International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

A NOVEL MULTIMODAL BIOMETRICS BASED AUTHENTICATION AND KEY EXCHANGE SYSTEM

Dr.K. Saraswathi, Assistant Professor, PG and Research Department of Computer Science, Govt. Arts College, Coimbatore.

Dr. N. Vimala, Assistant Professor, PG Department of Computer Science, LRG Govt. Arts College for Women, Tirupur.

Abstract

Security to the communications channels are latest threads to the communication society. Cryptography is the foremost technique for security and the new developments are needed in this area to get a strong security application. Biometrics is an emerging security technique which is mainly concentrate on the authentication security issues with the new multimodal technology. Biometrics based security features are already developed but for iris and retina based security is to be focused and exchanging of the key is a risky task for any one. Therefore this paper focused on the new technology multimodal biometrics for authentication and as well as for the key secured key exchange system.

Keywords- cryptography, biometrics, authentication security, key exchange, security.

I. Introduction

Today, most companies' host computers can be accessed by their employees whether in their office over a private communications network or from their homes or hotel rooms, while on the road through normal telephone lines. Network security [7] involves all activities that organizations, enterprises and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

Cryptography

Cryptography is an ancient technique for providing security. For several years, Cryptography was exclusively reserved for military and diplomatic applications. Shannon [8] presented “The communication theory of secrecy systems” which described a mathematical basis for cryptographic systems, beginning with the definition of a new model: Information Theory.

Encryption Algorithms

An encryption algorithm converts a plaintext (message) into a ciphertext which will be readable by its authorized receiver. This transformation is done through an encryption function which is parameterized by an encryption key. A confidential (authenticated) user can then decrypt the ciphertext through the deciphering function, provided that the user knows the equivalent deciphering key. This system is secure as far as it is not possible for an intruder to figure out the plaintext from the ciphertext and a fortiorito recover the deciphering key.

The two main types of encryption algorithms are implemented based on their keys which might be secret or public. Secret key systems necessitate the sharing of a secret among the authenticated users. The public-key systems eliminated these constraints. But, as public-key encryption algorithms are slow and do not facilitate online encryption, these algorithms are not very significant. In most of the present applications, the best result is a hybrid system which integrates both types of algorithm.

The encryption and decryption of the cryptosystem procedure can be described in figure 1.1.

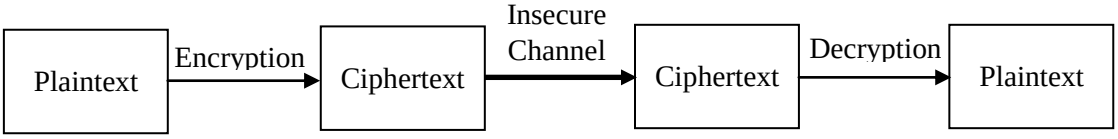

Figure 1: Work Flow of a Cryptosystem

Biometrics

Today, biometrics is a computerized method of recognizing an individual based on physiological (e.g., fingerprints, face, retina, iris) or behavioral characteristics (e.g., gait, signature). Each biometric feature has its own strength and weakness and the choice typically depends on the application. No single biometric feature is achieved to have been effective to meet the requirements of all applications. Since biometric characteristics are distinctive, they cannot be forgotten or lost and the person to be authenticated needs to be physically present at the point of identification. Biometrics is inherently more reliable and more capable than traditional knowledge-based and token-based techniques [16].The security and authentication of the users in the Wireless Local Area Networks (WLANs) is also a serious issue. Hence the security of 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. The main objective of this paper is to propose a novel technique for the network security by means of biometrics, developing a novel technique for personal authentication using biometrics and deniable authentication protocol and providing security to the users of the network by exploiting various biometric features like fingerprint, iris and retina.

The rest of this paper is organized as follows: Section II reviewofLiterature survey on biometric multimodal merits and demerits. Section III discusses on proposed methodology. Section IV Results and Discussions tell about the achieved results and discussed the overcome demerits of the existing system. Section V concludes with conclusion and future developments.

II. Literature Survey

Chen and Chandran [1] have presented an approach that generates deterministic bit-sequences from the output of a repetitive one-way transform through entropy based feature extraction procedure coupled with Reed-Solomon error correcting codes. The approach was evaluated through a 3D face data and was thus proved to be reliable in key generations of suitable length for 128- bit AES.

Uludag et al., [2] have defined a biometric approach as an automated technique for the recognition of a person based on behavioral or physiological features. The characteristic features widely used are hand geometry, handwriting, face, fingerprints, vein, voice, retina and iris. The authors explained that biometric techniques are now the key to a wide array of greatly secured identification and personal verification solutions.

The important differences between the physiological and the behavioral biometrics. The physiological biometrics comprise of measurements and data obtained together from the direct measurement of a part of the human body. These samples include hand geometry, iris-scan, facial recognition, fingerprint, etc..AlternativelyJain and Uludag [3] says, the behavioral characteristics begin from the functionalities of an individual and it indirectly computes unique features of the human body. These samples comprise of voice recognition, signature-scan, keystroke-scan, etc.. Time can act as a metric for behavioral biometrics, as it evaluates behavior by taking into account the timeline of a given process.

A technique which focuses on the security of fingerprint scanners. To carry out this technique, an example device is chosen and some efforts are made to break its protection. The authors have examined certain vulnerability and then three various ways to use these safety risks. The scope of the experiments is restricted to fingerprints, leaving hard and software attacks aside. UltimatelyAnttiSten et al., [4] says there are certain notes about protecting against these attacks. Sometimes, simple tools are utilized to fool a scanner. With higher level equipments, the percentage is most likely higher and the outcome shows that fingerprint scanner is secure enough to protect valuable assets.

The prototype of a verification system depending on hand geometry. The features comprised in this system are the length, width of the fingers and the thickness of the hand. In the verification phase a 16-dimensional feature vector is connected with the claimed identity and this is then compared with the feature vector of the hand whose identity has to be verified said by Jain et al., [5].a

Jane You et al., [6] have described a texture-based, dynamic selection approach to allow a fast search for the best matching of a palmprint template in the database in a hierarchical fashion.

III. Proposed Methodology

The proposed methodology uses biometric features such as fingerprint, iris and retina. The methodology aims at developing an efficient biometric authentication system for network security. The methodology used in the proposed approach is a Novel Multimodal Biometrics based Authentication and Key Exchange System.

Table. 1 Comparison of Various Biometrics Based Key Generation and Key Release Algorithms

Biometric Identifier	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	L
Voice	M	L	L	M	L	H	H
Signature	L	L	L	H	L	H	H

In Table.1, High, Medium and Low are represented by H, M and L respectively. The Biocryptosystem utilizes the merits of biometrics and the cryptographic framework [9]. This approach enhances user authenticity. Therefore, experiments are conducted in this area to determine the efficiency of the algorithms implemented to measure the accuracy and privacy of the user information. Moreover, biocryptosystem analyzes various properties and attributes of biometric identifier in determining the efficiency of the proposed algorithms.

Need For Multimodal Biometrics

Most of the biometric authentication systems employed in real-world applications are unimodal, which means that only a single source of information is used for authentication (e.g., single fingerprint or face). These unimodal biometric systems possess various limitations which may greatly affect the overall security of the user. Some of the limitations of the unimodal biometric systems are:

- Noisy data: A unimodal biometric feature such as a fingerprint image with a scar or a voice sample altered by cold is an example of noisy data. Noisy data could also be due to defective or improperly maintained sensors (e.g., presence of dirt on a fingerprint sensor) or adverse ambient conditions (e.g., poor illumination of a user's face in a face recognition system [10]).
- Intra-class variations: These variations are obviously caused by the user who is imperfectly interacting with the sensor (e.g., incorrect facial pose), or when the characteristic features of a sensor are altered during authentication (e.g., optical versus solid-state fingerprint sensors).
- Inter-class similarities: In a biometric system consisting of a vast number of users, there may be inter-class similarities (overlap) in the feature space of multiple users.
- Non-universality: The unimodal biometric systems mostly do not obtain meaningful biometric data from a subset of users. For instance, a fingerprint biometric system, may obtain incorrect minutiae features from the fingerprints of certain individuals, because of the poor quality of ridges.
- Spoof attacks: This type of attack is mostly relevant when behavioral characteristic features such as signature or voice are used. But, physical traits such as fingerprints are also vulnerable to spoof attacks [11].

The above mentioned limitations of unimodal biometric systems can be overcome by incorporating two or more sources of information for establishing identity [12]. Such systems are commonly called "multimodal biometric systems" and are expected to be more reliable because of the presence of multiple (comparatively) independent pieces of evidence [13]. These multimodal biometric systems are capable of meeting the strict performance necessities imposed by various

applications. They overcome the problem of non-universality, since multiple characteristic features guarantee adequate population coverage. They also prevent spoofing as it would be very tough for an attacker to spoof multiple biometric characteristic features of a genuine user simultaneously.

Proposed Multimodal Biometric Systems

In recent times, multimodal biometrics fusion methods have attracted much awareness as the additional information among various modalities could enhance the recognition accuracy. Several techniques have been proposed in this field. In common, they can be separated into three types:

- Fusion at the Feature Level
- Fusion at the Match Level
- Fusion at the Decision Level

In this proposed approach, the fusion at the feature level technique is used. The fusion at the feature level performs the mixing of feature sets equivalent to multiple modalities. As the feature set consists of richer data about the raw biometric data than the match score or the final decision, the integration at this level is estimated to afford better recognition results. On the other hand, the fusion at this level is very hard to achieve in practice because of the following reasons:

- The feature sets of multiple modalities may be incompatible (e.g., minutiae set of fingerprints and eigen-coefficients of face).
- The relationship between the feature spaces of different biometric systems may not be known.
- Concatenating two feature vectors may result in a feature vector with a very large dimensionality leading to the `curse of dimensionality' problem.

Biometric cryptosystems is a new method that merges biometrics and cryptography [17] and it is universally called “crypto-biometric systems”. The combination of biometrics and cryptography is generally performed in two distinct phases.

Thus, it is impossible for the hacker or the unauthenticated user to access the secure system. This paper uses biometrics features such as fingerprint, iris and retina to generate thecryptography key [14, 15].

Multimodal biometric fusion is used in this approach for providing better network security. The features obtained from the biometric features are combined using fusion techniques. From these fused features, a key is generated by the authentication protocol, which is more secure than any other technique.

IV. Results and Discussions

An evaluation study of the proposed biometric key exchange techniques is presented in this paper. The results of an extensive set of simulation tests are shown, in which the biometric approaches are compared under a wide variety of different scenarios. MATLAB is used for the computation of the numerical analysis.

The performances of the proposed approaches are evaluated based on various parametric standards like False Rejection Rate(FRR), False Acceptance Rate (FAR).

Table 2. Fingerprint-Iris 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’	50	105	57	357	107	78
II ‘security’	144	27	49	373	193	16

III 'security'	81	150	57	210	10	255
IV 'security'	147	247	116	121	205	240

The Table 2 gives represent the multimodal key authentication systems using the biometric feature level fusion combinations such as Fingerprint-Iris. The same passwords which are used in the unimodal retinal biometric key authentication system are taken for this multimodal Fingerprint-Iris key authentication system. Moreover, the same experimental procedure is taken up for this multimodal key authentication system.

Table 3 represents the fingerprint-iris-retina multimodal key authentication system. The feature points of fingerprint, iris and retina before and after transformation is obtained and tabulated. For password 'security', the feature points are obtained for four quadrants. Based on the transformation code from password represented by $T_u$and T_v, the transformed feature points are tabulated.

Table. 3 Fingerprint-Iris-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'	63	51	57	357	33	24
II 'security'	149	52	49	373	157	41
III 'security'	102	186	57	210	31	163
IV 'security'	145	248	116	121	203	241

The ultimate measure of the utility of a biometric system for a particular application is recognition rate. This can be described by two values are FAR and FRR.

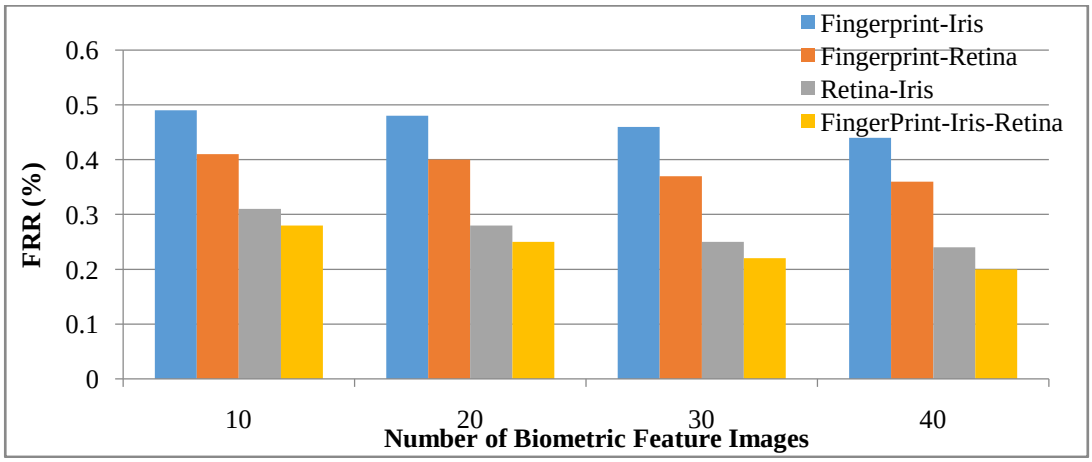

Figure 2: False Rejection Rate (FRR) (%) Comparison

It is clearly observed from the figure 2 that the proposed Fingerprint-Iris-Retina multimodal biometric authentication key exchange system provides better FRR when compared with other multimodal biometric features such as Fingerprint-Iris, Fingerprint-Retina and Retina-Iris. For the samples 31-40, the FRR obtained for the multimodal systems such as Fingerprint-Iris-Retina, Fingerprint-Iris, Fingerprint-Retina, and Retina-Iris are 0.20% 0.44%, 0.36%, and 0.24% respectively. Similarly for other samples, the proposed Fingerprint-Iris-Retina provides less FRR when compared with the other multimodal systems. Compared to existing method the proposed multimodal method of Fingerprint-Iris-Retina provides high accuracy of 95%.

V. CONCLUSION

This research work mainly concentrates on multimodal biometric for network security. Biometric systems are commonly used to control access to physical assets (laboratories, buildings, cash from ATMs, etc..) and logical information (personal computer accounts, secure electronic documents, etc.). The human biometrics such as hand geometry, face, fingerprint, retina, iris, DNA, signature and voice can effectively be used to ensure network security. In biometric cryptosystems, a cryptographic key is generated 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 ideas in the areas of image processing techniques are reused to extract the minutiae from the biometric image. The preprocessing techniques mentioned in this research play an important role in improving the performance of the biometric based network security system. The obtained performance measures revealed that the method could effectively provide network security. Therefore, it can directly be applied to fortify the existing standard single-server biometric based security applications. The future enhancements that can be incorporated into any research in future to improve the security and performance of the system Other biometric features like nose, ear, face, tooth, palmprint, profile line, etc., can be used in future for this research, which may increase the overall performance of the bio-cryptosystem and effective multimodal fusion techniques can be used for improved results in the biometric fusion.

References

1. Chen, B., & Chandran, V. (2007, December). Biometric based cryptographic key generation from faces. In Digital Image Computing Techniques and Applications, 9th Biennial Conference of the Australian Pattern Recognition Society on (pp. 394-401). IEEE.
2. Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. K. (2004). Biometric cryptosystems: issues and challenges. Proceedings of the IEEE, 92(6), 948-960.
3. Jain, A. K., &Uludag, U. (2003). Hiding biometric data. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 25(11), 1494-1498.
4. Stén, A., Kaseva, A., & Virtanen, T. (2003). Fooling fingerprint scanners-biometric vulnerabilities of the precise biometrics 100 SC scanner. InProceedings of 4th Australian Information Warfare and IT Security Conference (Vol. 2003, pp. 333-340).
5. Jain, A. K., Duin, R. P., & Mao, J. (2000). Statistical pattern recognition: A review. Pattern Analysis and Machine Intelligence, IEEE Transactions on,22(1), 4-37.
6. You, J., & Bhattacharya, P. (2000). A wavelet-based coarse-to-fine image matching scheme in a parallel virtual machine environment. Image Processing, IEEE Transactions on, 9(9), 1547-1559.
7. Kaufman, C., Perlman, R., &Speciner, M. (2002). Network security: private communication in a public world. Prentice Hall Press.
8. Shannon, P., Markiel, A., Ozier, O., Baliga, N. S., Wang, J. T., Ramage, D., ...&Ideker, T. (2003). Cytoscape: a software environment for integrated models of biomolecular interaction networks. Genome research, 13(11), 2498-2504.
9. Bangerter, E., Camenisch, J., &Lysyanskaya, A. (2004, April). A cryptographic framework for the controlled release of certified data. InSecurity Protocols (pp. 20-42). Springer Berlin Heidelberg.
10. Jain, A. K., & Ross, A. (2004). Multibiometric systems. Communications of the ACM, 47(1), 34-40.
11. Katiyar, R., Pathak, V. K., & Arya, K. V. (2013). A study on existing gait biometrics approaches and challenges. International Journal of Computer Science, 10(1), 135-144.
12. Ross, A., & Jain, A. K. (2004, September). Multimodal biometrics: An overview. In Signal Processing Conference, 2004 12th European (pp. 1221-1224). IEEE.
13. Stull, W. J. (1975). Community environment, zoning, and the market value of single-family homes. JL & Econ., 18, 535.

14. Al-Riyami, S. S., & Paterson, K. G. (2003). Certificateless public key cryptography. In Advances in cryptology-ASIACRYPT 2003 (pp. 452-473). Springer Berlin Heidelberg.
15. Seredynski, F., Bouvry, P., &Zomaya, A. Y. (2004). Cellular automata computations and secret key cryptography. parallel computing, 30(5), 753-766.
16. Gabrielli A,Proposal of Readout Technique for Low-Pitch Pixel Detectors, IEEE Nuclear Science Symposium Conference Record(NSS'07), Vol. 1, Pp. 824-826,2007.
17. Hao F, Anderson R and Daugman j, Combining crypto with biometrics effectively, IEEE Transactions on Computers, Vol. 55, Pp. 1081-1088,2006.