International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)

International Conference on Information Systems and Computing (ICISC-2013), INDIA.

A REVIEW ON CONTINUOUS AUTHENTICATION USING MULTIMODAL BIOMETRICS

S.Sudarvizhi[1], S.Sumathi[2]

[1]M.E Scholar, Communication Systems, Sri Sairam Engineering College, Chennai, India;
[2]Associate Professor, ECE, Sri Sairam Engineering College, Chennai, India.

Email: sudarvizhishanmugam@gmail.com

Abstract

Most existing computer and network systems authenticate a user only at the initial login session. This could be a critical security weakness, especially for high-security systems because it enables an impostor to access the system resources until the initial user logs out. This situation is encountered when the logged in user takes a short break without logging out or an impostor coerces the valid user to allow access to the system. Thus to ensure authenticity of the user during their entire active login period, a continuous verification is required. The current paper considers continuous unobstrusive biometric authentication as an approach to eliminate this problem. This paper discusses about the number of research works introduced to overcome the difficulties faced in continuous authentication.

Keywords-- **Continuous Authentication; Multimodal Biometrics; Continuous Verification;**

I. Introduction

USER authentication is extremely important for computer and network system security. Currently, knowledge-based methods (e.g., passwords) and token-based methods(e.g., smart cards) are the most popular approaches. However ,these methods have a number of security flaws. For example, passwords can be easily shared, stolen, and forgotten [1], [2].Similarly, smart cards can be shared, stolen, duplicated, or lost. To circumvent these issues,a number of login authentication methods, including textual , graphical passwords[3] and biometric authentication [4], have been utilized.

All of the above login methods share a common problem, namely, they authenticate a user only at the initial log-in session and do not reauthenticate a user until the user logs out. Anyone can access the system resources if the initial user does not properly log out or the user leaves the workstation unattended to take a short break without logging out. To resolve this problem, the system must continuously monitor and authenticate the user after the initial login session. In order to achieve this objective, we need to develop robust, reliable, and user-friendly methods for continuous user authentication. It is desirable that the resulting system has good usability by authenticating a user without his active cooperation.

Continuous Authentication is essential in online examinations where the user has to be continuously verified during the entire session. It can be used in many real time applications, when accessing a secure file or during the online banking transactions where there is need of highly secure continuous verification of the user. A number of biometric characteristics exist and are used in various applications. Each biometric has its own strengths and weaknesses, and the choice depends on the application.

Some of the commonly used hard biometrics are Face, Hand geometry, Fingerprint, Iris. Soft biometrics include Keystroke, Voice, Colour of the clothing, Facial colour etc [1,2]. A single biometric trait (unimodal technique) is not sufficient to authenticate a user continuously because the system sometimes cannot observe the biometric information. To address the limitations of single biometrics, using multimodal biometrics is a good solution. It is the combination of two or more biometric traits to raise systems security and reliability.

Multimodal has several advantage over unimodal. Combining the results obtained by different biometric traits by an effective fusion scheme can significantly improve the overall accuracy of the biometric system. Multimodal system increases the number of individuals that can enroll. It provides resistance against spoofing.

The proposed work includes Sclera and Fingerprint as their Multimodal biometric traits for continuous authentication of the user. The blood vessel structure of the sclera is unique to each person, and it can be remotely obtained non intrusively in the visible wavelengths.

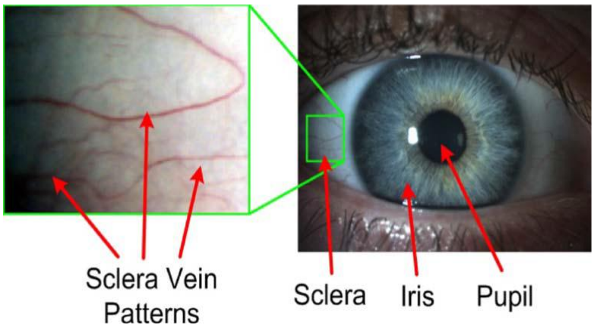


Fig.1. Structures of the eye and sclera region.

Therefore, it is well suited for human identification (ID) [5]. **Fig.1** shows the structure of the eye and sclera region. From **Table 1** we observe that iris achieves low FMR compared to face and voice but the proposed method uses Sclera recognition not Iris [2]. The reason is iris recognition need additional NIR illuminators and also the experimental results show that sclera recognition can achieve comparable recognition accuracy to iris recognition in the visible wavelengths [6]. Fingerprint is most unique, consistency over time and inherent ease in acquisition. The accuracy of the currently available fingerprint recognition systems is adequate for verification systems[7].

In continuous verification, we might observe situations like, a particular modality is missing or noisy observed samples etc[8]. For example, keystroke dynamics based detection is not available when a user is reading, face verification fails during user's non-frontal pose in front of the computer or due to poor surrounding light. To overcome these situations a verification process using multiple biometric traits must be designed. This brings in the possibility of different level of fusion and fusion strategies suitable for a continuous verification system.

1.1 Level of Fusion

In multimodal biometric systems information fusion can be classified into two main categories: pre-classification fusion and post classification fusion. In pre classification fusion information is combined prior to applying any matching algorithm, and in post-classification fusion information is combined after the application of matching algorithm[9].

Pre classification fusion can happen in two levels, sensor level and feature level. Post classification fusion can be divided into four categories based on the level of fusion: classifier selection level, decision level, rank level and matching score level [9]. A dynamic classifier selection can choose the best classifier result depending upon the input pattern. In rank level fusion the biometric matcher results are stored in a decreasing order of confidence and there are different methods to combine these rank levels[9].

Table 1
State-of-Art Error rates associated with different Biometric systems

Modality	TestLabel	FNMR	FMR
Fingerprint	FpVTE 2003	0.1%	1%
Fingerprint	FVC 2004	2%	2%
Face	FRVT 2002	10%	1%
Voice	NIST 2004	5-10%	2-5%
Iris	ITIRT 2005	0.99%	0.94%

Fusion at the decision level is considered rigid due to the availability of limited information and generally it is done by logical AND,OR majority voting rule. Fusion at the match score level is usually preferred because it is relatively easy to access and combine the scores presented by the different modalities[10].

II. PROPOSED WORK

The proposed work uses multimodal biometrics for continuous authentication namely sclera blood vein pattern and fingerprint. For initial log in uses sclera blood veins as it is unique to each individual and it is more accurate than any other biometric. The experimental results show that sclera recognition is a promising new biometrics for positive human ID.[7] A new method for sclera segmentation which works for both colour and grayscale images is proposed and, we designed a Gabor wavelet-based sclera pattern enhancement method to emphasize and binarize the sclera vessel patterns [6].Then continuously verifying the user by the biometric mouse.We acquire fingerprint images using the SecureGen^{TM} mouse **Fig.2** .

The mouse comes with a software development kit (SDK) that matches fingerprints, Given a new fingerprint image and a claimed identity, the image is matched against the claimed identity's template (captured at enrollment time) to produce a score S. Each verifier (sclera and fingerprint) computes a score from its input biometric data which is then integrated to arrive at the overall decision whether to accept the user or not. This work is a state of art advancement of Continuous Authentication offering an innovative perspective and primarily focus on the accuracy of the systems in order to reduce the false alarms.

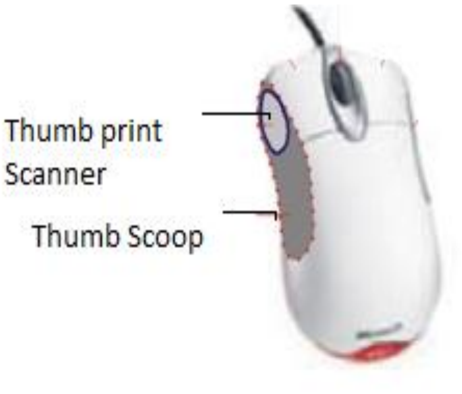


Fig.2 Proposed biometric mouse indicating the proposed position for the thumb print scanner (for a right hand user)

III. RELATED WORK

Some research studies have been reported on continuous authentication. Many of them use multimodal biometrics, but none of them can identify the user in the absence of biometric observation.

Zhi Zhou, Eliza Yingzi Du, and N. Luke Thomas [7] proposed sclera recognition method which can achieve comparable accuracy(EER = 1.34% and 3.83%) with that of the two iris recognition methods using visible-light-acquired images (EER = 2.38% and 3.72%). In particular, note that the iris patterns in dark eyes are hard to extract under visible light illumination. Therefore, these results show that sclera recognition could have some advantage over iris recognition in the visible wavelengths.

F. Pernus, S. Kovacic, and L. Gyergyek defined the Fingerprint is one of the most important biometric technology as it is more distinct, persistence and ease of acquisition. Fingerprint recognition is a process of determining whether two sets of fingerprint ridge detail are from the same person [5]. There are multiple approaches that are used in many different ways for fingerprint recognition which are minutiae, correlation, ridge pattern.

These types of approaches can be broadly categorized as minutiae based or texture based recognition [11].

Minutiae is the most popular approach that is used for fingerprint representation. It is based on local landmarks. The minutiae-based systems locate the points firstly. These points are called minutiae points which represent the fingerprint ridges either terminate or bifurcate in the fingerprint image, and then these minutiae points are matched in a given fingerprint and the stored template.[12] Minutiae points perform fairly high accurate fingerprint matching .

3.1 Hard Biometrics for Continuous Authentication

Hard Biometrics is generally taken to mean the measurement of some physical characteristic of the human body for the purpose of identifying the person. Common types of biometrics include fingerprint, face image, and iris/retina pattern[1],

Sim *et al.* [10] defined three criteria for continuous authentication using hard biometric traits: 1) different reliability of various modalities must be accounted for; 2) older biometric observations must be discounted to reflect their increasing uncertainty about the continued presence of the legitimate user; and 3) the user authentication certainty needs to be established at any point of time even when no observation of any of the biometric traits is available

3.2 Soft Biometrics for Continuous Authentication

Soft biometric traits are defined as “those characteristics that provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate any two individuals”. These traits include gender, ethnicity, colour of eye/skin/hair, height, weight, and SMT (scars, marks, and tattoos)[13,15].

Monrose and Rubin [1] proposed keystroke biometric technique for continuous authentication. When compared to proposed method this is based on a single biometric (unimodal technique), so in the absence of keystroke data, the system is not able to authenticate the user.

Altinok and Turk [16] proposed Continuous authentication techniques using face, voice, and fingerprint. They claimed that a continuous biometric authentication system should be able to provide a meaningful estimate of authentication certainty at any given time, even in the absence of any biometric data. They presented a new temporal integration technique that satisfied this requirement. Each match score is modelled as a Gaussian random variable and, as, the authentication uncertainty increases over time. Surprisingly, even in the absence of any biometric data, Altinok and Turk were able to provide an estimate of the authentication certainty. However, in such a scenario, the authentication certainty must go down rapidly with time in order to maintain the system security, regardless of whether the user is in front of the console or not. This leads to a decrease in the system usability where as in proposed system there is no change in the usability of system since the author is verified continuously during the session.

Sim and Zhang [10, 14] proposed a continuous authentication technique using face and fingerprint biometrics. They used a mouse with a built-in fingerprint sensor, which made fingerprint authentication a passive method for authentication.

The authors proposed that a continuous biometric authentication should satisfy the following three criteria.

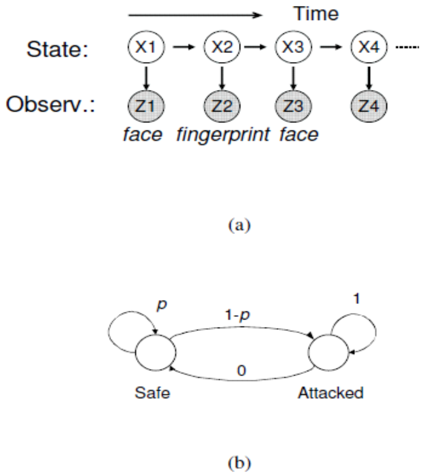
1. The difference in the reliability of different modalities must be accounted for.
2. Older biometric observations must be discounted to reflect the increased uncertainty of the continued presence of the legitimate user with time.
3. It should be possible to determine "authentication certainty" at any point in time, even when no biometric observations are available for one or more modalities.

The authors presented a new Holistic Fusion method that satisfied the above criteria. Their technique was based on using the Hidden Markov Model. **Fig 3** shows hidden model and state transition model. In addition, they proposed several new metrics to measure the performance of a continuous verification system. These include Time to Correct Reject, Probability of Time Correct Reject, Usability, and the Usability-Security Curve.

Sim and Zhang's technique had the same limitations as [16]; when no biometric observations are available, the authentication certainty must go down rapidly with time in order to protect the security, irrespective of whether the user is in front of the console or not. On comparing, the proposed method uses the same fingerprint biometric mouse for verification since sclera is more accurate biometric than face, it is used as initial login.

Similar to Sim and Zhang [10, 14], Azzini and Marrara [18,19] also proposed a continuous authentication technique using face and fingerprint biometrics. Their system checked the identity of the user only on the basis of face recognition. If the authentication certainty of face recognition falls below a threshold, then a new fingerprint acquisition is required. Again, the authentication certainty in this approach must go down rapidly with time in order to ensure the security, regardless of whether the user is in front of the console or not.

This method produces less accurate results in case of absence of particular modalitiy when compared to proposed method.



(a)

(b)

Fig 3 (a) Hidden model (b) State Transition Model

Kang and Ju [20] proposed a continuous authentication technique using face and behavioural biometrics. They used face trajectory and its pose as behavioural features. Because behavioural biometrics were used only for assisting face. Behavioural features are not consistent throughout the session, and also it is soft biometric so less reliable when compared to proposed method where we have used hard biometrics.

IV. Conclusion

It is realistic that initial one time login verification is inadequate to address the risk involved in post logged in session. Therefore this paper attempts to provide a comprehensive survey of research on the underlying building blocks required to build a continuous biometric authentication system. The first challenge is the choice of biometric. The proposed method revealed that sclera, mouse dynamics are the most suitable modalities. The challenge of unavailability of observation of one or more modalities at a particular time is addressed in the section on fusion of modalities.

In this paper we have viewed various existing methods used for continuous authentication using multi modal biometrics. The work done by sim and zhang[10,14] achieves probably accurate results but it is more complex. This is overcome by the proposed method. Continuous authentication is an emerging technique and only limited works were carried out which paves way for the researchers to invent new methods to reduce the error rates and to improve the accuracy and speed of the systems.

Acknowledgements

The authors would like to thanks University of Beira Interior, for providing the UBIRIS database for Sclera recognition and We are also grateful to our Institution for their constant support and encouragement.

REFERENCES

1. Journal Papers

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1,pp. 4–20, Jan. 2004.

[2] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp.125–143, Jun. 2006.

[3] X. Suo, Y. Zhu, and G. Owen, "Graphical passwords: A survey," in Proc. Annu. Computer Security Applications, 2005, pp. 463–472

[5] Zhi Zhou, Student Member, IEEE, Eliza Yingzi Du, Senior Member, IEEE, N. Luke Thomas, and Edward J. Delp, Fellow, IEEE," A New Human Identification Method:Sclera Recognition", IEEE transactions on systems, man, and cybernetics— part a: systems and humans, vol. 42, no. 3, may 2012

[6] S. Vannas and H. Teir, "Observations on structures and age changes inthe human SCLERA," Acta Ophthalmol., vol. 38, no. 3, pp. 268–279,Jun. 2000.

[8] Sandeep Kumar,Terence Sim,Rajkumar Janakiraman and Shen Zhang,"Using Continuous Biometric Verification to Protect Interactive Login Sessions, School of Computing,National University of singapore.

[9] Anil Jain,Kathik Nandakumar and Arun Ross,"score Normalisation in multimodal biometric systems",Pattern Recognition 38(2005)2270 2285.

[10] S. Zhang, R. Janakiraman, T. Sim and S. Kumar, "Continuous Verification Using Multimodal Biometrics," Proc.Second Int'l Conf. Biometrics, pp. 562-570, 2006.

[11] A. K. Jain, S. Prabhakar, and S. Chen, Combining multiple Matchers for a High SecurityFingerprint Verification System, Pattern Recognition Letters, 20(11-13), 1371-1379,1999.

[12] A.K.Jain, L. Hong, and R. Bolle, On-line fingerprint verification, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, 302-314, 1997.Fingerprint Recognition Page 41 of 123

[13] A. K. Jain, S. C. Dass, and K. Nandakumar, "Soft biometric traits for personal recognition systems," LNCS, vol. 3072, pp. 731–738, 2004.

[14] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous verification using multimodal biometrics," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 687–700, Apr. 2007.

[15] A. K. Jain, S. C. Dass, and K. Nandakumar, "Can soft biometric traits assist user recognition?," Proc. SPIE, vol. 5404, pp. 561–572, 2004.

[16] A. Altinok and M. Turk, "Temporal Integration for Continuous Multimodal Biometrics," Proc. Workshop on Multimodal User Authentication, pp. 131-137, 2003.

[17] Terence Sim, Sheng Zhang, Rajkumar Janakiraman and Sandeep Kumar, "Continuous Verification Using Multimodal Biometrics," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, 2007.

[18] Antonia Azzini, Stefania Marrara, Roberto Sassi and Fabio Scotti, "A fuzzy approach to multimodal biometric continuous authentication,"Fuzzy Optimal Decision Making, vol. 7, pp. 243-256, 2008.

2. Text Book

[4] A. K. Jain, P. Flynn, and A. A. Ross, Eds., Handbook of Biometrics. New York: Springer, 2007.

3. Conference Proceedings

[7] F. Pernus, S. Kovacic, and L. Gyergyek, Minutiae-based fingerprint recognition, Proceedings of the Fifth international Conference on Pattern Recognition, 1380-1382,1980.

[19] Antonia Azzini and Stefania Marrara, "Impostor Users Discovery Using a Multimodal Biometric Continuous Authentication Fuzzy System," Lecture Notes In Artificial Intelligence, vol. 5178, Proceedings of the 12th International Conference on Knowledge-Based Intelligent Information and Engineering Systems, Part II, Section II,pp. 371-378, 2008.

[20] Hang-Bong Kang and Myung-Ho Ju, "Multi-modal Feature Integration for Secure Authentication," International Conference on Intelligent Computing, pp.1191-1200, 2006.