Retinal Biometrics based Authentication and Key Exchange System

K. Saraswathi
Assistant Professor
Post Graduate and Research
Department of Computer Science
Government Arts College
Coimbatore, India

B. Jayaram
Assistant Professor
Department of CSE
PA College of Engineering and
Technology
Pollachi, Coimbatore, India

Dr. R. Balasubramanian
Dean Academic Affairs
PPG Institute of Technology
Coimbatore, India

ABSTRACT

The growth and development of the Internet in the recent years has been very significant. But, the security and authentication is still a challenging problem. The security and authentication of the users in the Wireless LANs is also a serious issue. Hence, the security of the network users has become a vital factor. There are various techniques available in the literature which make use of passwords, smart cards etc., to provide network related security. But these conventional authentication systems have lot of limitations. Most recently biometric features like fingerprint and iris are also used to provide security to the network users. These biometric features are very reliable compared to the traditional methods. This paper proposes an approach for network security using a novel technique for personal authentication, where the biometric feature used for authentication is the retinal vessel tree. The configuration of the retinal vessels is unique for each individual and that it does not vary forever, so it can be used for the authentication purpose. The diverse phases included in this proposed approach are user registration, Extraction of retinal features, Retina Normalization and building secret key. The performance of the proposed approach is evaluated using the experimental observation. The simplicity and efficiency of the proposed method make it readily to be applied alone or incorporated with other existing security methods.

Keywords

Biometric Security, Cryptography, Data Security, Retinal Biometrics, Localization and Normalization.

1. INTRODUCTION

The security and the authentication of users is an prime concern in the network environments. Traditional security systems like Passwords or Personal Identification Numbers (PIN) and key devices like Smart cards cannot provide security and reliability in all the scenarios. The main problem with these traditional techniques is that there is possibility to forget the password. Moreover, if the password is known to others, the unauthorized user can have access to the accounts of the valid user. Biometric based user authentication techniques provide a best solution for the above mentioned problem. This technique is extremely reliable and secure. The authentication server is completely secure where biometric verification data are stored in a central database [1]. The security of the biometrics based authentication system provides better security and authentication. Fingerprint, hand geometry, face, retina, iris, DNA, signature and voice are the most widely used biometric features.

Biometrics is the technique of evaluating and statistically analyzing biological data that can be used to recognize various biometric features. Therefore, the biometric approach provides higher security. An automated process of identifying an individual based on the individual's biometric features is the biometric approach. The process of a biometric system is described in a three-step process. The initial step known as user registration involves an observation, or collection, of the biometric data. This step uses different sensors, which vary between modality, to make possible the observation. In the next step, the resultant or observed data is converted and described using a digital representation called a template. There is variation in this step between modalities and also between vendors. In the third step, the newly obtained template is compared with one or more previously generated templates stored in a database. This comparison result is gives the matching and the non-matching result and is used to identify the authenticated user [3].

The matching and non-matching results are obtained based on the template information which are similar but not exactly the same. A match result is measured by the threshold value. If the match score is below the threshold value then the biometric data is rejected or if the match score is above the threshold value, then the biometric data is accepted. The threshold can be varied so that the biometric system can be more or less rigorous, depending on the requirements of any given biometric application [3]. Fingerprints are the most widely used biometric features in the biometric authentication system. But, fingerprints and iris biometric features can be misused in some cases. So this type of security measures cannot be implied in military and such most secure fields.

A novel biometric approach is proposed in this paper to provide security to the network communication. The Retinal biometric characteristic is used in this paper. Retinal scan captures the pattern of eye’s blood vessels. Retina as a biometric has certain advantages when compared to other biometrics. It is very secure and uses a stable physiological feature. Retina is very difficult to spoof. Retinal patterns are different for right and left eye. They are unique even for identical twins. Moreover, retinal patterns do not change with age. Unlike other biometric behavior, the image will not fall on the retina for dead person. As retina is present deep within a person’s eyes it is extremely unlikely to be distorted by any environmental or temporal conditions. Therefore retina is a significant biometric feature for high security systems. Some limitations of iris biometrics can be removed by integrating it with retina. Image processing technique is utilized to extract the biometric measurement called minutiae from the user’s Retinal Tree. The Retinal image of the user is stored as encrypted binary template, which is used for authentication purpose. Biometric verification data of the user are first altered into a strong secret key and is then stored in the server’s database during registration. The performance measures are obtained by evaluating the proposed system.

The remainder of this paper is organized as follows. Section 2 discusses some of the related work in association with biometric based network security. Section 3 describes the proposed Retinal biometric based approach. Section 4 demonstrates the performance measures and Section 5 concludes the paper with discussions and future work.

2. RELATED WORK

There are several approaches available in the literature in the field of establishing network security based on biometric features obtained from individual user [4] [5]. Some of the approaches based on the biometric technique are discussed in this section.

Rahman et.al, [6] proposed a new design for secure access of computers inside an organization from a remote location. They used biometrics features and a onetime password method on top of secure socket layer (SSL) for authentication. Furthermore, they also provided three layers of security levels for network communication, and also a mechanism for secure file accesses based on the security privileges assigned to various users is proposed. The files to be accessed from the server are classified into categories depending on their access privileges and encrypted using a key assigned to each category.

Chung et.al, in [7] proposed an approach for secret key generation based on biometrics for protection technique. The integration of the user's identity and biometric feature data to an entity is provided by an authority through a digitally signed data structure called a biometric certificate. Hence, the main aim of this paper is to propose a novel technique for generating biometric digital key with biometric certificate on fuzzy fingerprint vault mechanism. Biometric digital key from biometric data has various applications such as automatic identification, user authentication with message encryption, etc. Hence, their work analyzed the correlated existing system and proposed a simplified technique where a general fuzzy fingerprint vault using biometric certificate with security consideration.

Dutta et.al, in [8] proposed a novel technique for providing network security using biometric and cryptography. The author proposed a biometrics based (fingerprint) Encryption/Decryption technique, in which unique key is generated using partial portion of combined sender's and receiver's fingerprints. A random sequence is produced from this unique key, which is used as an asymmetric key for both Encryption and Decryption. Above found unique Key is send by the sender after watermarking it in sender's fingerprint along with Encrypted Message. The computational requirement and network security features are explained. The main advantage of the proposed system is that, it need not have to search from a database and security is maintained.

Network security issues are projected by Benavente et.al, in [9]. The Internet is developing as a public vehicle for remote operations. Integrating biometric information in the authentication chain brings out new problems. Remote virtual identity (rvi) is starting to play in the way towards an e-Europe, and applications for e-government integrate biometrics. Remote identity of subjects should be explicitly stated. The use of biometric authentication systems in network applications, in order to provide end-to-end security across the authentication chain aliveness detection and fake-resistive methods, network protocols, security infrastructure, integration of biometrics and public key infrastructure (PKI), etc has been demonstrated by several features. Their paper describes a mid-layer interoperable architecture furnished with a set of generic interfaces and protocol definitions. This approach enables a future introduction of new modules and applications with a minimal development effort.

A novel fingerprint based security system was proposed and designed by Suriza et.al, in [10]. User authentication in traditional system provides an identification number or a password that is unique and well protected to assure the overall system security. This type of security system becomes very weak. Biometrics-based system provides a new and better approach to user authentication. Biometrics authentication can be explained as an automated technique in which an individual identity is confirmed by examining a unique physiological trait or behavioral characteristic, such as fingerprint, iris, or signature, since physiological traits have stable physical characteristics. The design and development of a fingerprint-based security system, comprising the scanner, interface system, Boltzmann machine neural network and access control system is discussed in this paper. The results obtained both for the testing and simulation studies of the integrated system with real-life physical system have demonstrated the practicality of such system as well as its potential applications in many fields

Ronald in [11] described an intelligent approach for password in network security using biometrics. Passwords are the most important means of authenticating network users. But, password authentication provides only limited security. User passwords are routinely forgotten, stolen, shared, or intercepted by hackers. In order to design better security systems, network administrators are replacing network passwords with smartcards, biometric authentication, or a combination of the three. Smart cards are credit card-size devices that generate different random numbers about every minute, in sync with counterparts on each entry point in the network. Smart cards work well as long as the card isn't stolen. A healthier choice to ensure network security is the use of biometrics. Their paper addressed the different biometric approaches available to determine a person's identity. Also described the criteria for selecting, a biometric security solution. In conclusion, efforts to establish the biometric industry standards (including standard application program interfaces (APIs)) were discussed.

A.B. J. Teoh et.al, in [12] proposed a biometrics formulation which is based on the concealment of random kernel and the iris images to synthesize minimum average correlation energy (MACE) filter for iris authentication. Particularly, the training images are multiplied with the user-specific random kernel in frequency domain before biometric filter is created. The main aim of the proposed technique is to provide private biometrics realization in iris authentication in which biometric template can be reissued once it was compromised. Meanwhile, the proposed method is able to decrease the computational load, due to the filter size reduction.

Kwanghyuk Bae et.al, [13] proposed a new feature extraction algorithm based on Independent Component Analysis (ICA) for iris recognition. A traditional method based on Gabor wavelets should select the parameters (e.g., orientation, spatial location and frequency) for fixed bases. ICA is applied to create optimal basis vectors for the problem of extracting efficient feature vectors which represent iris signals. The basis vectors learned by ICA are localized in both frequency and space like Gabor wavelets. As feature vector the coefficients of the ICA expansion are used. Then, each of the iris feature vector is encoded into an iris code. Experimental results show that the proposed method has a similar Equal Error Rate (EER) to a conventional method based on Gabor wavelets and two advantages: first, the size of an iris code and the processing time of the feature extraction are considerably reduced; and second, it is possible to evaluate the linear transform for feature extraction from the iris signals themselves.

3. METHODOLOGY

Biometric cryptosystems [14] is the integration of cryptography and biometrics techniques. The main aim of biometric cryptosystems is to promote strengths of both fields. Cryptography offers high and adjustable security levels; biometrics brings in non-repudiation and eliminates the disadvantages of the traditional authentication systems etc. In biometric cryptosystems, a unique cryptographic key is produced from the biometric template of a user which is stored in the database. This unique key cannot be accessed without a proper biometric authentication system.

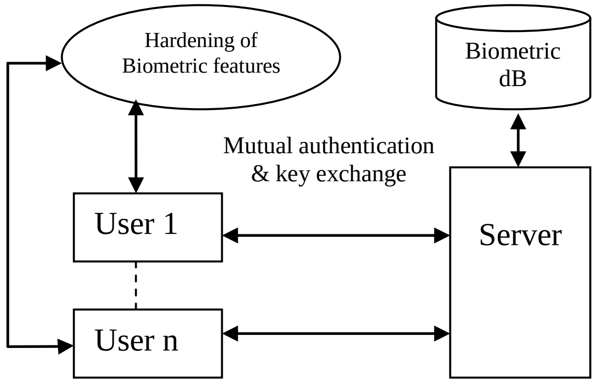


Fig 1.Biometric System

Figure 1 shows the overall structural design of the biometric system to improve network security. All the encrypted bifurcation point template of the user's retinal texture is stored in the database which is maintained in the Server. Users communicate with the server for the principle of user authentication, by providing the Retina texture of the user, which is transformed into a long secret detained by the server in its database [1].

Figure 2 shows extraction the minutiae points from biometric feature obtained from the user. The key vector is produced based on minutiae points (nodes and end points of retinal tree textures) are encountered in the given iris image [15]. Figure 2 displays various steps involved in the proposed system for network security using biometrics.

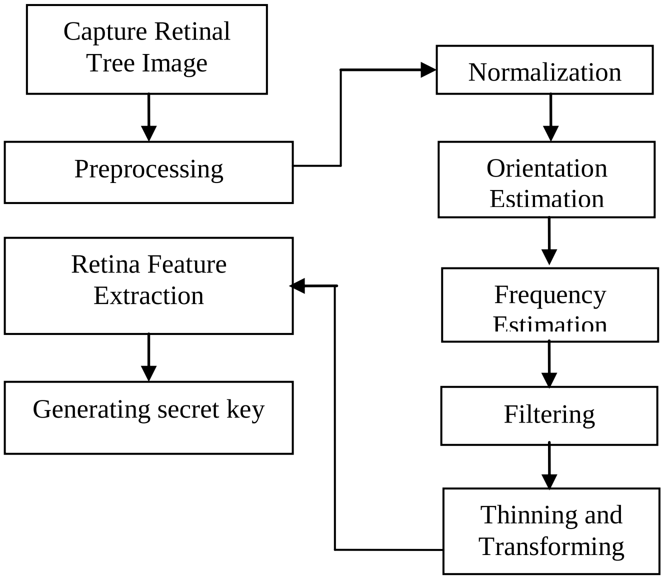


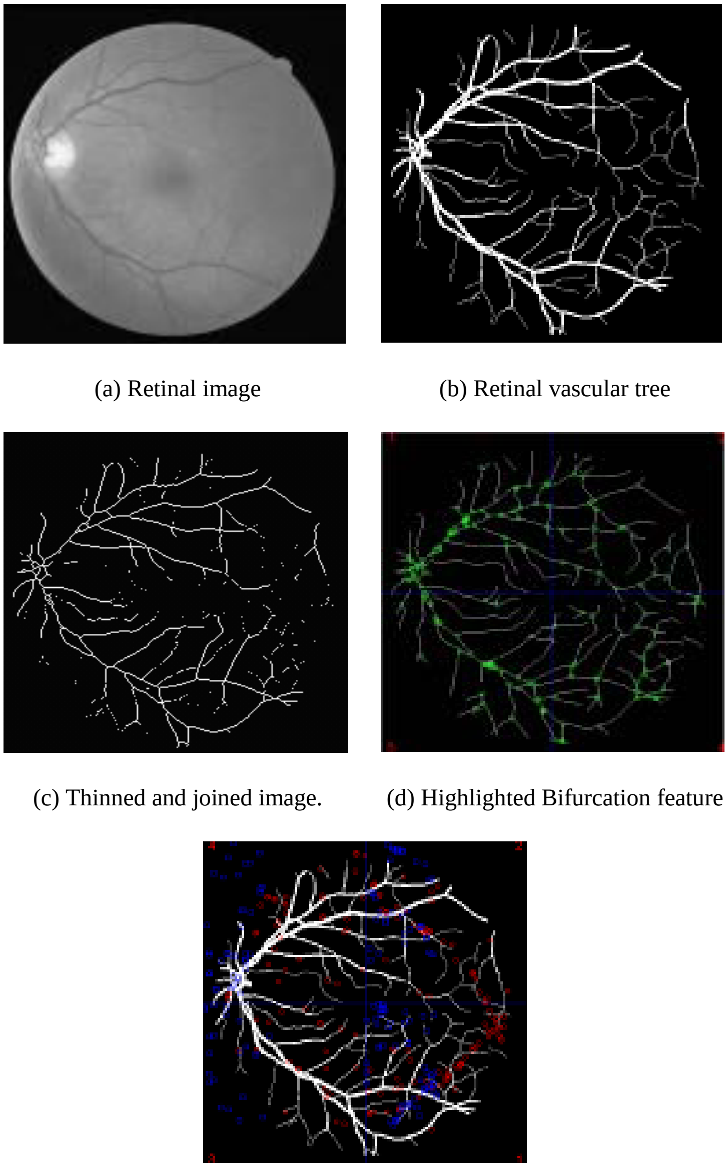
Fig 2 Steps involved in Extracting Feature Point

3.1 User Registration

This step widely called as Enrolment phase. To login into any security systems, the users provide their identity for the purpose of authentication. Hence a retina scanner is used to scan the retina of the user to reveal the user's identity for the first time. The obtained retina image undergoes a series of enhancement steps. This is described as follows.

3.2 Extraction of Feature point from Retina and Generation of Secret Key

The novel method of Li Chen [16] is used for extracting the bifurcation structure from retina. Thinning and joining morphological actions are done on the retinal texture. These operations highlight the retinal vascular patterns. Then the bifurcation feature points are obtained from the vascular patterns. The (x, y) co-ordinates of the bifurcation feature points of the retina is used for the creation of secret key.



(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

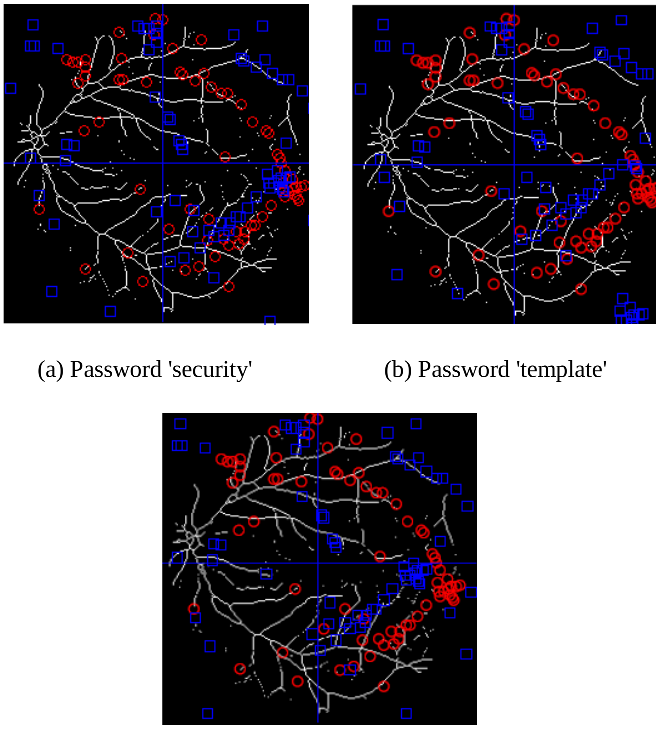
The permutation and translation operations are applied on the retinal vascular tree containing the highlighted bifurcation feature points. Fig 3(d) shows the feature point before transformation and Fig. 3(e) shows the feature point after transformation for retina. Thus new feature points are obtained from the original feature points. The user password is restricted with a constraint to the size of 8 characters. Hence, 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 iris template and retinal vascular tree is partitioned into 4 quadrants. Each quadrant is allocated with a one password block. Permutation is used in such a way that there is no change in the relative position of the feature point. Each 16 bit password block is divided into two components Tu of 7 bits and Tv of 9 bits in length. Tu and Tv denote the amount of translation in the horizontal and vertical directions, respectively.

The new feature points are obtained by the following transformation.

$$X'_u = (X_u + T_u) mod(2^7)$$

$$Y'_v = (Y_v + T_v) mod(2^9)$$

X_u and X'_u represent the horizontal distance between points before and after transformation respectively. Similarly Y_v and Y'_v denotes the vertical distance before and after transformation respectively. This transformation is applied for retina template.



(a) Password 'security'

(b) Password 'template'

(c) Password 'quadrant'

Fig 4. Transformed Retinal Features

3.3 Encoding

The transformed features are encoded in the server. Extra layer of security to the biometric database is provided by the password. The ridge and bifurcation points from retina are integrated together. Secret message is created as a 128 bit stream. This secret message is transformed with the password. The 16 bit CRC is added to transformed key S to obtain144 bit SC. The polynomial 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 eliminated in the combined set. x and y coordinates (each 8 bits) are concatenated to get 16 bit lock/unlock unit 'u'. The 'u' values are sorted and first N of them are selected. The Secret code (SC) is partitioned into 9 non overlapping segments of 16 bits each.

Each segment is altered to its decimal equivalent to account for the polynomial coefficients (C8, C7 …C0). All operations take place in Galois Field GF (216).

The projection of 'u' on polynomial 'p' is found. Now the Genuine points set G is (ui, P(ui)). Random chaff points are produced which are 10 times in number that of the genuine points. Both the genuine and chaff point sets are combined for the encoding.

3.4 Decoding

The encrypted data and bifurcation feature point are decrypted in the authentication phase by the user password. Password based transformation is applied to the query feature points and the dataserver 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 dataserver to separate the genuine point set for polynomial reconstruction. To decode the polynomial all combinations are tried from this set. Lagrangian interpolation method is used for polynomial reconstruction. For a particular 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 needed. If the combination set contains less than 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 doesn't match template image and the secret data cannot be extracted. If the remainder is not zero, then 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 128 bit secret data and the 16 bit CRC code.

Table 1 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’ ‘template’ ‘quadrant’	122	12	57 58 56	357 101 373	51 52 50	113 113 1
II ‘security’ ‘template’ ‘quadrant’	159	29	49 54 48	373 368 356	208 213 207	18 13 1
III ‘security’ ‘template’ ‘quadrant’	110	149	57 54 57	210 97 194	39 36 39	231 215 215
IV ‘security’ ‘template’ ‘quadrant’	181	227	116 58 110	121 101 116	169 169 163	220 200 215

This set is compared with the dataserver to separate the genuine point set for polynomial reconstruction. To decode the polynomial all combinations are tried from this set. Lagrangian interpolation method is used for polynomial reconstruction. For a particular 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 needed. If the combination set contains less than 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 doesn’t match template image and the secret data cannot be extracted. If the remainder is not zero, then 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 128 bit secret data and the 16 bit CRC code.

4. EXPERIMENTAL RESULTS

The polynomial projections are obtained from the vertical and horizontal distances of the retinal bifurcation features. The retinal template is altered for three different user passwords to check for revocability. The sample retinal bifurcation points from four quadrants after transformation using three different user passwords ‘security’, ‘template’ and ‘quadrant’ respectively is clearly shown in table 1. Fig.4 illustrates the password transformations.

Consider an 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 partitioned into four blocks of 16 bits each and these are further partitioned into 7 bits and 9 bits for transformation in horizontal and vertical directions respectively. The transformation of feature point is based on 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. Different transformed templates are acquired for the same original template when password is changed. This characteristic of password system provides revocability. Different passwords can be used for different applications to eliminate cross matching.

In modern biometrics, bifurcation points of retinal image can be captured, analyzed, and compared electronically, with relationship drawn between an original and a reference sample, as with other biometric approaches. There are two requirements for registration using retina. The user should get the biometric feature of the retina using suitable image processing techniques. The second is that the obtained feature should be encrypted with AES 128 bit symmetric cipher and is then transmitted to the server for storage in the database. Therefore, an outside attacker cannot detect the biometric feature by an exhaustive search either at the server side or by meet in the middle attack.

Table 2 False Rejection Rate (FRR) (%) Comparison

Degree of Polynomial	Without Hardening	Proposed
4	82.2	78.5
5	85.3	81.8
6	89.1	85.2
7	91.5	87.6
8	92.9	89.2
9	93.8	91.6

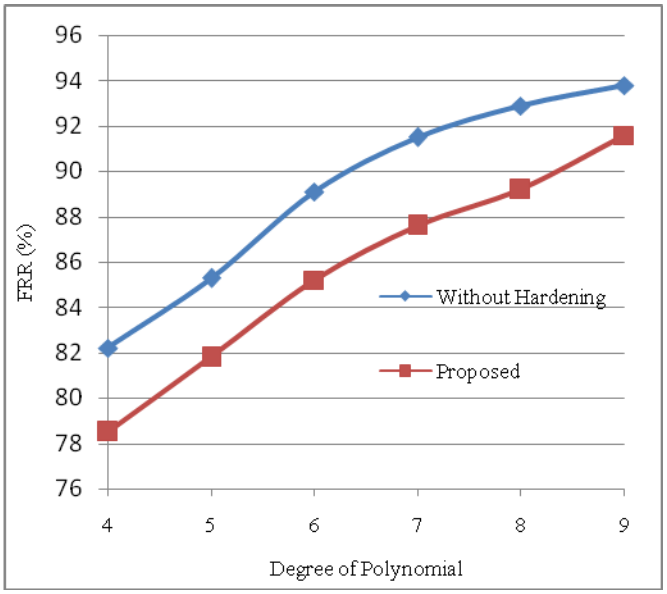


Fig 5. Resulted False Acceptance Rate

Table 3 False Acceptance Rate (FAR) (%) Comparison

Degree of Polynomial	Without Hardening	Proposed
4	0.31	0
5	0.26	0
6	0.17	0
7	0.11	0
8	0.06	0
9	0.02	0

Table 2 and figure 5 shows the resulted False Rejection Rate (FRR) for the proposed and existing technique. From the result, it can be observed that the proposed technique results in lesser False Rejection Rate when compared to the existing technique. Table 3 shows the resulted False Acceptance Rate (FAR) for the proposed and existing technique. From the result, it can be observed that the proposed technique results in False Acceptance Rate of 0 for all the Degree of Polynomial, whereas the existing techniques results with some percentage of False Acceptance Rate. From all the results obtained, it can be said that the proposed technique results in better security than the existing technique.

5. CONCLUSION

This paper proposes an approach for network security using Retinal biometrics feature. Biometric approaches are generally used for the authentication of physical assets or logical information (personal computer accounts etc). The human biometrics like can be efficiently used to ensure the network security. A cryptographic key is generated in the biometric system, from the biometric template of a user stored in the database in such a way that the key cannot be revealed without a proper biometric authentication. In this approach, the techniques in the areas of image processing are reused to extract the bifurcation points of retina biometric image. The preprocessing techniques explained in this paper play an vital role in enhancing the performance of the proposed biometric based network security system. The performance measures obtained clearly shows that the proposed method is very effective in providing network security. Hence, the proposed approach can utilized to support existing standard single-server biometric based security systems.

6. REFERENCES

[1] Rajeswari Mukesh, A. Damodaram, and V. Subbiah Bharathi, “Finger Print Based Authentication and Key Exchange System Secure Against Dictionary Attack,” IJCSNS International Journal of Computer Science and Network Security, Vol. 8, no. 10, pp. 14-20, 2008.

[2] T. Gunasekaran, and C. Parthasarathy, “Biometrics in Network Security,” International Journal of Computer Network and Security (IJCNS), vol. 1, no. 1, pp. 36-42, 2006.

[3] “Biometrics Security Considerations,” Systems and Network Analysis Center Information Assurance Directorate, www.nsa.gov/snac.

[4] P. Arul, and Dr. A. Shanmugam, “Generate A Key for AES Using Biometric for VOIP Network Security,” Journal of Theoretical and Applied Information Technology, pp. 107-112.

[5] S. Kasaei, and B. Boashash, “Fingerprint feature extraction using block-direction on reconstructed images,” In IEEE region TEN Conference on digital signal Processing applications, TENCON, pp. 303– 306, 1997.

[6] Mahfuzur Rahman, and Prabir Bhattacharya, “Secure Network Communication Using Biometrics,” IEEE International Conference on Multimedia and Expo (ICME'01), p. 52, 2001.

[7] Yunsu Chung, Kiyoung Moon, and Hyung-Woo Lee, “Biometric Certificate Based Biometric Digital Key Generation with Protection Mechanism,” Frontiers in the Convergence of Bioscience and Information Technologies, pp. 709-714, 2007.

[8] Sandip Dutta, Avijit Kar, N. C. Mahanti, and B. N. Chatterji, “Network Security Using Biometric and Cryptography,” Proceedings of the 10th International Conference on Advanced Concepts for Intelligent Vision Systems, pp. 38-44, 2008.

[9] O. S. Benavente, and R. Piccio-Marchetti, “Authentication services and biometrics: network security issues,” 39th Annual 2005 International Carnahan Conference on Security Technology, 2005. CCST '05, pp. 333-3336, 2005.

[10] Suriza Ahmad Zabidi, and Momoh-Jimoh E. Salami, “Design and Development of Intelligent Fingerprint-Based Security System,” Knowledge-Based Intelligent Information and Engineering Systems, vol. 3214, pp. 312-318, 2004.

[11] Ronald G. Wolak, “Network Security: Biometrics - The Password Alternative,” School of Computer and Information Sciences, 1998.

[12] S. C. Chong, A. B. J. Teoh, and D. C. L. Ngo, “Iris authentication using privatized advanced correlation filter,” in ICB, pages 382–388, 2006.

[13] K. Bae, S. Noh, and J. Kim, “Iris feature extraction using independent component analysis,” in Proceedings of the 4th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA ’03), vol. 2688, pp. 1059–1060,Guildford, UK, June 2003.

[14] Umut Uludag, Sharath Pankanti, Salil Prabhakar, and Anil K. Jain “Biometric Cryptosystems Issues and Challenges” Proceedings of the IEEE 2004.

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

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

AUTHOR BIOGRAPHY

K. Saraswathi received her B.Sc., and M.C.A., from Avinashilingam University, Coimbatore, TamilNadu, in 1993 and 1996 respectively. She obtained her M.Phil degree from Bharathiar University, Coimbatore, TamilNadu, in the year 2003. Currently she is working as Assistant Professor, Post Graduate and Research Department of Computer Science, Government Arts College, Coimbatore. She has the long experience of teaching post graduate and Graduate Students. She is currently pursuing her Research in the area of Crypto Systems under Mother Teresa University, Kodaikanal, TamilNadu. Her area of interest includes Biometrics, Cryptography, Network Security, Machine Learning and Artificial Intelligence. She has Co-authored a text book on ‘C’ published by Keerthi Publications. She has presented her publications in various international journals and conferences. She is a member of various professional bodies.

B. Jayaram obtained his M.E in Computer Science and Engineering in the year 2006 from Anna University, Chennai. He is currently working as Assistant Professor, Department of Computer Science & Engineering, PA College of Engineering and Technology, Pollachi. He has previously served as lecturer prior to this he had served as an active member of the development team in ERP products at Ramco Systems, Chennai. His area of interest includes data structure, computer networks, data mining, and biometrics.

Dr. R. Balasubramanian was born in 1947 in India. He obtained his B.Sc., and M.Sc., degree in Mathematics from Government Arts College, Coimbatore, TamilNadu, in 1967 and PSG Arts College, Coimbatore, TamilNadu, in 1969 respectively. He received his Ph.D., from PSG College of Technology, Coimbatore, TamilNadu, in the year 1990. He has published more than 15 research papers in national and international journals. He has been serving engineering educational service for the past four decades. He was formerly in PSG College of Technology, Coimbatore as Assistant Professor in the Department of Mathematics and Computer Applications. He served as Associate Dean of the Department of Computer Applications of Sri Krishna College of Engineering and Technology, Coimbatore. Currently taken charge as Dean Academic Affairs at PPG Institute of Technology, Coimbatore, before which he was a Dean Basic Sciences at Velammal Engineering College, Chennai. He has supervised one PhD thesis in Mathematics and supervising four doctoral works in Computer Applications. His mission is to impart quality, concept oriented education and mould younger generation.

He is member of the board of studies of many autonomous institutions and universities. He was the principal investigator of UGC sponsored research project. He is a referee of an international journal on mathematical modeling. He has authored a series of books on Engineering Mathematics and Computer Science. He is a life member of many professional bodies like ISTE, ISTAM and CSI.