SECURE AUTHENTICATION TECHNIQUES USING BIOMETRICS- A SURVEY

Sahana Serin Valiyaparambil1, Maya Mohan2, and Sruthy Manmadhan3
1M.Tech First Year Student, 2,3Assistant Professor
Department of Computer Science and Engineering,
N.S.S College of Engineering, Palakkad
Email: 1sahanaserinvp@gmail.com, 2mayajeevan@gmail.com, 3sruthym.88@gmail.com

***Abstract*—Protecting the sensitive information is paramount important in this digital world due to the vulnerable access by malicious users. To protect the information traditionally used authentication systems are based on the password, pattern, access card, lock and key etc. The identity of the user using traditional trends have a lot of issues of stolen the card, misuse of card, forgotten the password and different password attacks. To overcome these security breaches, new authentication techniques based on biometrics are introduced. Biometric is a technology of analysing and measuring biological data. It is the most trustworthy measure to identify a person uniquely. Using biometrics, a persons identity could be determined without any authority or knowledge. The merits of biometric are its uniqueness and stability that considered as an ideal biometric identifier. This paper introduces some biometric based authentication techniques that are using different kinds of biometrics and their fusion. The techniques includes authentication using fusion of finger knuckleprint and palmprint, face, ECG, low frequency brain signals, and combination of iris and sensor. This paper also discusses about the advantages, security and robustness of using biometric for authentication.**

Keywords : Biometrics, Unimodal, Multimodal, ECG, Authentication, Continuous authentication, Brain signals, Palmprint, Knuckleprint.

I. Introduction

Authentication is the process of determining whether someone is who it is declared to be. It is the process of verifying identity of the user. Biometrics is the technical term for body measurements and calculations. It refers to metrics related to human biological characteristics. The authentication techniques using human biological characteristics are referred to as biometric authentication. Traditional authentication systems are based on password, pattern, access card, lock and key etc. The identity of the user using traditional trends have a lot of issues of stolen the card, misuse of card, forgotten the password and different password attacks. To overcome these security breaches, new authentication techniques based on biometrics are introduced.

Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify that he or she is who is says he or she is. Biometric authentication systems compare a biometric data captured with confirmed authentic data in a database. If both samples of the biometric data match, authentication is confirmed. Biometric security has significant advantages over other forms of identification: it is fast and easy to use, and unlike a login or password, which requires memorization and is easily replicable, an individuals fingerprints, irises, and facial constructs should be impossible to duplicate. There are several techniques for biometric based authentication such as face recognition, ECG authentication, combination if iris and sensor, low frequency brain signals, fusion of finger knuckleprint and palmprint etc.

Biometric authentication is a what you are factor and it is based on unique individual characteristics. Two types of biometric properties are useful for authentication. Physical biometrics include DNA, fingerprints, facial recognition, and eye scans like iris and retina. Behavioral biometrics include voice recognition and handwritten signatures. The biometric authentication process consists of several stages: measurement, signal processing, pattern matching, and decision making.

II. Related Works

There are several techniques of biometric authentication. The oldest known use of biometric verification is fingerprinting. There are mainly three kinds of authentication:

- Unimodal authentication
- Multimodal authentication
- Continuous authentication

This chapter summarizes five different techniques of biometric authentication, unimodal authentication using face recognition, unimodal authentication using ECG signals, multimodal authentication combining iris and sensor, continuous authentication using brain signals and multimodal authentication combining palmprint and finger knuckleprint.

A. Authentication using Face Recognition

Vazquez-Fernandez et al in [1]presented the issues of using face recognition for authentication on mobile devices. Face recognition is the most common biometric authentication technique. It have advantages like ease of use, availability and security. But it have a lot of disadvantages like spoofing, stealing of template, power consumption, and unavailability under different lighting conditions etc. Nowadays, photos are publicly available on social networks like facebook. Using photos an attacker can authenticate to a face recognition system. Liveness detection is the major solution to this kind of spoofing.

Stealing of template is another issue in face recognition. A solution for this issue is that we can transform the biometric to template in a such a way that it satisfies three properties: Revocability, Renewability and Irreversibly. When using biometric authentication in mobile devices, power consumption is an issue. We can reduce power consumption by using energy efficient authentication algorithms[2]. One of the major issues in face recognition is availability under different lighting conditions. Face recognition can not use under darkness, strong sunlight and shadows.

B. ECG Authentication on Mobile Devices

ECG (Electocardiogram) is the process of recording the electrical activity of the heart over a period of time using electrodes placed on the skin. ECG can be used as a biometric technique for authentication on mobile devices. In order to apply ECG authentication to mobile phones, a number of factors need to be considered, namely, the number of electrodes, quality of mobile ECG sensors, time required to gain access to the phone. There are several ECG based algorithms but most of them takes large access time and some can not be used in mobile devices. Arteaga-Falconi et al in [3] presented an algorithm that takes only 4 s of acquisition time and can be used in mobile devices. This algorithm uses 2 electrodes (lead I) to record ECG signals. An ECG signal is distinct for every individual. Its uniqueness is a result of gender, heart mass orientation, conductivity, and order of activation of cardiac muscles. Peaks of ECG signal are P, R, and T, valleys are LP, Q, S, and TP. In this algorithm user need to touch two electrodes attached on the mobile back case using fingers. In the first stage, peaks and valleys (fiducial points) from the ECG signal are detected[4]. This allows us to align and normalize the signal in order to avoid the effects of changes in heart rate. Alignment is the process consists of shifting all the ECG heartbeats to align them around a reference point. Since R is the fiducial point less affected by noise (due to its distinguishable form), we use it to align all ECG heartbeats. Once the signal is normalized, we proceed to extract the features. If we are enrolling a new user, the extracted features allow us to create an enrollment template to be stored in memory. If we are authenticating a user, the extracted features generate an authentication template. This authentication template is used by the algorithm to authenticate a user against an enrollment template.

C. Multimodal Authentication Using Iris and Sensor

Multimodal authentication uses more than one traits for authentication. To improve biometric recognition robustness against attacks it is worth using multimodal recognition. Galdi et al in [5] presented a multimodal authentication system based on the combination of sensor recognition (hardwaremetry) and iris recognition (biometry). This can be implemented using smartphones. In this technique, iris image is captured using cameras and by finding sensor patters on the captured image, the camera model is identified. If both iris and sensor model matches, access granted. Hardwaremetry: In order to recognize the sensor that captured a given photo, we implemented the ESPN (Enhanced Sensor Pattern Noise) based algorithm presented by Li in[6]. This method extracts from a picture the noise pattern of the sensor, it can also be used to distinguish cameras of the same model. Biometry: For iris recognition here use CSUMs (Cumulative SUMs) algorithm[7]. This method analyzes the image local variation in gray level. In our implementation, the iris image is ïňĄrst normalized transforming the Cartesian coordinates in polar ones, obtaining a rectangular shape. Then the image is subdivided into cells and for each cell, the representative value X is computed as the average gray level. Then the cells are grouped (horizontally and vertically in turn) and the average value $\overline{X}$ of the representatives of the cells of each group is computed. Then CSUM is calculated for each group. Finally, the iris code is generated comparing each pair of consecutive sums and assigning values 1 or 2 to a cell if the value of the corresponding sum contributes respectively to an upward slope or to a downward slope. Otherwise, value 0 is assigned to the cell. The matching of the iris codes is performed by Hamming distance. If both iris code and noise pattern matches, then grant access to the user.

D. Continuous Authentication Using Brain Signals

Continuous authentication is a class of dynamic authentication that emphasizes authentication through a complete login session. Most users are familiar with the different forms of veriffcation needed to login to their computers, access their email accounts, or open their companys shared server. But in most of these instances, the user enters their username and password once, leaving these systems vulnerable to security breaches for the remainder of the workday. Continuous authentication is one of the new technologies which uses a persons behavior to continuously verify their identity throughout a session, not just at the entry login point. Continuous authentication is a method to identify uninterruptedly whether a subject is an eligible person or not. On the other hand, traditional authentication methods are static or one-time by using a password, a PIN (Personal Identiffcation Number), an electromagnetic card or a physical key. Such static authentication does not consider the weakness to impersonation at all. Therefore, a combination of both methods is expected to realize a better authentication system to the rapidly sophisticated ICT (information and communication technologies) world.

One of the biometrics suitable for continuous authentication is brain signals. This technique is presented by Matsuyama et al in [8]. Brain signals measured by near infrared spectroscopy (NIRS) can be used here. NIRS is more suited to continuous authentication than electroencephalogram (EEG). NIRS measures low frequency brain signals while EEG measures high frequency brain signals. NIRS machines can monitor changes in oxyhemoglobin, deoxyhemoglobin, and the total hemoglobin content and its normalized value. The subject has been assigned a typing task as an example, and probes are attached to his forehead. The brain signals of subject is collected when he is in rest case as well as when he is typing something[9]. Applications:

- The case where super user of a computer is periodically required to type a password.
- Authentication of a special purpose vehicle [10].

- Special Motorcycles.

E. Multimodal Authentication Using Palmprint and Finger Knuckleprint

Multimodal biometric is the usage of multiple biometric indicators by personal identification systems for identifying the individuals. Multimodal authentication provides more level of authentication than unimodal biometrics which uses only one biometric data such as fingerprint or face or palm print or iris. Here palmprint is combined with finger knuckleprint. . In past few years, society have noticed great attention in hand based biometric recognition systems (e.g. palm print [11], fingerprint and finger knuckleprint [12]) because of their low cost acquisition sensors, high performance, higher user acceptance and lesser need of user cooperation. The pattern formations at finger knuckle bending [13] as well as palmprint region are supposed to be stable and hence can be considered as discriminative biometric traits. Multimodal authentication using combination of palmrint and finger knuckleprint is presented by Nigam et al in [14]. Multimodal authentication provides more level of authentication than unimodal biometrics which uses only one biometric data such as fingerprint or face or palm print or iris. Here palmprint is combined with finger knuckleprint. The inner part of the hand is called palm and the extracted region of interest in between fingers and wrist is termed as palmprint. Pattern formation within this region are suppose to be stable as well as unique. Even mono zygotic twins are found to have different palmprint patterns. Hence one can consider it as a well-dened and discriminative biometric trait.

The first step in any biometric based authentication system is ROI (Region of interest) extraction[14]. In this work palm and knuckleprint ROI's are extracted. The next stage is transformation, where the ROI of palmprint and knuckleprint samples are normalized to smaller size in order to reduce the computation time. Every ROI is transformed into its corresponding vcode and hcode using SLG (Sign of Local Gradient) method [14]. vcode and hcode are more stable than gray-scale image and can provide robust features. Then matching of features extracted from hcode and vcode are done separately and finally score level fusion is done[15].

III. Discussions and Findings

Biometric authentication is a security process that uses unique biological characteristics of an individual to verify that he or she is who is says he or she is. Biometric authentication systems compare a biometric data capture to stored, confirmed authentic data in a database. If both samples of the biometric data match, authentication is confirmed. Biometric authentication is much easier to use than a password, especially a long one. It only takes a second (if that) for the most modern smartphones to recognize a fingerprint and allow a user to access the phone.

There are several kinds of biometric authentication. Biometric authentication systems that are using single biometric trait of the individual identification are called unimodal systems. Biometric systems which uses or are capable of using a combination of two or more biometric modalities to identify an individual are called multimodal biometric systems. The most important reason behind using multimodal biometric systems is to improve the recognition rate. Biometrics is used in many applications such as border control and voter id issuance. Theoretically, unimodal biometric identification might seem very proficient but in reality there are numerous challenges when enrolling large populations using just a single (unimodal) biometric. The major issue with unimodal biometric system is that only one technology can not be suitable for all applications. So using a multimodal biometric system will compensate the limitations of Unimodal biometric system.

Face recognition is the most common biometric authentication technique. It have advantages like ease of use, availability and security. But it have a lot of disadvantages like spoofing, stealing of template, power consumption, and unavailability under different lighting conditions etc.

ECG based authentication is a most secure technique which utilizes ECG signals for authentication. The human ECG, an electrical signal that is associated with the electrical activity of heart offers several benefits as a biometric: it is universal, continuous and difficult to falsify. The ECG signal from different individuals confirm to a fundamental morphology but also exhibits several personalized traits, such as relative timings of the various peaks, beat geometry, and responses to stress and activity. ECG based authentication technique have several advantages over face recognition like it is invisible to others, less signal acquisition time and less false acceptance rate etc. Eventhough it is more secure unimodal authentication technique, it is very difficult to implement since it has very complex design. This technique can be used in mobile devices too.

Multimodal authentication techniques that combines iris and sensor and palmprint and finger knuckleprint have more advantages over unimodal systems. The technique that combiles iris and sensor is very easy to use and it is applicable to smartphones. It is applicable when any user has to authenticate to a system using his smartphone. The use of the recognition of the smartphone in addition to the iris (combination of hardwaremetry and biometry) makes the spoofing attacks more difficult to be carried on. The opponent has to spoof both modules. So it is more complicated than spooïňĄng a system based only on biometric recognition. Multimodal system that combines palmprint and finger knuckleprint is easy to use and provide high performance. Since knuckleprint acquisition is not very common, it requires complex hardwares. A class of dynamic authentication that emphasizes authentication through a complete login session is called continuous authentication. Continuous authentication is just that a technology that can continuously verify the identity of the user throughout a session. Continuous authentication works passively in the background without disrupting the user experience. It is used in several applications like the case where super user of a computer is periodically required to type a password, authentication of a special purpose vehicle, special motorcycles etc. It is most accurate than singlemodal and multimodal biometric authentication and provides actual fraud detection. A general

comparison between these five techniques are given in the table 4.1 below.

TABLE I
COMPARISON

Technique	Advantages	Disadvantages
Face Recognition	Availability, Usability and Security	Spoofing, Stealing template and Power consumption
ECG	Invisible to others and less signal acquisition time	Difficult to implement and complex design
Iris and Sensor	More secure and applicable on Smartphone	Require dedicated sensor
Brain Signals	Reliable and low error rate	Complex design
Palm print and Knuckle print	Easy to implement and high performance	Require complex hardware for Knuckleprint acquisition

IV. CONCLUSION

Authentication is the process of determining whether a person is who he or she claims to be.Traditional authentication systems such as password, pattern, access card, lock and key etc have several issues like stolen the card, misuse of card, forgotten the password and different password attacks. To make the authentication process more secure, biometrics are used. Here we identified various techniques of secure authentication using biometrics. Authentication using face recognition have several issues like anti spoofing, template protection, availability under diiferent conditions and power consumption. We identified a new ECG authentication algorithm that can be used in mobile devices. The algorithm uses ECG for authentication and takes 4s for authentication. Then we studied multi modal authentication using iris and sensor recognition on smartphones. It is based on the combination of sensor recognition (hardwaremetry) and iris recognition (biometry), i.e, something the user has and something the user is.

Unimodal authentication uses only one biometric trait for authentication and multimodal uses more than one traits for authentication. Then we studied about another class of authentication that is continuous authentication using low frequency brain signals. And finally hand biometric system fusing finger knuckleprint and palmprint. Multimodal systems are more secure than single modal systems. But its implementation is a little complex and require additional hardware or sensors. And it requires more processing power too. This multimodal authentication technique is fusion of palmprint and finger knuckleprint. It uses palmprint and finger knuckleprint as two biometric traits. Use of more biometric modalities has resulted in secure and high accurate biometric identification system, while the unimodal biometric system will not be able to give correct identification for non-universality. For an example, some percentages of the people may wear cut prints, fingerprint where the biometric can reduce the incorrect results. In multimodal biometric systems, one failure of the technology cannot effect on the individual identification and technologies have been successfully used. Therefore spoofing is reduced to a greater extent and will improve the efficiency of whole system.

REFERENCES

[1] Esteban Vazquez-Fernandez and Daniel Gonzales-Jimenez, (November 2016) , "Face recognition for authentication on mobile devices", *Image and Vision Computing*, Vol. 55, pp. 31-33.

[2] C. Ding and D. Tao, (2015) , " Robust face recognition via multimodal deep face representation", *IEEE Transactions on Multimedia*, Vol. 17 no. 11 pp. 2049-2058.

[3] Juan Sebastian Artiaga-Falcony, Hussein Al Osman and Abdulmotaleb El Saddik, (2015) , "ECG Authentication for Mobile Devices", *IEEE Transactions on Instrumentation and Measurement*.

[4] N. M. Arzeno, Z.-D. Deng, and C.-S. Poon, (2008) , " Analysis of first-derivative based QRS detection algorithms" , *IEEE Trans. Biomed. Eng.*, vol. 55, no. 2, pp. 478-484.

[5] Chiara Galdi, Michele Nappi and Jean-Luc Dugelay, (October 2016) , " Multimodal authentication on smartphones: Combining iris and sensor recognition for a double check of user identity", *Pattern Recognition Letters*, Vol. 82, pp. 144-153.

[6] C. T. Li, (2010) , " Source camera identiïňĄcation using enhanced sensor pattern noise", *IEEE Trans. Inf. Forens. Secur.* vol. 5 no. 2 pp. 280-287.

[7] J. G. Ko, Y. H . Gil, J. H. Yoo, K. I. Chung, (2007) " A novel and efficien tfeature extraction method for iris recognition", *ETRIJ.* vol. 29(3) pp. 399-401.

[8] Yasuo Matsuyama, Michitaro Shozawa and Rayota Yokote, (September 2015) , " Brain signalâĂŹs low-frequency fits the continuous authentication", *Neurocomputing*, Vol. 164, pp. 137-143.

[9] Y. Matsuyama, F. Matsushima, Y. Nishida, T. Hatakeyama and N. Ochiai,S.Aida, (2009) " Multimodal belief integration by HMM/SVM-embedded Bayesian network: applications to ambulating PC operation body motions and brain signals" , *Lecture Notes in Computer Science*, vol. 5768, pp. 767-778.

[10] I. Nakanishi and S. Baba, S. Li, (2011) , " Evaluation of brain waves as biometrics for driver authentication using simpliïňĄed driving simulator", *Proceedings of the International Conference on Biometrics and Kansei Engineering*, pp. 71-76.

[11] G. Badrinath and P. Gupta, (2014) , " Palmprint based recognition system using phase difference information", *Future Gener. Comput. Syst.*, in press.

[12] A. Nigam and P. Gupta, (2011) , " Finger knuckleprint based recognition system using feature tracking", *Chinese Conference on Biometric Recognition*, pp. 125-132.

[13] L. Zhang, L. Zhang, D. Zhang and H. Zhu, (2011) , " Ensemble of local and global information for ïňĄnger-

knuckle-print recognition", *Pattern Recognit*. vol. 44 (9) , pp. 1990-1998.

[14] Aditya Nigam and phalguni Gupta, (March 2015) , " Designing an accurate hand biometric based authentication system fusing finger knuckleprint and palmprint", *Neurocomputing*, Vol. 151, Part 3, pp. 1120-1132.

[15] B. D. Lucas and T. Kanade, (1981) , " An iterative image registration technique with an application to stereo vision", *International Joint Conference on Artificial Intelligence*, pp. 674-679.