International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 6, November- December 2017 ISSN 2278-6856

AN OVER LOOK– VARIOUS APPROACHES FOR RECOGNITION

Dr.A.P.Caroline Hirudhaya Ph.D.,

Associate Professor, Department of Information Technology, KG College of Arts and Science, Coimbatore.

Abstract

In this paper, we analyze enhancing the Security and Privacy of multimodal biometric system. Comparing with the traditional authentication technology(password, ID, keys, etc), biometric recognition technology make users not to remember password and take keys and therefore to avoid some problems such as forgetting password, losing keys and potential secure problem etc. Biometric recognition technology operates simply, so users can finish identification without special skills and action. As a result biometric recognition technology has drawn more and more attention as a replacement of traditional authentication technology. Recently biometric recognition technology has widely development and application in various fields. However, with the development of technology the traditional, unimodal biometric system performance could not satisfy people's request of security. Multimodal biometric technology is to do identification by using two or more human physical characteristics or behavior characteristics. This paper presents the review of multimodal biometrics. This includes applications, challenges and areas of research in multimodal biometrics. The different fusion techniques of multimodal biometrics have been discussed.

Keywords: Authentication, Biometric, Cryptography, MultimodalRecognition, , Security.

1. INTRODUCTION

Biometric recognition, or simply biometrics, refers to the automatic recognition of individual person based on their physiological and/or behavioral characteristics. Biometrics helps us to confirm or ascertain an individual's identity based on who she/he is, rather than by what she/he possesses (e.g., an ID card) or what she/he knows (e.g., a password). Existing biometric systems make use of identifiers such as fingerprints, hand geometry, iris, face and voice to establish the individuality.

Biometric systems are growing popular as a measure to identify human being by computing one's physiological or behavioral characteristics. Biometrics identifies the person by physiological or behavioral characteristics of the person rather than what the person carries, unlike the conventional authorization systems like smart cards. Unlike the possession-based and knowledge- based personal identification schemes, the biometric identifiers cannot be misplaced, forgotten, guessed, or easily forged. Traditional personal identification approaches use are knowledge-based, something that you know such as Personal Identification Number (PIN), or something that you have, such as an ID card, which are not sufficiently reliable to satisfy the security requirements of electronic transactions because they be deficient in the ability to distinguish between a genuine individual and impostor who fraudulently acquires the access privilege. Biometrics, which refers to the identification of the individual based on his/her physiological or behavioral characteristics, relies on something which you are or which you do to make personal identification and, therefore, inherently has the ability to differentiate between a genuine individual and a fraudulent impostor. Any human physiological or behavioral characteristic can be used as a biometric characteristic (pointer) to make personal identification as long as it satisfies the requirements of the biometrics like Universality, Uniqueness, Durability, Collectability, Performance, Acceptability and Circumvention. The physiological biometric features include face, finger print, speech, gait and so on. The behavioral biometric features include speech, signature, and so on.

This paper is organized with the discussions on Multi algorithm and multi sample approach. The need for multimodal biometrics is illustrated in Section 3, the review of related work, different fusion techniques are presented in Section 4. Applications, challenges and research areas are given in Section 5 and Section 6 respectively. Conclusions and future enhancement are presented in the last section of the paper.

2. MULTIMODAL BIOMETRICS

More than one physiological or behavioral characteristic for enrollment, verification or *identification* is known as **Multimodal Biometrics.** The combination of the Fingerprint, Iris, Retina, Finger, Geometry, Signature/Handwriting, Voice, Facial Proportions and Hand Geometry, are used to evaluate the *identity* of a person and consequently providing the best security measures available. If one of the biometric characteristics fails for any reason, system can still use another one or two of them to provide accurate identification of a person.

3. NEED OF MULTIMODAL BIOMETRICS

Most of the biometric systems deployed in real world applications are unimodal, which rely on the evidence of single source of information for authentication (e.g. fingerprint, face, voice etc.). These systems are susceptible to variety of problems such as noisy data, intra-class variations, inter-class similarities, non-universality and spoofing. These problems lead to considerably high false acceptance rate (FAR) and false rejection rate (FRR), limited discrimination capability, upper bound in

performance and lack of permanence [8]. Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity. These systems allow the integration of two or more types of biometric systems known as multimodal biometric systems. These systems are more dependable due to the presence of multiple, independent biometrics [9]. These systems are able to meet the inflexible performance requirements imposed by various applications. They address the problem of non-universality, since multiple traits ensure sufficient population coverage. They also discourage spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. Furthermore, they can facilitate a challenge – response type of mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a 'live' user is indeed present at the point of data acquisition.

4. RELATED WORK

In 2007**, Mayank Vatsa et al**, proposed a feature based watermarking algorithm to protect the biometric templates in a multimodal biometric system. Using redundant discrete wavelet transform, the voice coefficients are embedded into the color face image while preserving the facial features. The robustness of the watermarking algorithm is evaluated by comparing the recognition accuracies of face, voice, and multimodal biometric algorithms. Experimental results show that the proposed biometric watermarking algorithm is pliant to various signal processing attacks with 0 - 1.3% decreased multimodal biometric verification accuracy.

Kevin Daimi and Katherine Snyder established that to ensure more reliable verification and identification security checks, the traits that really characterize an individual person should be employed. Biometrics furnish this purpose as they offer automated methods for identification and verification based on measurable physiological or behavioral characteristics such as fingerprint , iris, and retina recognition. Security is a need due to the nature of today's society. Security requirements play a critical role in all software systems. This is particularly true when the software system is a security system itself. If a security system, such as a biometric system, is compromised, disastrous consequences are to be expected.

Doroteo T. Toledano, et al emphasized on the use of more modern and ample databases, which can be retracted from using them in order to be able to compare their results to those of other researchers. In this framework, it is necessary to have a way of comparing results across different databases.

Ajay Kumar, et al introduced a new approach for the adaptive combination of multiple biometrics, the results to dynamically ensure the desired level of security is presented. The proposed method uses a hybrid PSO to attain adaptive combination of multiple biometrics from their matching score performance.

Kamalam.K, has made a study on routing protocols in authentication of data transmission through wireless sensor networks.

5. APPLICATIONS

- The defense and intelligence communities need automated methods, which are capable of rapidly determining an individual's true **identity** as well as any previously used identities and past activities, over a geospatial continuum from set of acquired data.

- A homeland security and law enforcement community require technologies to secure the borders and **to identify criminals** in the civilian law enforcement environment. Key applications include border management, **interface for criminal and civil applications, and first responder verification.**

- Enterprise solutions require the oversight of people, processes and technologies. **Network infrastructure has become essential to functions of business, government, and web based business model**s. Consequently providing security in access to these systems and ensuring the user's identity is essential. Personal information and Business transactions require **fraud prevent solutions** with increased security level and have to be cost effective and user friendly.

- Key application areas include customer **verification** at physical point of sale, online customer verification etc.

6.CHALLENGES AND RESEARCH AREAS

Based on applications and facts presented in the previous sections, followings are the challenges in designing the multi modal systems. Successful pursuit of these biometric challenges will generate significant advances to improve safety and security in future missions. The sensors used for acquiring the data should show consistency in performance under variety of operational environment. Fundamental understanding of biometric technologies, operational requirements and privacy principles to enable beneficial public argue on where and how biometrics systems should be used, to be embedded with privacy functionality into every layer of architecture, protective solutions that meet operational needs, enhance public confidence in biometric technology and safeguard personal information are to be studied. Designing biometric sensors, which automatically recognize the operating environment (outdoor / indoor / lighting etc) and communicate with other system components to automatically adjust settings to deliver optimal data, is also a challenging area. The sensor should be fast in acquiring quality images from a distance and should have low cost with no failures to enroll [5].

The multimodal biometric systems can be improved by enhancing matching algorithms, integration of multiple sensors, analysis of the scalability of biometric systems, followed by research on scalability improvements and quality measures to help decision making and in matching

process. Open standards for biometric data interchange formats, file formats, applications interfaces, implementation agreements, testing methodology, adoption of standards based solutions, strategy for auditing biometric systems and records and framework for integration of privacy principles are the possible research areas in the field.

7. CONCLUSION AND FUTURE ENHANCEMENT

This paper presented the various issues related to multimodal biometric systems. By combining multiple sources of information, the improvement in the performance of biometric system can be attained. Various fusion levels and scenarios of multimodal systems are discussed. Fusion at the match score level is the most popular due to the ease in accessing and consolidating matching scores. Performance gain is pronounced when uncorrelated traits are used in a multimodal system. The challenges faced by multimodal biometric system and possible research areas are also discussed in the paper.

In this research we propose a new multimodal biometric system with the combination of Hand Geometry, palm print and knuckle. The idea behind taking these three biometrics is that the three features are extracted from a hand itself. Using a single device we can extract the features of these three modals. In other multimodal biometric system such as face, finger and ear, Irish, face and finger or the combination of multimodal from different portion of body definitely need separate device for extracting the features. In practical there is a need of scanning the features multiple times during online verification of users for the application like attendance tracking, online accounts and etc. So it's not robust for the real-time application. In these scenarios we are proposing these three multimodal biometric and various enhancements in these three systems because each system has its own disadvantages in literature.

To improve the security of our multimodal biometric, we use cryptography to securely store and transfer and biometric features. If the user is able to authenticate himself using a strongly encrypted version of his biometric, that may be a secure biometric system. In literature many problems were identified when biometrics are used in encrypted domain. In our research we analyze the existing problem of cryptography on biometrics and proposed a security in an effective manner.

The future system probably belongs to a secured multimodal biometric systems as they alleviate a few of the problems observed in unimodal biometric systems. Multimodal biometric systems can integrate information at various levels, the most popular one being fusion at the matching score level. Besides improving matching performance, they also address the problem of no universality and spoofing. Finally, the use of biometrics raises several privacy questions. A sound trade-off between security and privacy may be necessary; but we can only enforce collective accountability and acceptability standards through common legislation [1]. For example, if and when face recognition technology improves to the point where surveillance cameras can routinely recognize individuals, privacy, as it has existed in the public sphere, will be wiped out. Even today, in some major cities, you are recorded approximately 60 times during the day by various surveillance cameras

References

[1]. A.K. Jain, A. Ross, "Multibiometric systems". Communications of the ACM, vol. 47, pp. 34-40, 2004.
[2]. Chander Kant, Rajender Nath, "Reducing Process-Time for Fingerprint Identification System", International Journals of Biometric and Bioinformatics, Vol. 3, Issue 1, pp.1- 9, 2009.
[3]. Chang, K. I., K. W. Bowyer, and P. J. Flynn, "An evaluation of multi-modal 2D+3D face biometrics," IEEE Trans. on PAMI 27 (4), pp. 619-624, April 2005.
[4]. Gokberk, B., A.A. Salah. and L. Akarun, "Rank-Based Decision Fusion for 3D Shape-Based Face Recognition," LNCS 3546: AVBPA, pp. 1019-1028, July 2005.
[5]. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition". IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, pp. 4–20, Jan, 2004.
[6]. Phillips, P.J., P. Grother R.J. Michaels, D.M. Blackburn and E. Tabassi and J.M. Bone, "FRVT 2002: overview and summary", March 2003.
[7]. Xu, C., Y. Wang, T. Tan and L. Quan, Automatic 3D face recognition combining global geometric features with local shape variation information," Aut. Face and Gesture Recog., pp. 308 -313, 2004.
[8]. Kamalam.K."Routing Protocols in Authentication way for Data Transmission in Wireless Sensor Networks", International journal for Trends in Engineering and Technology, Vol_10., No-1.,2015.

AUTHOR

A.P.Caroline Hirudhaya received her Ph.D degree from Manonmaniam Sundaranar University in 2015, working as Associate Professor in KG College of Arts and Science, Coimbatore.