IACSIT International Journal of Engineering and Technology, Vol.3, No.1, February 2011
ISSN: 1793-8236

Iris Biometrics Based Authentication and Key Exchange System

K. Saraswathi, B. Jayaram and Dr. R. Balasubramanian

Abstract—**Wireless Local Area Networks (WLANs) are gaining gratitude as they are fast, cost effective, supple and easy to use. The networks face severe issues and challenges in establishing security to the users' of the network. With users accessing networks remotely, exchanging data by means of the Internet and carrying around laptops containing sensitive data, ensuring security is an increasingly multifarious challenge. Therefore it is essential to make sure the security of the network users. In order to offer network security many techniques and systems have been proposed earlier in literature. Most of these traditional methods uses password, smart cards and so on to provide security to the network users. Though these traditional methods are effectual in ensuring security they posses some limitations too. This paper proposes an approach for network security by means of biometrics. As we all know biometric systems are generally used to control access to physical assets (laboratories, buildings, cash from ATMs, etc.) or logical information such as personal computer accounts, secure electronic documents etc., The human biometrics such as hand geometry, face, fingerprint, retina, iris, DNA, signature and voice can be effectively used to ensure the network security. The different phases included in this proposed approach are user registration, Extraction of minutiae points and secret key, Iris localization and Normalization. Furthermore, biometric authentication systems can be more opportune for the users since it involves no password that might be feared to be forgotten by the network users or key to be lost and therefore a single biometric trait (e.g. Iris) can be used to access several accounts without the burden of remembering passwords. In this paper the Iris biometric is used to provide security. This proposed paper also explains some of the Iris localization and Normalization techniques to make the biometric template noise free. Experiments are conducted to appraise the performance measure of the proposed approach.**

Index Terms—**Biometric Security, Cryptography, Data Security, Iris Biometrics, Localization and Normalization.**

I. Introduction

Accurate and automatic identification and authentication of users is an elemental problem in network environments. Communal secrets such as Personal Identification Numbers or Passwords and key devices like Smart cards are not just enough in some cases. This authentication method has habitually been based on passwords. The trouble with these traditional approaches is that there is possibility to forget the password. Moreover, compromised password directs to a fact, that unauthorized user can have access to the accounts of the valid user. The Biometric based user authentication systems are very much secured and efficient to use and place total trust on the authentication server where biometric verification data are stored in a central database [1]. This biometrics based user authentication system improves the network security. Some of most extensively used biometric are hand geometry, face, fingerprint, retina, iris, DNA, signature and voice.

Biometrics is the knowledge of measuring and statistically analyzing Biological data can be used to recognize different body parts like the eyes, fingerprints, facial characteristics, voice, iris etc. Thus, it takes security to the next level by not just confining it to authenticating passwords, iris matching techniques [2]. A biometric system provides an automated method of recognizing an individual based on the individual's biometric characteristics. The process of a biometric system can be described, in a beginner's manner, by a three-step process. The initial step in this process involves an observation, or collection, of the biometric data which is formally known as user registration. This step uses different sensors, which vary between modality, to make possible the observation. The second step converts and describes the experimental data using a digital representation called a template. This pace varies between modalities and also between vendors. In the third step, the recently acquired template is compared with one or more previously generated templates stored in a database. The consequence of this comparison is a "match" or a "non-match" and is used for actions such as permitting access, sounding an alarm, etc [3].

Finalizing a match or non-match is based on the obtained resultant template being analogous, but not one and the same, to the stored template. A threshold determines the gauge of similarity necessary to result in a match declaration. The recognition or rejection of biometric data is completely dependent on the match score falling above or below the threshold. The threshold is changeable so that the biometric system can be more or less stringent, depending on the requirements of any given biometric application [3]. Amongst all the biometric techniques, today fingerprints are the most widely used biometric features for personal identification because of their high acceptability, Immutability and individuality.

This paper proposes a new technique to secure the network communication using biometric characteristics obtained from the individuals. The biometric characteristic used in this paper is Iris. This proposed paper utilizes image processing technique to haul out the biometric measurement called minutiae from the user's Iris. The user's individual iris image is converted and stored as encrypted binary

K. Saraswathi, Asst.Proffessor is with the Department of Computer Science, Govt Arts College, Udumalpet, Tirupur, India.

B. Jayaram, Asst.Proffessor is with the Department of Computer Science & Engineering, PA College of Engineering and Technology,Pollachi,Coimbatore,India

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

template, which is used for authentication by the server of the network. The user's biometric authentication data are first transformed into a strong secret and is then stored in the server's database during registration. The proposed system is evaluated to establish the performance measures.

The remainder sections of this paper are organized as follows. Section 2 discusses a few of the related work proposed earlier in association to biometric based network security. Section 3 describes the proposed idea of providing network security using the biometric characteristics obtained iris. Section 4 illustrates the performance measures and finally section 5 concludes the paper with directions to future work.

II. Related Work

A lot of research work has been performed in the field of establishing network security based on biometric features obtained from individual user [14] [15]. This section of the paper discusses a few of the related work proposed earlier in association to biometric based network security.

In their work [4] Rahman et al. proposed design for secure access of computers inside an organization from a remote location. They used biometrics features and a one-time 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 categorized based on their access privileges and encrypted using a key assigned to each category. The test results of their approach evaluated the performance measure of their proposed approach.

Chung et al. in [5] described a technique for biometric based secret key generation for protection mechanism. The strap 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. Therefore, the main objective (or contribution) of their work is to propose a simple method for generating biometric digital key with biometric certificate on fuzzy fingerprint vault mechanism. Biometric digital key from biometric data has a lot of applications such as automatic identification, user authentication with message encryption, etc. Therefore, their work analyzed the associated scheme and proposed a simplified model where a general fuzzy fingerprint vault using biometric certificate with security consideration.

Dutta et al. in [6] presented a new method for providing network security using biometric and cryptography. They proposed a biometrics-based (for e.g. fingerprint) Encryption/Decryption method, in which unique key is generated using partial portion of combined sender's and receiver's fingerprints. From this inimitable key a random sequence is generated, which is used as an asymmetric key for both Encryption and Decryption. Above inimitable 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 described. Proposed system has a benefit that for public key, it has not to search from a database and security is maintained.

Network security issues are projected by Benavente et al. in [7]. The Internet is more and more becoming a public vehicle for remote operations. Integrating biometric information in the validation chain exposes new problems. Remote unrealistic identity is starting to play in the way towards an e-Europe, and applications for e-government integrate biometrics. Remote identity of subjects should be unambiguously stated. Numerous features drive the spread of biometric authentication 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. Their paper proposed a mid-layer interoperable design furnished with a set of generic interfaces and protocol definitions. Their scheme enables an upcoming introduction of new modules and applications with a minimal development effort.

A.B. J. Teoh et al. in [18] presented a private 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. Specifically, the training images are multiplied with the user-specific random kernel in frequency domain before biometric filter is created. The objective of their proposed method is to provide private biometrics realization in their iris authentication in which biometric template can be reissued once it was compromised. Meanwhile, their proposed method is able to decrease the computational load, due to the filter size reduction.

Kwanghyuk Bae et al [19] proposed a new feature extraction algorithm based on Independent Component Analysis (ICA) for iris recognition. A conventional method based on Gabor wavelets should select the parameters (e.g., spatial location, orientation, and frequency) for fixed bases. ICA is applied to generate 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 space and frequency like Gabor wavelets. The coefficients of the ICA expansion are used as feature vector. Then, each iris feature vector is encoded into an iris code. Experimental results[19] 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 significantly reduced; and second, it is possible to estimate the linear transform for feature extraction from the iris signals themselves.

An intelligent fingerprint based on the security system was designed and developed by Suriza et al. in [8]. Traditionally, user authentication is intended to provide an identification number or a password that is unique and well protected to assure the overall system security. This type of security system is very delicate in an area where a higher level of security system is required. Biometrics-based system brings a new and better approach to user authentication. Biometrics authentication is a mechanized method whereby 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 integration between the hardware and the software is accomplished by using Visual Basic 6 programming language. The results obtained mutually for the simulation studies and testing of the incorporated system with real-life physical system have demonstrated the practicality of such system as well as its potential applications in many fields

Ronald in [9] put forth an alternative approach for password in network security using biometrics. Passwords are the most important means of authenticating network users. However, network administrators are becoming alarmed about the limited security provided by password authentication. Many administrators are now finalising that their password-based security systems are not all that secure. User passwords are habitually stolen, forgotten, shared, or intercepted by hackers. Another serious problem is that computer users have become too trusting. They routinely use the same password to enter both secure and insecure Web sites as well as their networks at work. In response to the proven lack of security provided by password authentication, network administrators are replacing network passwords with smartcards, biometric authentication, or a combination of the three. Smart cards are credit card-size devices that engender 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 better choice to ensure network security is the use of biometrics. Their paper investigated the different biometric techniques on hand to determine a person's identity. Also described, were the criteria for selecting a biometric security solution. In conclusion, efforts to set up biometric industry standards (including standard application program interfaces (APIs)) were discussed.

III. Proposed Approach

Biometric cryptosystems [10] join together cryptography and biometrics to promote from the strengths of both fields. In such systems, whereas cryptography provides high and adjustable security levels, biometrics brings in non-repudiation and eliminates the must to remember passwords or to carry tokens etc. In biometric cryptosystems, a cryptographic key is formed from the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication.

The overall architecture of the biometric system to advance the network security is shown in figure 1. The Server preserves a database where the encrypted minutia template of the user's Iris texture is stored. In this arrangement, users communicate with the server for the principle of user authentication, by rendering users' iris, which is transformed into a long secret detained by the server in its database [1].

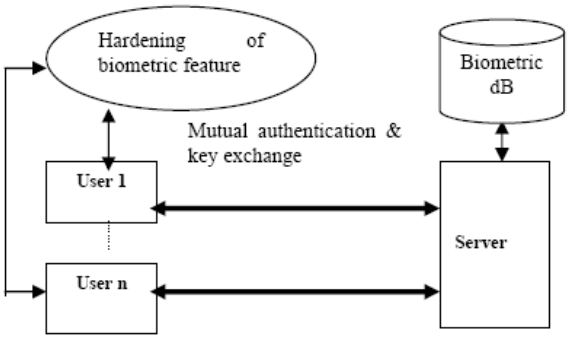


Figure 1.Biometric System

Figure 2 shows a familiar idea of obtaining the minutiae points from biometric feature obtained from the user. The key vector is formed based on minutiae points (nodes and end points of iris textures) are encountered in the given iris image [11]. Figure 2 shows a variety of steps involved in the proposed system for network security using biometrics.

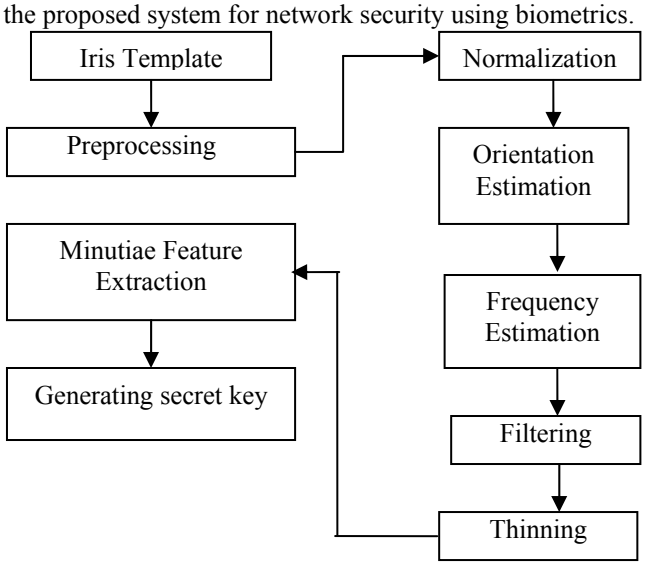


Figure 2 Steps involved in Extracting Feature Point

A. User Registration

This step is popularly known as Enrolment phase. In all the security system to enroll as a rightful user in a service, a user must previously register with the service provider by ascertaining his/her identity with the provider. Therefore a scanner is used to scan the iris of the user to reveal his/her identity for the first time. The iris image therefore obtained undergoes a series of enhancement steps. This is described in the subsequent section of this proposed paper.

B. Extraction of Minutiae and Secret Key

Iris Localization and Normalization:

We use the iris image data base from CASIA Iris image Database [CAS03a] and MMU Iris Database [MMU04a]. CASIA Iris Image Data base contributes a total number of 756 iris image which were taken in two different time frames. Every iris images is 8-bit gray scale with resolution 320 X 280. MMU data base consist a total number of 450 iris images which were captured by LG Iris Access®2200.

Canny edge detection is performed mutually in vertical direction and horizontal directions as suggested by Wildes et a [11]. The iris images found in CASIA database has iris radius 80 to 150 and pupil radius from 30 to 75 pixels, which were found manually and given to the Hough

transform. If we perform Hough transform first for iris/sclera boundary and then to iris/pupil boundary then the results are accurate. The output of this step results in storing the radius and x, y parameters of inner and outer circles.

Canny edge detection is used to construct edges in horizontal direction and then Hough transform is implemented on it. If the maximum Hough space is less than the threshold it represents non occlusion of eyelids. For isolating eyelashes it is easier by using thresholding, since they are darker when compared with other elements in eye. The eye images collected from the above database are of gray scale and their contrast is enhanced using histogram equalization.

Fig 3 Localized iris image

Daugman [12] suggested normal Cartesian to polar transformation that maps each pixel in the iris area into a pair of polar coordinates(r, θ), where r and θ are on the intervals of [0 1] and [0 2π].

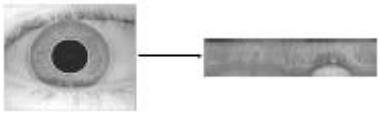


Fig 4 Normalized Iris

C. Generation of Secret Key

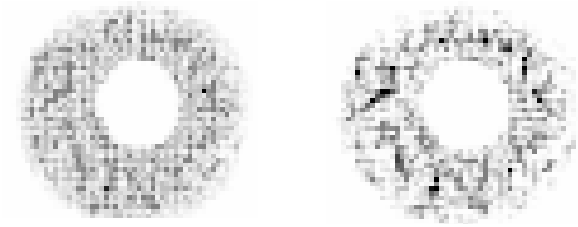
A typical iris exhibits rich texture information in the immediate vicinity of the pupil which tapers away in intensity as one move away from the pupil. Similarly there is a chance of having noise in iris patterns at top an bottom rows even after preprocessing. Also the iris pixels near the pupil have more variations than those of farther from the pupil. Thus after leaving 3 rows of patterns both at bottom and top, remaining rows are sued to extract the key.

D. Extraction of Lock/Unlock Data

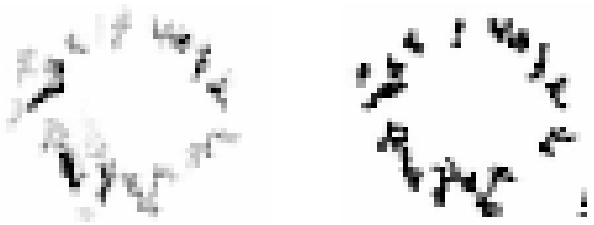
On the highlighted iris structures as a whole, the following sequence of morphological operations [13] is used to extract the pseudo structures.

Close – by - reconstruction top-hat (figure 5(a)) opening (figure 5(b)), area opening to remove structures in according to its size resulting image with structures disposed in layers (figure 5(c)) and thresholding is applied to obtain binary image.

For appropriate representation of structures, thinning is used so that it presents every structure itself as an agglomerate of pixels. It is shown in figure 6.



(a) Closing-by-tophat (b) Opening



c) Thresholded images

Figure 5 Morphological operations on Iris Textures

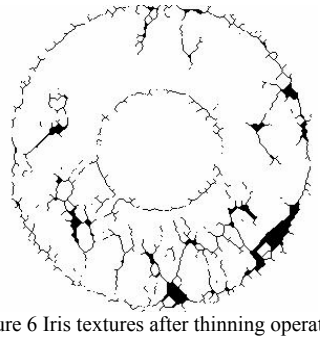


Figure 6 Iris textures after thinning operation

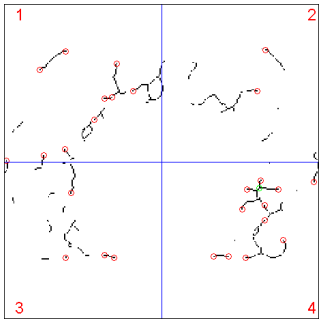


Figure 7(a) Minutiae representation of Nodes and end points are shown in circles.

From the above iris rim containing iris pseudo textures, the polar coordinates of minutiae (nodes and end points of iris textures) are extracted by resizing the image into a standard format of 256 x 256 as shown in figure 7.

IV. Implementation

The implementation stage consists of three operations, namely transformation, encoding and finally decoding.

(a) Transformation:

Simple operations such as translation and permutation are used to transform the original minutiae features into new minutiae. The password given by the user is limited to 8 characters so that its length is 64 bits, which is divided into 4 blocks of each 16bits length. Similarly iris circular rim containing minutiae is divided into 4 quadrants as shown in figure 7(a) and for each quadrant one password block is

assigned. The 4 quadrants are permuted such that relative positions of the minutiae within each quadrant are not changed as shown in figure 7(b).

Each password block is divided into two components T_r of 7 bits and T_θ of 9 bits length. Where T_r is the translation in radial direction and T_θ is in angular direction. These translation values are added to original values modulo the appropriate range

$$Q_r' = (Q_r + T_r) mod (2^7)$$
$$Q_\theta' = (Q_\theta + T_\theta) mod (2^9)$$

Where Q_r and Q_r' are the radial values before and after transmission respectively. Similarly Q_θ and Q_θ' are the angular values before and after transformation respectively.

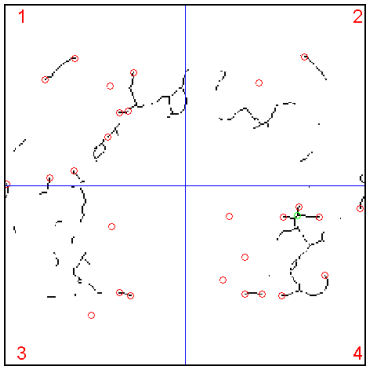


Figure 7(b) Minutiae before and after permutation

(b) Encoding:

The transformed minutiae are encoded in the database using the same procedure that is described earlier section. This layer of encryption prevents an imposter without knowledge of the password from modifying the database.

(c) Decoding:

During authentication phase, the encrypted database and the minutiae data are decrypted using the password given by the user. The template and query data sets are aligned and the password based transformation is applied to these query minutiae and used for unlocking the database.

(d) *The Iris Authentication Protocol*

To initiate a request for service, user computes his FP1 = E_{AES}(FP), where FP is the iris template, then the user sends the user ID along with FP1 to the server. In Lee et al.[16]'s protocol, the authority selects two large prime numbers p and q, where q|p-1. Let g be an element of order q in GF(p). Assume H(...) is a collision-free hash function with an output of q bits. The secret key of the sender S is $X_S \in Zq^*$ and $Y_S = g^{X_S} \bmod p$ is the corresponding public key. Similarly, (X_R, Y_R) is the key pair of the receiver R, where $X_R \in Zq^*$ and $Y_R \in gX_R \bmod p$. The symbol "||" is the concatenate operator of strings. In this work, Li Gang's[17] protocol is adopted to implement the authentication protocol.

Let t1 and t2 be the minutiae template of FP1 and FP2,

Step 1. S chooses t, $t1 \in {}_RZq^*$ and computes $r=g^t \bmod p$, $r_1=g^{t1} \bmod p$ and $\sigma_1=H(r||T)X_S+t_1r_1 \bmod q$, where T is a time stamp, and then he sends (r, T, r1,σ1) to R;

Step 2. R checks whether $g^{\sigma 1} \equiv Y_s^{H(r||T)} r_1 \bmod p$. If not, R stops. Otherwise, R chooses $t_2 \in {}_RZ_q^*$ and computes $r_2 = g^{t2} \bmod p$ and σ_2 $H(r||T)$ $X_R+t_2r_2 \bmod q$, and then he sends(r,T,r2, σ2) to S;

Step 3. S verifies whether $g^{\sigma 2} \equiv Y_R^{H(r||T)} r_2 \bmod p$.

If not, S stops. Otherwise, S computes

$\sigma=H(M||T)X_S+tr \bmod q$,

$k=(Y_R)^\sigma \bmod p$

and $MAC=H(k||M||T||r_1||\sigma_1||r_2||\sigma_2)$. Finally, S sends MAC with M to R;

Step 4. R computes $k'=(Y_s^{H(M||T)}r^r \bmod p$ and verifies whether $H(k'||M||T||r_1||\sigma_1||\ r_2||\sigma_2)=MAC$.

If the above equation holds, R accepts it. Otherwise, R rejects it and authentication becomes fail. These are the different steps involved in designing a iris based biometric authentication system for network security.

V. Performance Measures

This section of the paper explains the performance measures of our approach. The Iris processing has been done using CASIA and CUHK Iris datasets [18, 19] in MATLAB. The polar indices Q_r (radial value) and Q_θ (angular value) of nodes and end points are used for projections of the polynomial. Nodes and end points are shown in the Figure 7 which was obtained after a sequence of morphological operations. Some of the minutiae extracted from a sample iris are shown in table 1. Password used for the transformation is 'FEATURES'.

Where 1 represents ridge ending point and 0 represent secluded point in an iris image. The performance measures obtained, exposed that the proposed method effectively provides network security. Therefore it can be directly applied to strengthen existing standard single-server biometric based security applications. In the context of modern biometrics, these features, called iris minutiae, can be captured, analyzed, and compared electronically, with correlations drawn between a live sample and a reference sample, as with other biometric technologies. There are two requirements for registration using iris. The user should obtain the biometric feature from his iris using appropriate image processing techniques as one mentioned in the previous section.

TABLE I MINUTIAE EXTRACTED FROM A IRIS TEXTURE

Quadrant	Distance Q_r (7 –bits)	Orientation Q_θ (9-bits)	Minutiae Value (16-bits)
I.	41	54	0101001 000110110
II.	99	8	1100011 000001000
III.	94	140	1011110 010001100
IV.	18	158	0010010 010011110

The second is that the minutia template supposed to be encrypted with AES 128 bit symmetric cipher and is then transmitted to the server for storage in the database, so that it should not be possible for an outside attacker to determine the biometric feature by an exhaustive search either at the server side or by meet in the middle attack.

Existing system and the proposed system are compared by the wrongly matched samples. The observations are made for the Iris datasets [18, 19] and the wrongly matched templates are noted. This is presented in table 2.

TABLE II WRONGLY MATCHED TEMPLATE

Number of Templates	Existing approach	Proposed approach
150	11	3
300	18	11
450	31	20
600	43	29

From table 2 it can be observed that the proposed approach has very less wrong matching when compared to the existing approach. The comparison is given in the figure 8.

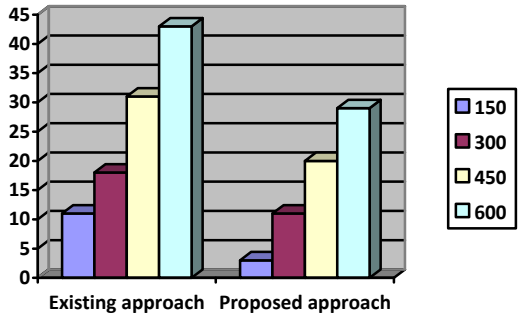


Fig 8 comparison of existing and proposed approach with wrong matching

The figure clearly illustrates that the proposed approach have very less wrong matching even when the number of samples is high.

VI. CONCLUSION

This paper proposes an approach for network security by means of biometrics. Biometric systems are commonly used to organize accessing of physical assets such as laboratories, buildings, cash from ATMs, etc., or logical information such as personal computer accounts, secure electronic documents, etc. The human biometrics like fingerprint, hand geometry, face, retina, iris, DNA, signature and voice can be effectively used to ensure the network security. In biometric cryptosystems, a cryptographic key is obtained from the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication. In this system, the concept in the areas of image processing technique is reused to extract the minutiae from Iris biometric image. The preprocessing techniques projected in this paper play an important role in improving the performance of the proposed biometric based network security system. The performance measures obtained exposed that the proposed method effectively provides network security. Therefore it can be directly applied to strengthen existing standard single-server biometric based security applications.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

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

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

[12] J. Daugman, "How iris recognition Works," in *IEEE Transactions on Circuits and Systems for video Technology*, vol.14, no.1, pp21-30, January 2004.

[13] H. Heijmans, Morphological Image Operators, Academy Press, 1994.

[14] 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.

[15] 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.

[16] N. K. Ratha, J. H. Connell, and R. M. Bolle "Enhancing security and privacy in biometrics based authentication systems", IBM Systems Journal, vol. 40, pp. 614-634, 2001.

[17] Alexander P. Pons , and Peter Polak, "Understanding user perspectives on biometric technology," Communications of the ACM, vol. 51, no. 9, pp. 115-118, September 2008.

[18] 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.

[19] 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.

[20] Bansal, Atul; Agarwal, Ravinder; Sharma, R.K., "Trends in Iris Recognition Algorithms", International Conference on Mathematical/Analytical Modelling and Computer Simulation (AMS), 2010, Publication Year: 2010 , Pp: 337 - 340

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, Department of Computer Science, Government Arts College, Udumalpet. 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 national 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.