ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Biometric Identification Using Eye Tracker

Rameez Ali P[1], S Vijayanand[2]

P.G. Student, Department of Computer Engineering, SVH Engineering College, Gopichettipalayam, Tamilnadu, India[1]

Associate Professor, Department of Computer Engineering, SVH Engineering College, Gopichettipalayam, Tamilnadu, India[2]

ABSTRACT: Biometric identification is one of the most secure existing identification methods. Algorithms based on eye tracking techniques are being studied now by many authors as eye trackershad become more accessible during the last few years. This paper is related to a biometric identification approach and problem of providing accurate identification results by using low frequency eye tracker. This paper presents a review of the related works in the field as well as a general classification of different identification types. We stated a formal description of a saccade and an analyzed fragment of the gaze trajectory containing saccade, which is based on the finite differences method, and revealed features of the eye movements that can be used for the identification purpose. Two classifiers are proposed and compared based on the experimental results obtained for them.

KEYWORDS:Access control, authentication, biometrics (access control), identification of persons.

I. INTRODUCTION

In the wake of heightened regarding security and swift progression in networking, communication and mobility, there are rapid demand in reliable user authentication techniques. Majority of the authentication systems found today are of not very flexible (can be broken or stolen) to attacks, rather it can control access to computer systems or secured locations utilizing passwords. Thus, in most of the application areas, biometrics has emerged practically as a better alternative to conventional identification methods in recent. Biometrics which deals with the science of recognizing a person on the basis her/his physiological or behavioral traits has started to achieve acquiescence as a genuine method for identifying an person`s identity. Biometric technologies have confirmed its importance in the fields such as security, access control and monitoring applications. Technologies are always innovative and seem to be fast growing. Besides conventional authentication methods, biometric systems provides various advantages that are numbered below 1) Using direct covert observation, a biometric information can't be attained 2) reproduction and sharing is impracticable 3) By easing the necessity to keep in mind lengthy and random passwords, it augments user expediency, 4) It safeguards against negation by the user. Unlike passwords, biometrics also bestows the similar level of security to every user and is extremely immune to brute force attacks. The important biometric characteristics currently in use includes fingerprint, DNA, iris pattern, retina, ear, face, thermogram, gait, hand geometry, palm-vein pattern, keystroke dynamics, smell, signature, and voice.

II. RELATED WORK

The vulnerability of conventional biometrics to spoof has caused considerable concern especially in those fields that require high reliable user identification. This heightened concern leads to great interest in assessing the probability and efficiency of using eye movements in identification systems. By applying eye movements as biometrics a new approach has been taken into human identification including all the crucial attributes of previous traditional identification that may offer certain notable advantages. The most obvious is the inherent difficulty in forging them. The purpose of this article is to review examples of researches utilizing eye movements in human identification. These studies can be divided into two groups: the first group utilizes eye movement bioelectrical signals in identification purpose and another one uses eye movement tracking in human identification.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Recently, biometric identification techniques have attracted great attention due to increasing demand of high-performance security systems. Compared with conventional identification methods, biometric techniques provide more reliable and robust solutions. In this paper, a novel video-based biometric identification model based on eye tracking technique is proposed. Inspired by visual attention, video clips are designed for subjects to view in order to capture eye tracking data reflecting their physiological and behavioral characteristics. Various visual attention characteristics, including acceleration, geometric, and muscle properties, are extracted from eye gaze data and used as biometric features to identify persons. An algorithm based on mutual information of features is adopted to perform feature evaluation for obtaining a set of the most discriminative features for biometric identification. Experiments are conducted by using two types of classifiers, Back-Propagation (BP) neural network and Support Vector Machine (SVM). Experimental results show that using video-based eye tracking data for biometric identification is feasible. In particular, eye tracking can be used as an additional biometric modal to enhance the performance of current biometric person identification systems.

III. PROPOSED ALGORITHM

Biometric-based authentication systems represent a valid alternative to conventional approaches. Traditionally biometric systems, operating on a single biometric feature, have many limitations, which are as follows.

1) Trouble with data sensors*:* Captured sensor data are often affected by noise due to the environmental conditions (insufficient light, powder, etc.) or due to user physiological and physical conditions (cold, cut fingers, etc).

2) Distinctiveness ability:Not all biometric features have the same distinctiveness degree (for example, hand geometry-based biometric systems are less selective than the fingerprint-based ones).

3) Lack of universality*:* All biometric features are universal, but due to the wide variety and complexity of the human body, not everyone is endowed with the same physical features and might not contain all the biometric features, which a system might allow.

Biometric systems that generally employ a single attribute for recognition (that is., unimodal biometric systems) are influenced by some practical issues like noisy sensor data, non-universality and/or lack of distinctiveness of the biometric trait, unacceptable error rates, and spoof attacks. Unfortunately, encryption algorithms are designed to remove any similarity that exists within the data to defeat attacks, while pattern classification algorithms require the similarity of data to be preserved to achieve high accuracy.Fig. 1. Shows scheme of the identification algorithm.

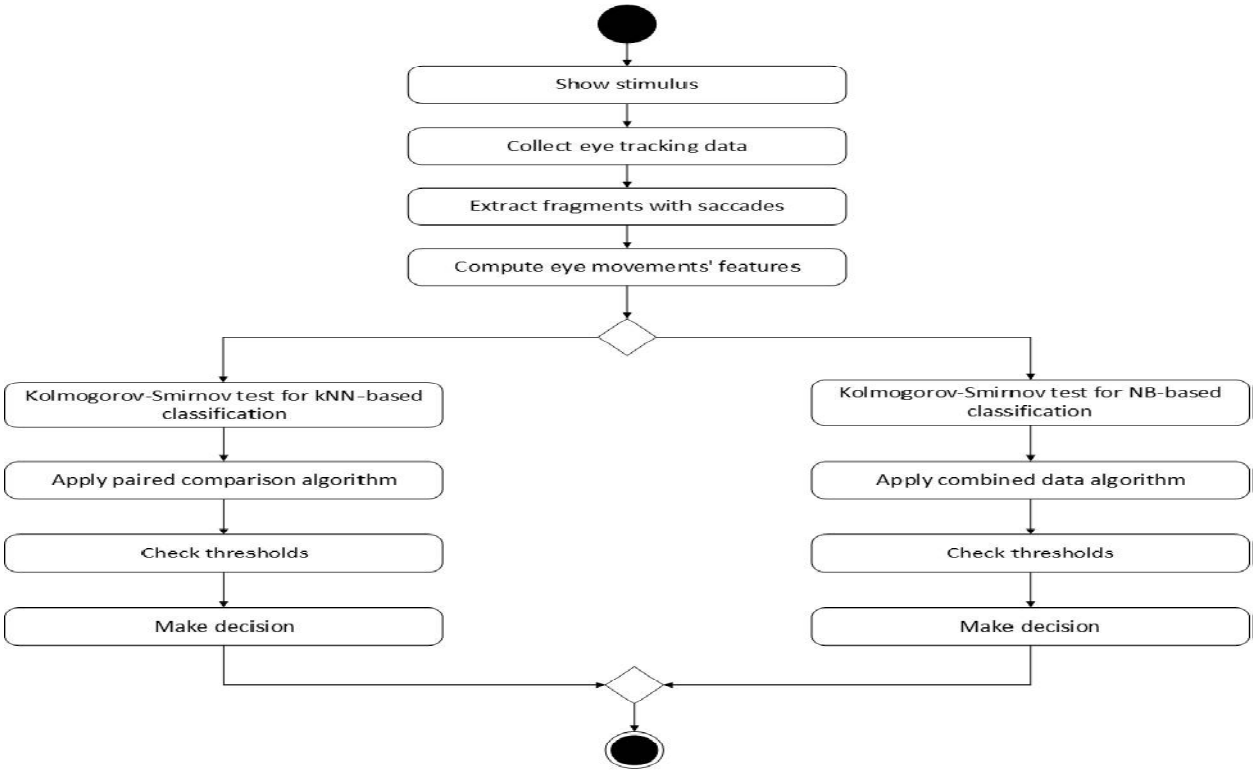

Fig. 1. Scheme of the identification algorithm.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Eye movement characteristics: Eye movements are generated by complex anatomical components, in which six Extraocular Muscles (EOMs) move the eye globe. These movements are subject to the muscular features and tissues surrounding the eye globe Eye movements are basically of two types: fixations and saccades [. A fixation is the maintaining of the eye focus on a single location to capture EOM characteristics by extracting the velocity and acceleration of the fixations and saccades made by the eye. This approach requires a preprocessing step were the complete eye movement signal is filtered using low-pass and moving average function. A Velocity–Threshold (I-VT) algorithm was implemented to identify saccades and fixations in the filtered signal based on the velocity of the directional shifts of the eye with a threshold of 40°/s. The threshold value was derived from the work. Additional filtering was carried out to remove fixations and saccades with a duration less than 16 ms, as those are highly vulnerable to noise, and the unclassified parts of the signal, which normally denote a poor recording quality by the eye tracker. Each classified fixation and saccade as a sub-signal. These sub-signals were statistically processed to calculate their acceleration and velocity, providing a number of features, namely: fixation angular velocity of the eyes, fixation velocity of left and right eye, fixation acceleration of left and right eye, saccade angular velocity of eyes, saccade velocity of left and right eye and saccade acceleration of left and right eye. In addition, three statistical characteristics were computed for each feature: mean, standard deviation, and peak value. All these features were analyzed using a Chi-squared ranking technique to determine their importance and remove irrelevant ones. While initially 36 features were defined for eye movements and 48 for iris, the relevant input features used in this work were 24 for eye movements and 18 for iris. The top-ranked input features were the mean and standard deviation of eye movement and iris velocity, and the peak value of eye movement and iris acceleration.

CLIENT BASED LOGIN AND CRYPTO FUSION MATCHING REQUEST: At present, we have three sets of features. They are as follows 1) Fingerprint features, 2) Iris features and 3) Face features. The three sets of features are fused to obtain a multimodal biometric template that can carry out biometric authentication. A multi-biometric fusion template is used for generating a 256-bit cryptographic key which is used for cryptosystem with user authentication.

As per procedure client need to clears the login access for to access account thus send the fusion value which generated from multi biometric images given at client side. Send the fusion value as key with encrypted identity data to the server.

IV. SIMULATION RESULTS

Implementation is stage in the thesis where the theoretical design is turned into the working system. The most crucial stage is giving the users confidence that the new system will work effectively and efficiently. The performance of reliability of the system is tested and it gained acceptance.

Multimodal biometric systems elegantly address several of the problems present in unimodal systems. By combining multiple sources of information, these systems improve matching performance, increase population coverage, deter spoofing, and facilitate indexing. Various fusion levels and scenarios are possible in multimodal systems. 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. Incorporating user-specific parameters can further improve performance of these systems.

The use of multimodal biometrics for key generation provides better security, as it is made difficult for an intruder to spool multiple biometric traits simultaneously. Moreover, the incorporation of biometrics into cryptography shuns the need to remember or carry long passwords or keys. The steps involved in the proposed multimodal-based approach for cryptographic key generation are,

1) Feature extraction from fingerprint.
2) Feature extraction from iris.
3) Feature extraction from face.
4) Fusion of fingerprint, face and iris features.
5) Generation and Matching of cryptographic key from fused features.

In addition, the achievable accuracy is analyzed in terms of false acceptance rate/false rejection rate at each model. Finally, a comparison on the relative advantages and disadvantages of the proposed models is discussed in the following parameters.In a multi biometric system operating in a verification mode, there are four possible outcomes:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

1) Genuine acceptance;
2) Imposter rejection;
3) Genuine rejection (false reject);
4) Imposter acceptance (false accept).

Decision Level Matching Accuracy: An efficient and accurate alignment algorithm in the preprocessing stage plays a crucial role in the performance of the whole system, affecting greatly the speed and accuracy otherwise. As consider this our proposed work gives better accuracy then the existing one.

Consequently, the overall performance of feature extraction and fusion matching can be significantly improved by combining results of several matchers when compared on existing work.Hence, the combination of these alignment fusion methods effectively strengthens the performance of the matcher.

V. CONCLUSION AND FUTURE WORK

Security and accuracy are two major factors influencing the performance of a biometric cryptosystem. The majority of work in this field uses average min-entropy or conditional Shannon entropy as the security metric. However, in this work, we point out the limitation of entropy in measuring the security of biometric cryptosystems, and correct the entropy-based security analysis of some popular fingerprint based cryptosystems. Then we propose a new security analysis framework, which jointly considers information-theoretic and computational security, thus being able to measure the security of biometric cryptosystems more comprehensively. In terms of accuracy analysis, we reanalyze the accuracy of MBCF and MBCD from the theoretical perspective. The results show that better accuracy of MBC than SBC is not theoretically guaranteed. As a matter of fact, whether or not MBCF or MBCD can offer an improvement of accuracy over SBC depends on several factors: selected biometric traits, fusion algorithms, decision rules, etc. Finally, we propose a practical MBCD construction, which uses fingerprints from multiple fingers to encrypt the cryptographic key. The experimental results and security analysis prove that the proposed construction provides stronger security and better authentication accuracy compared to the corresponding SBC.

However, widespread applications of biometrics have brought about new security challenges. Proposed methods to improve the security analysis by accurately modeling the biometric feature distributions; and evaluation of the proposed cryptosystem on large multimodal databases. So for future work, we will try to incorporate these features into the state-of-the-art minutiae-based matchers for further improvement of the matching performance. Also, our matching method needs to be improved for images with a small foreground area and those of low quality. Therefore, in future work, we will develop the use of global knowledge of multibiometric, such as fingerprint - singular point position, to enhance the matching accuracy. We will also develop a robust preprocessing method to reduce enhancement errors. The above concepts and techniques open up some important avenues for future research.

REFERENCES

[1] Y. Sutcu, Q. Li, and N. Memon, "Secure biometric templates from fingerprint-face features," in Proc. IEEE Conf. Comput. Vis. PatternRecognit. (CVPR), Minneapolis, MN, USA, Jun. 2007, pp. 1–6.
[2] A. Ross, J. Shah, and A. K. Jain, "From template to image: Reconstructing fingerprints from minutiae points," IEEE Trans. Pattern Anal.Mach. Intell., vol. 29, no. 4, pp. 544–560, Apr. 2007.
[3] S. Wang and J. Hu, "Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach," PatternRecognit., vol. 45, no. 12, pp. 4129–4137, Dec. 2012.
[4] T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinate-based cancelable fingerprint templates," Pattern Recognit., vol. 44, nos. 10–11, pp. 2555–2564, Oct./Nov. 2011.
[5] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," IEEE Trans. Pattern Anal. Mach.Intell., vol. 29, no. 4, pp. 561–572, Apr. 2007.
[6] C. Lee, J.-Y. Choi, K.-A. Toh, and S. Lee, "Alignment-free cancelable fingerprint templates based on local minutiae information," IEEE Trans.Syst., Man, Cybern. B, Cybern., vol. 37, no. 4, pp. 980–992, Aug. 2007.
[7] A. Cavoukian and A. Stoianov, "Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy," Information Privacy Commissioner, Toronto, ON, Canada, Tech. Rep., 2007. [8] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," Proc. IEEE, vol. 92, no. 6, pp. 948–960, Jun. 2004.
[9] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in Proc. 6th ACM Conf. Comput. Commun. Secur., Singapore, 1999, pp. 28–36.
[10] A. Juels and M. Sudan, "A fuzzy vault scheme," Designs, Codes Cryptograph., vol. 38, no. 2, pp. 237–257, Feb. 2006.
[11] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in Proc. Eurocrypt, 2004, pp. 523–540.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

[12] J. D. Golic and M. Baltatu, "Entropy analysis and new constructions of biometric key generation systems," IEEE Trans. Inf. Theory, vol. 54, no. 5, pp. 2026–2040, May 2008.
[13] B. Fu, S. X. Yang, J. Li, and D. Hu, "Multibiometric cryptosystem: Model structure and performance analysis," IEEE Trans. Inf. ForensicsSecurity, vol. 4, no. 4, pp. 867–882, Dec. 2009.
[14] A. Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric cryptosystems based on feature-level fusion," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 255–268, Feb. 2012.
[15] K. Nandakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," in Proc. IEEE Int. Conf. Biometrics, Theory, Appl. Syst., Arlington, VA, USA, Sep./Oct. 2008, pp. 1–6.