Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

A Survey on Biometrics based Key Authentication using Neural Network

Dr. P.M.Gomathi[1]

[1] Anna University, Coimbatore

Received: 1 May 2011 Accepted: 27 May 2011 Published: 8 June 2011

Abstract

Abstracts -The conventional method for user authentication is a password known to the user only.There is no security in the use of passwords if the password is known to an imposter and also it can be forgotten. So it is necessary to develop a better security system. Hence, to improve the user authentication passwords are replaced with biometric identification of the user. Thus usage of biometrics in authentication system becomes a vital technique. Biometric scheme are being widely employed because of their security merits over the earlier authentication system based on records that can be easily lost, guessed or forged. This is because the biometrics is unique for every individual and is complex than passwords. Commonly used biometrics is fingerprint, iris, retina, face, hand geometry, palm, etc. The two issues to be considered for user authentication system are recognition of the authorized user and rejection of the impostor. So a better classifier is necessary to perform this task. Some of the widely used classifier is based on fuzzy logic, neural network, etc. Among those, neural network can be efficient in classification. This survey provides various biometrics based authentication system based on neural network.

Index terms— Neural network, authentication system, biometrics and key authentication.

1 Introduction

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 conventional approaches 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.

It's comparably much difficult to use conventional knowledge-based and token-based approaches, since these techniques are easily overcome by electronically interconnected information society. Thus, it's very vital to have accurate automatic personal identification in a variety of applications in this electronically interconnected society.

Biometric authentication systems have gained importance because of the key role of the information security and privacy. Biometric recognition is one of the most important techniques for the security privacy due to its distinctive nature of biometric traits such as fingerprints, iris, faces, palm, etc. Biometrics is the study of identification based on physical or behavioral characteristics and is widely adopted in providing better authentication.

Biometric characteristics play a key role in personal authentication applications because they possess the physiological properties like universality, uniqueness, permanence, collectablilty, performance, acceptability, and circumvention.

2 Figure 1: Biometric System

Figure **??** 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 provide their biometric feature to communicate with the server, which is transformed into a long secret detained by the server in its database [16].

Since there are various techniques on biometrics, still there are several researches in the field of biometrics. Several techniques have been incorporated with the biometric authentication system to improve the performance of the authentication system. Neural network is a technique which is very effectively used in the biometrics authentication systems. The two issues to be considered for user authentication system are recognition of authorized user and rejection of

3 Hardening of Biometric features User 1

User n

4 Server

5 Biometric dB

6 Mutual authentication & key

Author ? : Research Scholar, Anna University, Coimbatore, India Author ? : Associate Professor, Government Arts College, Salem, India : uthentication and security become much popular because of the arrival of new upcoming technologies like electronic banking, ecommerce, and smartcards and an increased emphasis on the privacy and security of information stored in various databases, automatic personal identification has become a very important field in the area of biometrics. Perfect automatic personal identification is very vital in a broad range of applications which involves the use of passports, cellular telephones, automatic teller machines, and driver licenses.

7 A

July imposters. These two issues can be incorporated into the biometric authentication system using the classifiers. There are several classifiers available in the literature such as fuzzy, neural networks etc.

This paper investigates on the biometrics authentication systems. Moreover, the biometric authentication system which uses the neural network techniques is also discussed.

8 II.

9 Literature Survey

Hao et al., [1] presented a technique for combining crypto with biometrics effectively. The author proposed a practical and secure way to incorporate the iris biometric into cryptographic applications. The author proposed a two-layer error correction approach that merges Hadamard and Reed-Solomon codes for deliberating on the error patterns within iris codes. The key was obtained from the iris image of the user through the supplementary error correction data that do not disclose the key and can be saved in a tamperresistant token like a smart card. The performance evaluation of the methodology was performed with the samples from 70 different eyes, 10 samples being obtained from every eye. It was observed that an errorfree key can be reproduced consistently from genuine iris codes with a success rate of 99.5 percent. It is likely to generate up to 140 bits of biometric key, more than adequate for 128-bit AES. Kwanghyuk Bae et al., [2] proposed an Iris feature extraction using Independent Component Analysis (ICA). A traditional approach based on Gabor wavelets selects the parameters (e.g., orientation, spatial location and frequency) for fixed bases. ICA is applied to generate optimal basis vectors for the difficulty of extracting effective feature vectors which represent iris signals. The base vectors learned by ICA are localized in both frequency and space like Gabor wavelets. The feature vectors are obtained from the coefficients of the ICA expansion. Then, each of the iris feature vector is encoded into an iris code. From the experimental observational, it is observed that the proposed approach has a similar Equal Error Rate (EER) to a conventional technique based on Gabor wavelets. The advantages of the proposed technique are

? The size of an iris code and the processing time of the feature extraction are signsificantly very less; ? The linear transform can be calculated for feature extraction from the iris signals themselves.

Dutta et al., [3] put forth a network security using biometric and cryptography. The author presented a biometrics based Encryption/Decryption method, 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. The unique Key obtained is send by the sender after watermarking it in sender's fingerprint along with Encrypted Message. This paper explains the computational requirement and network security features. The main advantage of the proposed approach is that it need not have to search from a database for a public key and security is highly maintained. Several fusion approaches have been widely used in integrating separate information from dissimilar modalities to provide complementary data. F. Alsaade et al., [4] proposed an enhancement of multimodal biometric verification using a combination of fusion methods. The main aim of this research is to enhance the accuracy of multimodal biometrics with the help of the suitable fusion method. The effectiveness of

the proposed method lies in raising the authentication accuracy. Such an approach which builds a multimodal biometrics system has not been investigated. The proposed fusion process has two stages. In the first stage, score fusion in Unimodal biometrics based on several matching approach is accomplished. This is attained by the classifiers like Support Vector Machines (SVM), Brute Search Force (BFS) and Logistic regression (LR) which has good learning mechanisms. In the second stage, the obtained fused scores for face and voice modalities are additionally integrated by SVM, LR or BFS. The experiment is performed using face and speech modalities. The experimental result clearly shows the advantages of using a combination of fusion methods at the Unimodal and multimodal levels.

Sanches-Reillo et al., [5] proposed a biometric identification through hand geometry measurements. The measured approaches are used after capturing and pre-processing the images of the hand. The main angles and distances of the hand are partitioned into four types: width, heights, deviations, and angles between the inter-finger points. Thirty-one features are extracted, and a discriminatory analysis is applied, then a feature vector consisting of 25 components is attained. The feature vectors are the inputs for a comparison process used to decide the individuality of the user whose hand has been photographed. Euclidean distance, Hamming distance, Gaussian Mixture Models (GMMs) and Radial Basis Function Neural Networks are used for the classification and verification. The proposed approach provides a success rate of about 96% by using GMM.

10 Global Journal of Computer

Beng et al., [6] put forth a secure biometric key generation with biometric helper. The proposed approach consists of a code redundancy construction and a randomized feature discretization process. The code redundancy construction allowed the reduction of the errors as well as even more; on the other hand the randomized feature discretization process controlled the intra-class variations of biometric data to the lowest level. The randomized biometric helper assures that a biometric-key was simple to be invalidated as soon as the key get conciliated. The proposed approach is evaluated using subset of the Facial Recognition Technology (FERET) database.

Ratha N. K. et al., [7] put forth enhancing security and privacy in biometrics-based authentication systems. The author proposed the evaluation techniques for biometrics based authentication systems (FRR). There has been a considerable surge in the use of biometrics for user authentication in recent years. Biometrics-based authentication tenders more improvement over other authentication methods. It is very vital that biometricsdependent authentication systems should be implemented to resist attacks when employed in security-critical applications, mainly in unattended distant applications such as e-commerce. In this paper the author sketch the natural potency of biometricsbased authentication, recognize the un-healthy links in systems utilizing biometrics-based authentication, and developed new method for discarding some of these weak links. This paper mainly deals with the fingerprint authentication but this analysis can be extended to other biometrics-based techniques.

Bolle R. M. et al., [8] proposed evaluation techniques for biometrics based authentication systems (FRR). Biometrics-based authentication is growing because of increasing ease-of-use and consistency. Performance evaluation of such systems is an important concern. The author conventionally neglected to address the two features of performance evaluation. First one is the "difficulty" of the information that is deployed in a study manipulates the evaluation results. The author proposed some new measures to differentiate the data set so that the performance of a given system on dissimilar data sets can be compared easily. Next, conventional studies regularly have stated that the false reject and false accept rates (FRR & FAR) in the form of match score distributions. But for these distributions no confidence intervals are computed. So there is no sign of significance for the given estimates. To measure the confidence intervals the author systematically studied and compared the parametric and nonparametric methods. This paper highly focuses on false reject rate estimates.

Zhang G. H. et al. [9] put forth a biometrics based security solution for encryption and authentication in tele-healthcare systems. In telehealthcare applications, security and privacy are becoming the most critical issues among all others in data transmission. This paper proposes a new method for wireless communication based on biometrics which incorporates the encryption and authentication techniques within a body sensor network (BSN). Also it has been formulated between a BSN and a remote server (RS) of a tele-healthcare system. This technique targets to utilize static and dynamic biometric qualities to create authentication and encryption keys respectively. 64 and 128 bits of key lengths were created from electrocardiogram and photoplethysmogram of 9 subjects and fingerprint images of 20 subjects. The entropy of the keys are ranging from 0.662 to 1 and the hamming distances between them is non-zero. The author concluded that using biometric approach, random and distinctive keys can be created for encrypting and authenticating data in tele-healthcare systems.

Zhenhua Wu [10] proposed biometrics authentication system on open network and security analysis. Authentication systems based on biometrics are rapidly increasing to direct physical access to highsecurity amenities. It is very need to address the vulnerability in an open network. This paper implements a biometrics-based network authentication system united with public key encryption technology to assure the authenticity of biometric data at transmission. The possible weaknesses of a biometrics-based network authentication system are analyzed. For a network based system which follows the authentication protocol, the proposed model can deliberately provides highly secured authentication service.

11 YaghoubI Z. et al. [11] put forth multimodal

biometric recognition inspired by visual cortex and support vector machine classifier. A personal identification method with a high confidence coefficient which is based on biometrics is considered to be an efficient method for automatic identification. A multimodal biometric model is formulated by integrating the evidence obtained from numerous biometric resources which uniquely gives improved recognition performance when compared to single biometric modality systems. Hence in this paper, for individual authentication features of ear and face are used. The attributes that are extracted from HMAX model are transformation and scale-invariant. Then to differentiate the classes, support vector machine (SVM) and Knearest neighbor (KNN) classifiers are used. The matching-score levels are used at fusion phase. Experimental result demonstrates that the accuracy rate of ORL face database is 96% and USTB ear database showed 94% accuracy rate. But 98% accuracy rate can be obtained on face and ear multimodal biometric.

Harun N. et al., **??**12] proposed performance of keystroke biometrics authentication system using Multilayer Perceptron neural network (MLP NN). The utilization of computer has been increased faster also the usage of web applications like e-commerce, online banking services, webmail, and blogs are increased. A password system is necessary in all sorts of internet applications. Hence we are in need of a password authentication system to enable only the authentic July individual can login to the application. Conventionally passwords and personal identification numbers (PIN) have been exercised to login such applications. Even though, without detection it is simple for illegal persons to utilize these systems. This paper uses the keystroke biometrics as a transparent level of user authentication. The paper mainly concentrates on using the time interval between keystrokes as a characteristic of individuals' typing speed to recognize the authentic users and refuse pretenders. To train and authorize the characteristic, Multilayer Perceptron (MLP) neural network with a Back Propagation (BP) learning algorithm is used.

Hong Ye, et al. [13] put forth biometric system by foot pressure change based on neural network. A new method has been imposed to extract the features of center of foot pressure (COP) acquired by a load distribution sensor and implement this method to build a biometrics personal identification technique. In this method, a user is supposed to stand with slipper on load distribution sensor, and obtain pressure data during a simple motion, as touching a bell nearer by one hand but without movements of feet. A biometrics individual identification model has been proposed with fewer information, time and little space. From the obtained pressure data the site of COP can be computed. The characteristics for identification are removed from the position and the movement of COP. Then k-out-of-n system is developed and a neural network (NN) system with the feature constraint and enter trial data to the two systems. At last these two techniques were compared. From the experimental result, it is observed that the proposed approach achieves an accuracy of 12.0% in FRR (False Rejection Rate) and 1.0% in FAR (False Acceptance Rate). Urias et al., [14] proposed a new method for response integration in modular neural networks using type-2 fuzzy logic. Biometric authentication is used to achieve person recognition. Biometric characteristics like face, fingerprint, and voice are used. A modular neural network of three modules is used. Each module is a local expert on person recognition based on each of the biometric features. The response integration approach of the modular neural network has the objective of integrating the responses of the modules to enhance the recognition rate of the individual modules. The results of a type-2 fuzzy logic approach for response integration has shown higher performance over type-1 fuzzy logic approaches. D. R. Shashikumar et al., [15] proposed a biometric security system based on signature verification using neural networks. The signature verification is the behavioral parameter of biometrics and is used to authenticate a person. A characteristic signature verification approach usually contains four components namely data acquisition, preprocessing, feature extraction and verification. The global and grid features are incorporated to produce new set of features for the verification of signature. Neural Network is used as a classifier for the authentication of a signature. The performance is evaluated based on the verification on random, unskilled and skilled signature counterfeits along with authenticated signatures. FAR and FRR results for the proposed approach is very significant when compared to the existing algorithms. [1] An error-free key can be reproduced consistently from genuine iris codes with a success rate of 99.5 percent.

[2]

The size of an iris code and the processing time of the feature extraction are significantly very less.

[3]

This approach need not have to search from a database for a public key and security is highly maintained.

[4]

To enhance the accuracy of multimodal biometrics with the help of the suitable fusion method.

[5]

The proposed approach provides a success rate of about 96% by using GMM.

[9]

The author concluded that using biometric approach, random and distinctive keys can be created for encrypting and authenticating data in tele-healthcare systems.

[10]

This paper implements a biometrics-based network authentication system united with public key encryption technology to assure the authenticity of biometric data at transmission.

[11] Accuracy rate of ORL face database is 96% and USTB Ear database showed 94% accuracy rate.

[12]

Concentrates on using the time interval between keystrokes as a characteristic of individuals' typing speed to recognize the authentic users and refuse pretenders.

[13]

The proposed approach achieves an accuracy of 12.0% in FRR (False Rejection Rate) and 1.0% in FAR (False Acceptance Rate).

[14]

The response integration approach of the modular neural network has the objective of integrating the responses of the modules to enhance the recognition rate of the individual modules.

[15]

The global and grid features are incorporated to produce new set of features for the verification of signature. FAR and FRR results for the proposed approach is very significant when compared to the existing algorithms.

The advantages of the existing systems are provided in table **??**. By analyzing the advantages of the existing system, the system to be proposed should resulted in all the advantages provided by various III.

12 Future Work

By analyzing the existing biometrics based security system, it can be clearly said that the usage of neural network along with biometrics features will provide better security than other techniques. In future, biometrics secure system can be developed by combining two or more biometrics features like fingerprint, iris, retina, palm, tooth, face, etc., this will provide better security because it is almost impossible to crack more than one biometrics features. Also, the neural network used in security system can also be altered to improve the accuracy for classification. For this purpose more efficient and suitable neural network can be used.

13 IV.

14 Conclusion

Biometric systems are generally used to control access to physical assets (laboratories, buildings, cash from ATMs, etc.) or logical information (secure electronic documents, personal computer accounts etc). The human biometrics like fingerprint, hand geometry, face, retina, iris, DNA, signature and voice can be effectively 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 successful biometric authentication. The two issues to be considered for user authentication system are recognition of the authorized user and rejection of the impostor. So a better classifier is necessary to perform this task. Some of the widely used classifier is based on fuzzy logic, neural network, etc. Among those, neural network can be efficient in classification. This paper provides various available biometric techniques with some discussion. This survey will help the researchers to develop better biometric techniques. By analyzing the advantages of the existing system, it is suggested to use the neural network classifier combined with the biometric technique to achieve a better security system with maximum advantage. [1] [2]

[1] © 2011 Global Journals Inc. (US)

[2] © 2011 Global Journals Inc. (US) July


Global Journals Inc.
Global Journal of Computer Science & Technology

Figure 1:

[Zhang et al. ()] 'A biometrics based security solution for encryption and authentication in tele-healthcare systems'. G H Zhang , C C Y Poon , Y T Zhang . *ISABEL 2009, 2nd International Symposium on Applied Sciences in Biomedical and Communication Technologies*, 2009. p. .

[Urias et al. ()] 'A New Method for Response Integration in Modular Neural Networks using Type-2 Fuzzy Logic for Biometric Systems'. J Urias , D Hidalgo , P Melin , O Castillo . *IJCNN 2007, International Joint Conference on Neural Networks*, 2007. p. .

[Sanchez-Reillo et al. (2000)] 'Biometric Identification Through Hand Geometry Measurements'. R Sanchez-Reillo , C Sanchez-Avila , A Gonzalez-Marcos . *IEEE Trans. on PAMI* October 2000. 22 (10) p. .

[Shashikumar et al. ()] 'Biometric security system based on signature verification using neural networks'. D R Shashikumar , K B Raja , R K Chhotaray , Sabyasachi Pattanaik . *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, 2010. p. .

[Hong Ye et al. ()] 'Biometric System by Foot Pressure Change Based on Neural Network'. , S Hong Ye , Y Kobashi , K Hata , K Taniguchi , Asari . *39th International Symposium on Multiple-Valued Logic*, 2009. p. . (ISMVL '0)

[Hao et al. ()] 'Combining crypto with biometrics effectively'. F Hao , R Anderson , J Daugman . *IEEE Transactions on Computers* 2006. 55 p. .

[Dutta et al. ()] Sandip Dutta , Avijit Kar , N C Mahanti , B N Chatterji . *Proceedings of the 10th International Conference on Advanced Concepts for Intelligent Vision Systems*, (the 10th International Conference on Advanced Concepts for Intelligent Vision Systems) 2008. p. .

[Alsaade and Zahrani ()] 'Enhancement of Multimodal Biometric Verification Using a Combination of Fusion Methods'. F Alsaade , M Zahrani . *SETIT 2009 5th International Conference: Sciences of Electronic, Technologies of In formation and Telecommunications*, March 22-26, 2009.

[Ratha et al. ()] 'Enhancing security and privacy in biometricsbased authentication systems'. N K Ratha , J H Connell , R M Bolle . *IBM Systems Journal* 2001. 40 (3) p. .

[Bolle et al. ()] 'Evaluation techniques for biometrics based authentication systems (FRR)'. R M Bolle , S Pankanti , N K Ratha . *Proceedings 15th International Conference on Pattern Recognition*, (15th International Conference on Pattern Recognition) 2000. 2 p. .

[Rajeswari Mukesh et al. ()] 'Finger Print Based Authentication and Key Exchange System Secure Against Dictionary Attack'. A Rajeswari Mukesh , V Damodaram , Subbiah , Bharathi . *IJCSNS International Journal of Computer Science and Network Security* 2008. 8 (10) p. .

[Global Journal of Computer Science and Technology Volume XI Issue XI Version I ()] *Global Journal of Computer Science and Technology Volume XI Issue XI Version I*, 2011.

[Bae et al. (2003)] 'Iris feature extraction using independent component analysis'. K Bae , S Noh , J Kim . *Proceedings of the 4th International Conference on Audio-and Video-Based Biometric Person Authentication (AVBPA '03)*, (the 4th International Conference on Audio-and Video-Based Biometric Person Authentication (AVBPA '03)Guildford, UK) June 2003. 2688 p. .

[Beng et al. (2008)] 'Secure biometrickey generation with biometric helper'. Jin A Beng , Kar-Ann Teoh , Toh . *proceedings of 3rd IEEE Conference on Industrial Electronics and Applications*, (3rd IEEE Conference on Industrial Electronics and ApplicationsSingapore) June 2008. p. .

[Wu ()] Zhenhua Wu . *International Symposium on Electronic Commerce and Security*, 2008. p. .