzzy vault has been proposed to give safe and secure storage [4] [5]. This fuzzy vault system uses biometric system along with randomly generated cryptographic key and it enhance the security like system authentication and access permission. This research paper concentrates a heuristic verification system of biometric, with the combination usage of soft biometrics features measurement and fuzzy vault scheme. According to the proposed approach, use retina as soft biometric template which is unaltered for entire lifetime of the user. Numerous testing were directed to inspect the execution of the proposed verification framework.

## RELATED WORK

Abhilasha et al [5] [6] [7] mentioned in their paper that vector space model has been used to create biometric key with cryptography. In vector space model the keys are kept secret and thus the system has more confidentiality in maintaining biometric data. This system use the advantages of biometric authentication. The second phase combines several authentication factors concurrently with soft biometric to provide more security. The main advantage of this system is, to authenticate using biometric any of the combination of factors may use. Their proposed method enhance the biometric data security and reliability. The challenges and issues of authentication system implementation is discussed by Uludag et al [10]. They proposed various methods combined with cryptographic key and template using biometric stored in the database for authentication. They assessed the performance for binding and generation algorithms using fingerprint. They revealed that it is very big challenges to generate biometric key due to extreme data acquisition variations. They provide more reliability and

suitability of this algorithm for digital rights management systems. Experimental results shown their performance and discussed in improving authentication. Cimato et al. [12] proposed a biometric authentication technique using multiple biometric data. The privacy of the document is guaranteed against loss or steal of the document since, the control of authentication can be performed offline and it is not possible to show any information. Proposed approach of them ensures security with high level as they are using various biometric data. These techniques are highly developed to make fast the security system and make it very convenient and coherent the process for identification. The combination of cryptography with soft biometrics increases the confidentiality using biometric templates which stored in the database for verification.

Hao et al [15] proposed a security system which combines iris soft biometric with cryptographic key for the first time. A string of binary data called as biometric key has been generated from the iris. This key created with a support of auxiliary error correction data from iris image, this cannot be disclosed and can be stored in a smart card [12] [13]. The regeneration of security key based on token and biometric of iris. So the system hacker in a position to retrieve the both keys. According to this paper, they applied and evaluated this strategy with 70 different samples of iris and 10 samples biometric data from left eye and right eye. From these samples they find out key with no error may be regenerated from a genuine point of iris with almost 99% rate successfully.

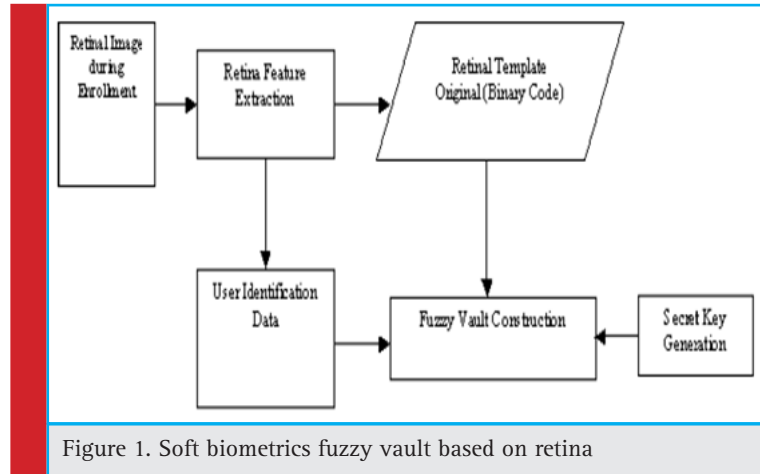
## PROPOSED APPROACH

Our fuzzy vault constructing based on the retina for biometric methodology followed three steps. The first step is the random transformation applied in to the retinal temple. This method provide the advantages for soft biometrics and fuzzy frame work, its enhance the high level security and privacy. The second template which got from the first step is secured using the application of fuzzy vault.

The third and final step consist the random generation of key from the template construct soft biometric measurement, password from the user and fuzzy vault. To provide the extra layer the password has been given. Fig 1 displays soft biometric tempering of fuzzy vault scheme based on the retina

### A. Feature Point Extraction – Retinal Bifurcation

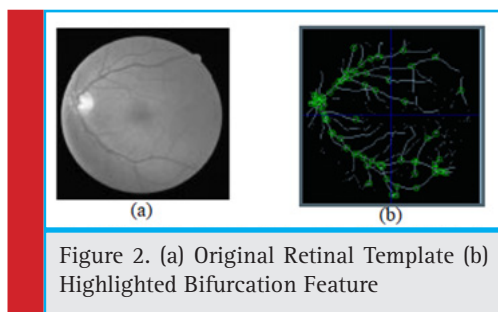
RBFPE technique is implemented by Chen et al. in [19] is followed in this paper. There is a need to extract the bifurcation from retina. The bifurcation point fixed and to retrieve the bifurcation feature. Again the bifurcation



points of retinal are extracted to improve the security and privacy.

Soft Biometrics traits are physical, behavioral or adhered human characteristics, classifiable in pre-defined human compliant categories like color, height, skin color, eye color, weight etc. is used in most of the research work. The fuzzy vault scheme and soft biometrics together exploit the performance of authentication now a days. In the proposed method bifurcation feature of retina retrieved from pattern of retina.

Thinning and Joining operations are applied into the retinal template as a major process. During this process the vascular pattern extracted. End of the this process from the retinal template, the bifurcation feature points are extracted, it is shown in the figure 2. The actual retinal template shown in figure 2a. After completion of the thinning and joining process the highlighted bifurcation feature points of retinal vascular tree shown in figure 2b.



### B. The Retinal Fuzzy Vault Hardening

This step is the tedious and significant step in the authentication design system to enhance security. All the templates stored in the database. During hardening the retinal fuzzy vault using password the sample of retinal are retrived from the database first and it has been resized depending upon the requirement. The system highlights

the feature points of retinal bifurcation to identify to lock or unlock data. The permutation and translation are subjected by the bifurcation feature points.

The primary and essential need of this procedure is to attain the parameters like  $(u, v, \theta)$ . Here  $u, v$  are proposes a row and column indicator of the image and  $\theta$  represent the orientation. This translated feature biometrics points are more secured in the fuzzy vault. It generate a 128 bit random key. A password with 64 bit is used to transform the randomly generated key. And also the same may be used for encrypting the vault

### C. Extracted Bifurcation Feature Transformation

Permutation, combination and translation are used to create the vascular tree and based on this only the bifurcation points are described. At the end of this operation a new points created from the original bifurcation transformation. Only a single character has been used for the password of the user. The password of the user character length is 8. So it occupies 64 bits. There is a limitation for the number of characters in the password. Only 8 characters of password length used in this research. So 64 bits are weighted for randomization totally. In this 16 bits, divided by 4 blocks. Every block comprising of 16 bit. The first five character is password and the remaining three characters are biometrics of the user. The implementation of proposed method we put VAULT as a password. Height of the user is the sixth character and gender as seventh character and the eighth characters is the color of iris.

At the first level implementation the bifurcation has been divided into four quadrants. All the quadrants is operated with a single password before permutation combination and translation process. The relative position cannot be changed in the bifurcation points. 2 bit block to be segmented of the each quadrant of 16 bits. The first one consist of nine bits and remaining has 7 bits. The  $T_u$  has seven bit and  $T_v$  has nine bits length. The

translation amount in the horizontal direction is  $T_u$  and vertical direction is  $T_v$ .

Fig 3 shows transformed retinal bifurcation points.

The new retinal point is derived from the followings:

$$X_{u'} = (X_u + T_u) \bmod (2^7)$$

$$Y_{v'} = (Y_v + T_v) \bmod (2^9)$$

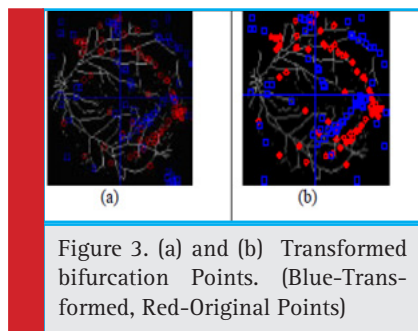
The distance in horizontal direction is  $X_u$  before transformation. Likewise the distance in horizontal direction after transformation is  $X_{u'}$ . Similarly,  $Y_v$  is the distances before transformation.  $Y_{v'}$  is the distance after transformation.

#### D. Encoding and Decoding the Vault

According to this stage it provide security to the the vault temporarily modified from the password. The proposed approach in this step replaces Reed-Solomon reconstruction step using Lagrange interpolation. For error detection the Cyclic Redundancy Check has used. The retrieved feature points are changed as binary strings. The chaff points generation method mentioned in [6][7] are used to implement this step. At the last the feature points obtained and it combined with chaff points to make imposter unaware of genuine points in the retina and the same reverse technique is used for vault decoding.

### TRANSMISSION WITH THE SECURITY

The generated key has been placed in to the application and it will be transmitted in the wireless networks. As the data size increased when apply the security, an existing sleep wake up method has been used to transfer from source to destination. In this method, only one node is active in a region and the remaining are in sleep state. During the transmission all the secured data transmitted from one active node to another active node.



### EXPERIMENTS AND RESULTS

This research method is implemented using MATLAB. The required parameters which are used in this is  $c$  denotes the count of the chaff points,  $r$  the count of the

genuine points. From this the total counts of points are  $(t+c)$ . When chaff points increases the privacy and security also increased. The number of chaff point declared in the system should be more than ten times. Then only the retinal templates will be available with the genuine points. The capable of being this work is evaluated using the retinal transforming template technique for biometric features and password given by the user. This research proposed to make use of eight character for security vault as mentioned above. The eight characters formed with the user password and the remaining characters are soft biometrics. Those eight character grouped into two parts and it consist five character as password. The sixth character is height of the user, seventh character represents the gender and eighth denotes the gender and iris color.

The table 1 shows an example transformation code obtained from soft biometrics and bifurcation feature points before transformation and after transformation. The 8 character has been taken for secure fuzzy vault. ASCII value of all the characters used in the implementation calculated. The five character password VAULT determined as 86, 65,85,76,84. The rest of the three characters are soft biometrics of the user. The ASCII value of height represents one parameter and gender for one parameter and iris color is one parameter. Many applications uses different password for cross matching purpose.

This proposed multimodal biometric key based network security in order to transfer data in a secure way and with the process of authentication and validation used secret key generated from the fused images of fingerprint, iris and retina. The evaluation of the proposed method is proved with three different metrics of false rejection rate (FRR), false acceptance rate (FAR) and the processing time of proposed method compared with the existing ones.

#### Performance Comparison of Proposed Multimodal Biometric Method with Single Biometric Based on False Rejection Rate in Network Security Systems

The metric FRR is defined as a percentage of real users which rejected by the biometric system. In authentication biometric system, the user of the system will make the claims of their identity, hence the security system must not reject an enrolled user and number of False Rejections must be kept as small as possible. Thus False Rejection must be minimized in comparison to False Acceptance.

The table 1 and figure 4 shows the performance of proposed fusion technique authentication system by varying the number of users which ranges from 1 to 100. From the result it is observed that the single biometric based authentication system fingerprint, iris and retina

Table 1. Feature Points						
1 <sup>st</sup> Quadrant and soft biometric features	Feature Points				Transformation code obtained from soft biometric	
	Before Transformation		After Transformation			
	Horizontal Distance Xu	Horizontal Distance Yv	Horizontal Distance Xu'	Horizontal Distance Yv'	Row index with respect to horizontal axis Tu	Column index with respect to horizontal axis Tv
'VAULT' Height=157 Iris Color='B' Gender='M'	105	18	55	84	78	322

Table 1. Performance Analysis of Proposed Method based on False Rejection Rate				
User	Finger print	Iris	Retina	Proposed Method
1 - 10	86.5	87.4	91.4	88.3
11 -20	88.5	82.9	93.5	83.2
21-30	91	87.8	93.2	86.2
31-40	90.7	88.3	91	87.6
41-50	91.7	91.3	93.8	90.3
51-60	85.2	84.6	89.8	83.7
61-70	90.5	88.8	92.5	86.7
71-80	89.3	86.8	91.7	84.4
81-90	90.3	87.9	93.8	86.4
91-100	90.9	89.2	93.6	88

Table 2. Performance Comparison of Proposed Fusion method with single biometrics based on False Acceptance Rate				
User	Finger print	Iris	Retina	Proposed Fused Image
1 - 10	0.43	0.48	0.38	0.11
11 -20	0.42	0.45	0.4	0.1
21-30	0.41	0.43	0.43	0.14
31-40	0.38	0.39	0.41	0.08
41-50	0.37	0.4	0.38	0.09
51-60	0.44	0.42	0.33	0.07
61-70	0.43	0.43	0.31	0.16
71-80	0.42	0.45	0.41	0.24
81-90	0.4	0.47	0.43	0.19
91-100	0.46	0.42	0.4	0.16

have less value of rejection rate while the proposed multimodal fusion method produce high false rejection rate and proved its performance is better than the others in validation and verification of network security.

**Performance comparison of proposed fusion method based security using False Acceptance Rate**

In biometric system based identification the users doesn't make claim about their identities. So it necessitates the

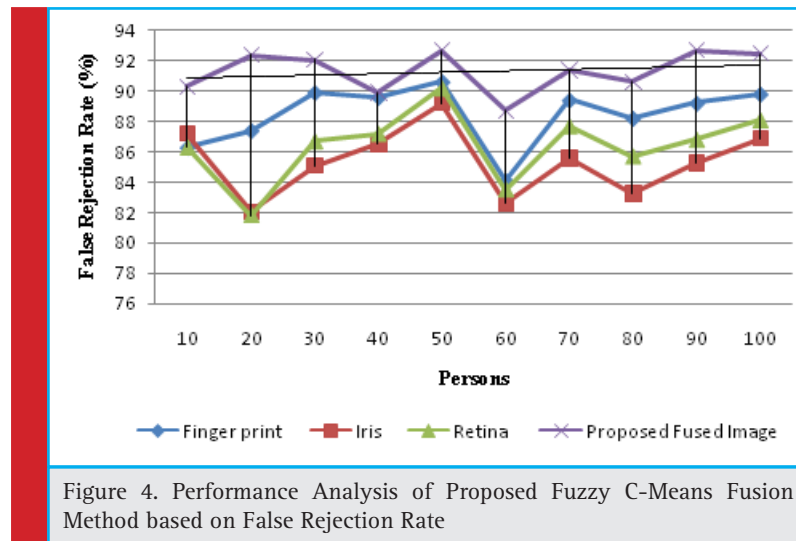


Figure 4. Performance Analysis of Proposed Fuzzy C-Means Fusion Method based on False Rejection Rate

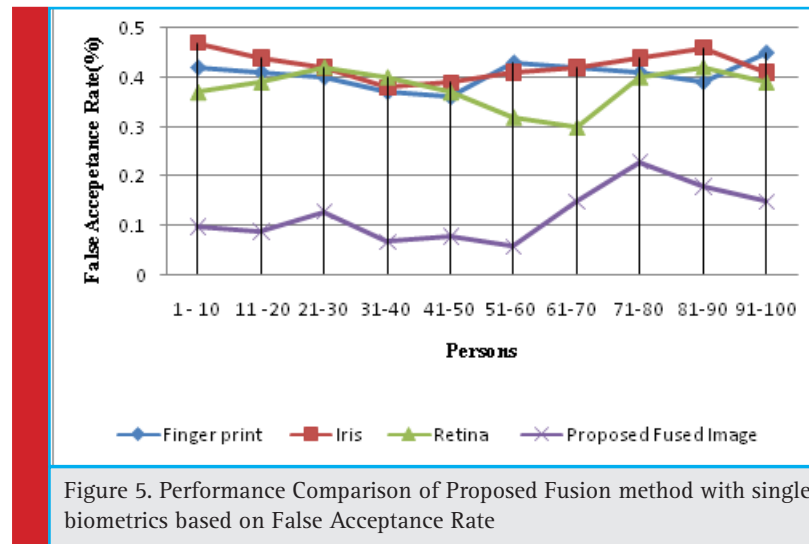


Figure 5. Performance Comparison of Proposed Fusion method with single biometrics based on False Acceptance Rate

importance of false acceptance rate must be smaller as much as possible so that the malicious users can not able to access the system under security. Thus the value of false acceptance rate must be considerably minimized comparing to false rejections

The table 2 and figure 5 depicts the performance of the proposed fusion technique false acceptance rate of the system by varying the number of users which ranges from 1 to 100. From the result it is observed that the single biometric based authentication holds the high value of false acceptance rate while the proposed multimodal biometric based authentication system produced low value of false acceptance. It proves that it is very hard to brute force the multimodal based key generation secure system.

## CONCLUSION

Even though there is no perfect accuracy technique for the past decades, lot of methods given by the researchers. The proposed research consist of proper design and implementation to enhance the overall security. The secure system should be more secure and as well as user friendly. The proposed method satisfies the more security and user friendly as it is the combination of soft biometrics features and framework taken from the cryptographic for verification. The advantage of this method is determination of retinal based genuine point is the challenge one for the hackers. Fuzzy vault frame work comprises the cryptographic key generation with soft biometrics. The password given by the user is additional layer to provide security. If anyone know the password it is not possible to match the biometric template developed by this method. In the future works the existing security system can be eradicated and the proposed sys-

tem can be implemented. In this work has been proposed with the 8 character from soft biometrics and password. In future there is many characters of human being can be increase. During the transmission life time, energy and efficiency has to be concentrated when apply these type of security. The convenience and adroitness may give higher level of security, as unapproved access would cut a shrewd gadget down and bargaining different endpoints on the system. The latest approaches not much suitable in IoT for user authentication. Though the classical security authentication provide adequate security, biometrics provide high level security for smart devices too.

## REFERENCES

- [1] K. Jain, L. Hong, and R. Bolle, O-line Fingerprint Verification, IEEE Transaction on Pattern Analysis and Machine Learning, vol. 19, no. 4, pp. 302-314, April 1997.
- [2] C Harris, M Stephens, A Combined Corner and Edge Detector, in Proceedings of the Alvey Vision Conference (University of Manchester, 1988), pp. 147-151
- [3] S Sukumaran, M Punithavalli, Retina recognition based on fractal dimension. IJCSNS Int J Comput Sci and Netw Secur. 9(10), 66-7 (2016)
- [4] M. A. Olsen, V. Smida, C. Busch, Finger image quality assessment features—definitions and evaluation *IET Biometrics*, 2015.
- [5] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, Generating Cancelable fingerprint templates, IEEE Transactions on Pattern Analysis and Machine Learning, vol. 29, no. 4, pp. 561-572, 2007.
- [6] Aujol, J. F., Aubert, G., Blanc-Féraud, L. and Chambolle, A, 2005 Image decomposition into a bounded variation component and an oscillating component Journal of Mathematical Imaging and Vision, Vol.22, No.1, pp.71-88.

- [7] Miles EP and Nuttall AL, 1993, Matched filter estimation of serial blood vessel diameters from video images IEEE Trans Med Imag, Vol. 12, No.2, pp. 147–152.
- [8] Abhilasha Bhargav-Spantzel, Anna Squicciarini, and Elisa Bertino, Privacy preserving multi-factor authentication with biometrics, Conference on Computer and Communications Security, pp. 63-72, 2006.
- [9] Maciej Szymkowski; Khalid Saeed, A novel approach to fingerprint identification using method of sectorization, International Conference on Biometrics and Kansei Engineering (ICBAKE), September 2017, pp: 55-59
- [10] M. Ortega, C. Mariño, M. G. Penedo, M. Blanco, and F.González, 2006, “Personal authentication based on feature extraction and optic nerve location in digital retinal images”. WSEAS Transactions on Computers, Vol.5, No.6, pp.1169–1176.
- [11] Jinyang shi, Zhiyang you, Ming gu and Kwok-yan lam, 2008, “Biomapping: Privacy TrustWorthy Biometrics Using Noninvertible and Discriminable Constructions”. in Proc. ICPR 2008.
- [12] J.J. Staal, M.D. Abramoff, M. Niemeijer, M.A. Viergever and B. van Ginneken, 2014, “Ridge based vessel segmentation in color images of the retina”. IEEE Transactions on Medical Imaging, Vol. 23, pp. 501-509.
- [13] Oechslin, Philippe (2003): Making a Faster Cryptanalytic Time-Memory Trade-Off, Laboratoires de Security et de Cryptography (LASEC), Ecole Polytechnic
- [14] Zalewski, Michal. Silence on the wire, a field guide to passive reconnaissance and indirect attacks. 2005, No Starch press.
- [15] Cransor, 2015 Lorrie Faith Cranor, Simson Garfinkel, “Security and usability: designing secure systems that people can use, O’Reilly Media, Inc., 2005, ISBN 0596008279
- [16] Lai. 2011 Lifeng Lai, Sui Wai Ho and H. Vicent Poor Privacy Security Trade-Offs in Biometric Security Systems - Part 2: Multi Use Case IEEE Transactions on Information Forensic and Security, Vol 6, No.1, March 2011
- [17] Jain, A., Bolle, R. and Pankanti S. (2009). Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers.
- [18] Srinivasa Reddy, and 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
- [19] Savvides, B. V. K. V. Kumar, and P. K. Khosla, Cancelable Biometric filters for face recognition, Proceedings of ICPR, Vol. 3, pp. 922-925, Cambridge, UK, September 2004