International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

A Review on Security System Using Biometric Parameter

Mr. Pund Kishor Jagannath

[1]*M.E student, VLSI AND EMBEDDED SYSTEM,*

Siddhant College of Engineering, Sudumbare, Pune - 412109,

Maharashtra state, India

Prof. V.S. Bhatlavande

[2]*Assistant Professor, Department of Electronics and telecommunication Engineering,*

Siddhant College of Engineering, Sudumbare, Pune - 412109,

Maharashtra state, India

Abstract - *In today's world use of Security system is increasing due to its numerous advantages, easiness etc. Security system is that which provides protection to any vulnerable and valuable asset, such as a person, dwelling, community, item, nation, or organization. There are various technologies exist which are used for Security purpose. One of them is creation of security system using biometrics modalities. By using different Biometrics parameter we can create security system, which will be useful for the person's identification and authentication and also for access control. This security system can be used anywhere as per the requirement of the user. For keeping the things confidential people needs security system, that security system should not be known or recognizable to anyone. As the Biometric parameters i.e. human characteristics and traits can allow people identification and authentication, it is used for security purpose globally. Researchers are working on the different biometric parameters which can be used for the creation of the security system. In this paper we are going to discuss how the security system is getting more secure as the previous one. There are different biometric parameters which are used for the creation of security system. These parameters has uniqueness that's why they are used for the security purpose, because there spoofing is more difficult for the unknown person. As security goes on increasing it also increased the complexity, but created more secured system.*

***Key Words*: Biometric, confidential, authentication, spoofing, uniqueness**.

1. INTRODUCTION

In recent years, the increasing interest in security system has led to the creation of numerous and very diverse initiatives focused on a various biometric parameters such as physical (Fingerprint, Face, Iris, Ear, Retina, Hands) and behavioral (Walking, signature, typing patterns) etc. Now days, whole word is facing a problem of insecurity in case of things, in case of documentation, in case of jewelry, in case of Banking etc. There are number of things which are insecure because of increased in the hacking and thieves. As the technology is getting advance new techniques are proposed for the security. The study of automated identification and verification of person with the help of human's physical or behavioral characteristics and traits is called as biometric. Biometrics parameter has advantage that it has no risk of forgetting, losing it, getting it stolen, getting is copy, being used by anyone else. And it has properties like Universal, Uniqueness, Permanence and Collectability. Now again question arises that why to go for biometric? Answer is that it is more secure because of its simplicity and easiness. In this only the intended person has the access control for the authentication. For this various methods or parameters are used for it such as face, iris, fingerprint, ECG or key, password, magnetic card or smartcard.

2. BIOMETRICS

Biometrics is related to the human characteristics and traits. Biometrics authentication is mostly used in computer science for identification and access control for security purpose. It is also used to identify individuals in groups that

are under security. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric characteristics are often classified as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the human body. Examples include, but are not limited to fingerprint, ECG, face recognition, ear recognition, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a human being, including but not limited to typing rhythm, walking style, and speech. Since biometric parameters are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric parameters raises privacy concerns about the ultimate use of this information.

Many different aspects of human physical, chemistry or behavior can be used for biometric authentication. Convenient biometric use dependent on the application. Certain biometrics parameter will be better than others based on the required levels of convenience and security. No single biometric will meet all the requirements of every possible application.

2.1 Features of Biometrics security System

1) Unique, Uniqueness which means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.

2) Highly measurable, Measurability (collectability) relates to the ease of accretion or measurement of the trait. In addition, obtained data should be in a form that permits subsequent processing and extraction of the relevant feature sets.

3) Performance is good, which relates to the accuracy, speed, and robustness of technology used.

4) Highly universal, Universality means that every person using a system should possess the characteristics.

5) Highly acceptable, Acceptability relates to how well individuals in the pertinent population accept the technology such that they are willing to have their biometric attribute captured and assessed.

2.2 Challenges of Biometrics security systems

Biometrics security systems face some main challenges, these are high initial cost, time consuming, knowledgeable person required for its use, somewhat complex. The main intention of this research is to design and implement a security system using Biometrics parameter which can give access control for the recognition and authentication of a person to the system. The security system requires number of sensors depending on the level of security that is to be required by user.

3. LITERATURE REVIEW

In this section, we are discussing various Security System using biometric parameters, with their technology with features, benefit and limitations they have.

3.1 Security of Multimodal Biometric Systems against Spoof Attacks

In this paper author discussed the various attacks done on the biometric security system, Spoof attacks are one of the main threats against the security of biometric systems for identity recognition. Multimodal biometrics systems are more robust to spoof attacks than the single biometric system. Author discussed various methods, through which spoofing of biometric parameter is done such as perfect replica of biometric parameter. He designed a security system against spoofing attacks to make more robust security system.

3.2 A Novel Approach to Improve Biometric Recognition Using Rank Level Fusion

This paper introduces a novel approach for rank level fusion which gives quality performance gain verified by experimental results. In the absence of ranked trait and instead of using the entire template, we propose using K partitions of the template. The way proposed in the paper is useful for generating sequential ranks and survivor lists on separation of template to lift confidence levels by incorporating information from partitions. The proposed algorithm constantly generates ranks for each separation of the user template. Ranks from template partitions are consolidated to evaluate the fusion rank for the classification. This paper scrutinizes rank level fusion for palm print biometric using two ways: (1) fixed threshold and resulting residual list, and (2) iterative thresholds and iteratively refined survivor list. The above approaches achieve identical performances as related manifestations of fusion architecture. The experimental results support the proposition of high in-template complementary of palm print for a user and its relevance to the intra-modal fusion framework. Experimental results using recommended approach on real palm print data from 100 users show superior performance with recognition accuracy of 99 % as

compared to recognition accuracy of 95% achieved with the conventional approach.

3.3 Biometric Recognition Using 3D Ear Shape

In this paper Ping Yan and Kevin W. Bowyer presented a complete system for ear biometrics, including automated distribution of the ear in a profile view image and 3D shape matching for recognition. We evaluated this system with the biggest experimental study to date in ear biometrics, achieving a rank-one recognition rate of 97.8 percent for an identification scene and an equal error rate of 1.2 percent for a verification scenario on a database of 415 subjects and 1,386 total probes.

3.4 Biometric recognition in telecom environment

Latest telecom environment provides a rich set of services that require secure and reliable authentication. Biometric recognition is the only authentication technique that depends on person's characteristics for personal authentication. This paper gives an analysis of a biometric system and biometric recognition techniques that use characteristics that are most relevant for application in telecom environment. Further, it analyses potential use case scenarios where those techniques could be applied.

3.5 ECG Biometric Recognition: A Comparative Analysis

In this paper, we analyzed most of the techniques that have been applied to the use of the electrocardiogram for biometric recognition. In particular, we classified the methodologies based on the features and the classification schemes. Finally, a correlative analysis of the authentication performance of a few of the ECG biometric systems is presented, using our in house database. The comparative study includes the cases where training and testing data come from the same and distinct sessions (days). The authentication results show that most of the algorithms that have been proposed for ECG-based biometrics executed well when the training and testing data come from the same session. However, when training and testing data come from distinct sessions, performance degradation occurs. Multiple training sessions were incorporated to decline the loss in performance. That notwithstanding, only a few of the proposed ECG recognition algorithms emerges to be able to support performance improvement due to multiple training sessions. Only three of these algorithms produced equal error rates (EERs) in the single digits, including an EER of 5.5% using a method proposed by us.

3.6 Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition

In this paper, we present a innovative software-based fake detection method that can be used in multiple biometric systems to detect distinct types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding aliveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image aspect or quality assessment. The proposed approach presents a very low degree of complexity, which makes it convenient for real-time applications, using 25 general image quality features extracted from one image (i.e., the same collected for authentication purposes) to distinguish between legitimate and impostor samples. The experimental results, obtained on openly available data sets of fingerprint, iris, and 2D face, show that the proposed method is highly aggressive compared with other state-of-the-art approaches and that the analysis of the general image quality of real biometric samples admits highly valuable information that may be very efficiently used to discriminate them from fake traits.

COMPARATIVE ANALYSIS

By overlooking above surveyed papers, all the security system uses biometric parameters. Biometrics modality plays a very essential role in all these security systems.

CONCLUSION

We have studied different techniques for security system using biometric modalities. Various authors give various techniques with algorithm, block diagram and their explanation with proper layout of successful execution with adequate strengths and imperfection. All systems are planned in this surveyed papers are designed and tested practically. Main purpose of this method of implementation is that all systems are in uncertain condition.

REFERENCES

[1] https://en.wikipedia.org/wiki/Security.

[2]https://en.wikipedia.org/wiki/Biometrics.

[3] Javier Galbally, Sébastien Marcel, *Member, IEEE*, and Julian Fierrez "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 23, NO. 2, FEBRUARY 2014

[4] Jay Bhatnagar, Ajay Kumar, Nipun Saggar "A Novel Approach to Improve Biometric Recognition Using Rank Level Fusion" Biometrics Research Laboratory Department of Electrical Engineering, Indian Institute of Technology Delhi, Hauz Khas, New Delhi 110 016, INDIA, IEEE 2007

[5] Ping Yan and Kevin W. Bowyer, "Biometric Recognition Using 3D Ear Shape" IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 29, NO. 8, AUGUST 2007

[6] A. K. Jain and A. Ross, "Introduction to biometrics," in *Handbook of Biometrics*. New York, NY, USA: Springer-Verlag, 2008, pp. 1–22.

[7] Ikenna Odinaka, *Student Member, IEEE*, Po-Hsiang Lai, *Student Member, IEEE*, AlanD.Kaplan, *Member, IEEE*, Joseph A. O'Sullivan, *Fellow, IEEE*, Erik J. Sirevaag, and John W. Rohrbaugh "ECG Biometric Recognition: A Comparative Analysis" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 6, DECEMBER 2012

[8] *ISO/IEC 19792:2009, Information Technology—Security Techniques- Security Evaluation of Biometrics*, ISO/IEC Standard 19792, 2009.

[9] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, "Image manipulation detection," *J. Electron. Imag.*, vol. 15, no. 4, pp. 041102-1–041102-17, 2006.

[10] K. A. Nixon, V. Aimale, and R. K. Rowe, "Spoof detection schemes," *Handbook of Biometrics*. New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.

[11]Ivan Krevatin, "Biometric recognition in telecom environment" 978-1-4244-7445-5/10/$26.00 ©2010 IEEE Journal.

[12] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in *Proc. IEEE IJCB*, Oct. 2011, pp. 1–7.