THINK INDIA JOURNAL

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

User Authentication Using Hard And Soft Biometric Traits

Surender Kumar[1], Professor (Dr.) R.K Bathla[2]

[1]Research Scholar Department of Computer Science, DeshBhagat University, Mandi Gobindgarh, Punjab &Head, P.G. Department of Computer Science, Sri Guru TegBahadurKhalsa College Sri Anandpur Sahib, Punjab.

[2]Research Guide, Professor Department of Computer Science, DeshBhagat University, MandiGobindgarh, Punjab.

Abstract

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. To deal with these issues, many other login authentication methods, including textual and graphical passwords and biometric authentication such as face recognition and fingerprint have been utilized.

Biometric authentication has been getting widespread attention over the past decade with growing demands in automated secured personal identification. Continuous Authentication (CA) system verifies the user continuously once a person is logged in. Continuous Authentication system prevents the intruders from invoking the system.Continuous user authentication that primarily uses hard and soft biometric traits produce the maximum accuracy compared to existing methods. This paper presents an approach towards implementing continuous user authentication on a personal system by integrating hard and soft biometrics traits.

Keywords: Biometrics recognition, continuous user authentication, integration, soft biometrics, hard biometrics,system login.

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. To deal with these issues, many other login authentication methods, including textual and graphical passwords and biometric authentication such as face recognition and fingerprint have been utilized[1].

Continuous authentication is a guard constantly watching over who is using a computer, using facial features and soft biometric identifying attribute. Continuous identity authentication can prevent an unauthorized person from slipping in and using the computer system after the initial authentication of the identity of the authorized user. The system must continuously monitor and authenticate the user after the initial login session. In order to achieve this objective, there is need of developing 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[2].

II.BIOMETRICS

Biometrics is the science of automatically recognizing people based on physical or behavioural characteristics such as face, fingerprint, iris, hand, voice, gait and signature. In terms of usability, the available methods for continuous authentication are limited. For example, systems that request a user to frequently enter his password for continuous authentication are irritating to the user. The method of limiting user's privilege depending on the availability of hard biometric is also not satisfactory; the user will face the inconvenience with limited privilege whenever the system fails to acquire the user's

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

hard biometric trait. Biometric traits are passive in terms of user involvement (e.g., face and soft biometrics) would be more appropriate for continuous authentication [3].

Biometrics is defined as the identification of an individual based on physiological and behavioral characteristics. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, Palm print, hand geometry, iris recognition, retina. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to: typing rhythm, gait, and voice[4]. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods and are difficult to counterfeit and hence results in higher accuracy when compared to other methods such as using passwords and ID cards [5].

III. SOFT-BIOMETRICS

Soft Biometrics is a set of traits providing information about an individual, though these are not able to individually authenticate the subject because they lack distinctiveness and permanence. These traits include gender, ethnicity, and color of eye/skin/hair, height, weight, and SMT (scars, marks, and tattoos). While soft biometric traits do not have sufficient discriminatory information to fully authenticate the user, it has been shown that they can improve system login security when combined with hard biometric traits (e.g., fingerprint, face, iris, palm vein, etc.). The soft biometric is not meant to uniquely identify a user. However, the soft biometric can be used to decide whether the user who is currently using the system is the same as the user who initially logged in the system. Soft biometric is not expensive to compute, can be sensed at a distance, do not require the additional devices[6].

IV. HARD BIOMETRICS

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[7], Sim et al. [8] 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.

V. PROPOSED WORK

The proposed work uses hard and soft biometric traits for continuous user authentication. Integrated in this implementation are modules—which utilize hard and soft biometrics separately—to continuously verify the user throughout the session. In this system, we use the facial features (e.g. face) of the user as the hard biometric trait, which is captured using an image-based face recognition algorithm. Weuse the color of user's clothes for the soft biometric measure, since it is more tolerant towards the user's posture. The control flow of the system alternates between the soft and hard biometrics module depending upon the need to reinforce the system's belief.

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

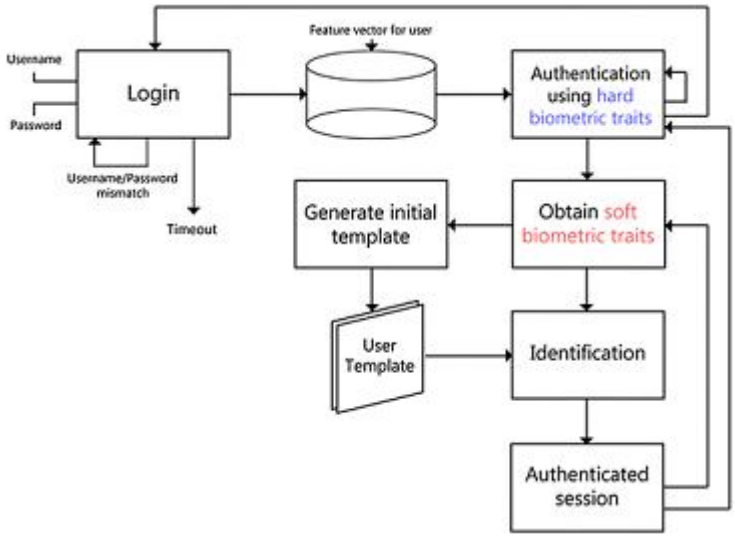

Figure1: User Authentication System Architecture

When the user successfully logs-in, the control alternates between the hard and soft biometrics mode.This framework consists of four modes as described in Figure 2.

a) Mode I- Initial Login – Authentication

b) Mode II- Continuous Authentication

c) Mode III- Enrolment Template Update

d) Mode IV- Re-login Authentication

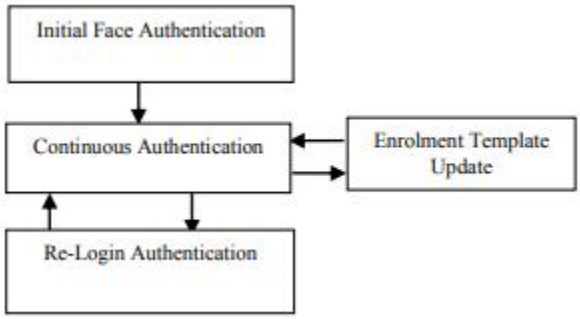

Figure2: Continuous User Authentication Framework

a) Initial Login – Authentication Mode

In this mode , the user is authenticated based on their facial features(e.g. face of the user).

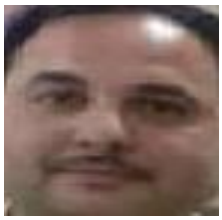

Figure 3: Soft Face, Hard Face

b) Continuous Authentication Mode

Continuous authentication starts after login session. The system continuously authenticates the user by using the “soft face” and “clothing” enrolment templates registered in Mode I (initial login authentication as in Fig 3). Any time the system recognizes that the user is no longer present in front of the console, the system status changes to Mode III (enrolment template update).

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

c) Enrolment Template Update Mode

The system status enters Mode III whenever the similarity score falls below threshold score due to the change in the ambient illumination or user's absence in front of the console.This mode is introduced to reduce the false rejects caused by illumination changes.When an illumination change is detected, we update the user's biometric template to maintain successful continuous authentication in the modified operating environment.

d) Re-login Authentication Mode

The status moves to this mode every time the system detects that the user is no longer in front of the console. In this mode, the system is locked and it tries to detect the user and re-authenticate him automatically. If the system detects a user and re-authenticates the user as genuine, thestatus moves to Mode II again.There will be a small discontinuity in the values of soft biometrics if the imposter tries to replace the authenticated user. When there is a discontinuity in the similarity scores based on the soft biometric, the system enters re-login authentication mode. In the re-login authentication mode, the user must provide valid soft and hard biometrics.

Figure 4: Sample Images

VI. Flowchart of Proposed Approach

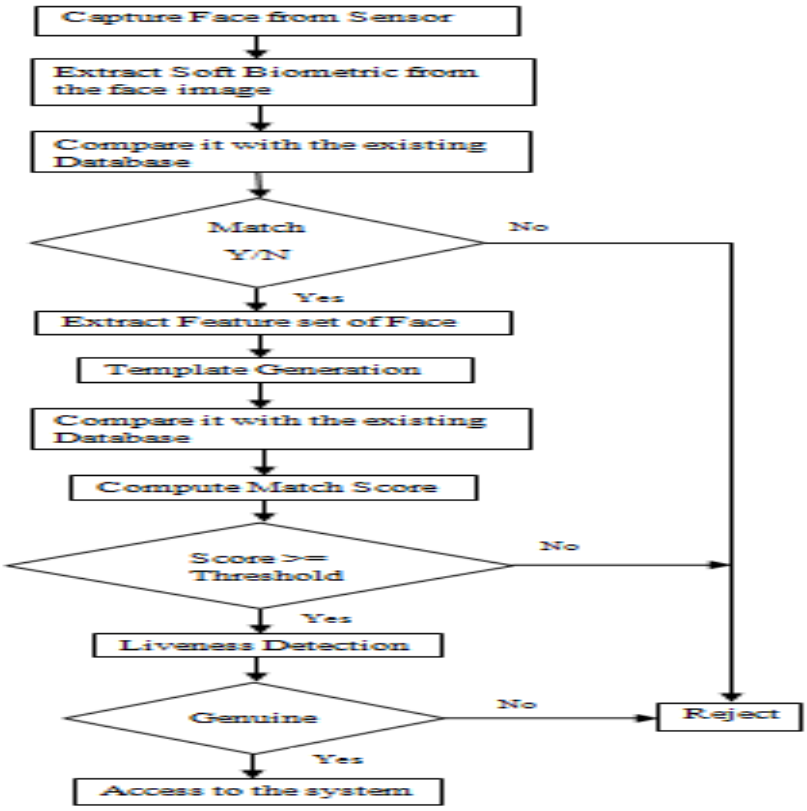

Figure 5: Working Module

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

VII. Proposed Algorithmic Approach

1) Capture Face from Sensor

2) Extract soft biometric from the face image

3) Compare it with the existing database

4) If (soft trait feature matched)

6) Extract feature set of face

6) Generate template of feature set

6) Compare it with the existing database

8) Compute match score

9) If (score >= threshold)

10) Apply Liveness detection technique

11) If (Identified as genuine)

12) Allow access to the system

13) Else

14) Reject user

16) End If

16) Else

16) Reject user

18) End If

19) Else

20) Reject user

VIII. CONCLUSION AND FUTURE WORK

The proposed approach presents a technique for liveness detection which uses the concept of soft biometrics. This technique ensures the detection of fake images and also verifies that the person is a legitimate user or not. But the traditional method does not use the concept of soft biometrics. Therefore, this method performs the liveness detection process even if the data is being presented by an imposter and hence is more time consuming. The main advantage of the proposed scheme is that if the person is found fake then it is detected at the soft biometric test module and the further computations are not performed. Hence, the performance of the system is improved. The new framework integrates hard and soft biometric traits for continuous user authentication.Soft biometrics like face and clothing color are registered every time the user is logged in and continuously authenticate the user based on their hard and soft biometrics.Soft biometrics for continuous authentication offers high usability and, using both soft and hard biometrics (face recognition) for Re-login authentication, leads to higher security. Also, no additional hardware is required for soft biometrics.

In future, the Soft Biometric Traits may be expanded to include more features such as the complexion of the user, eye color or other facial features like facial hair.

REFERENCES

[1] K. Niinumaand A.K. Jain, “Continuous user authentication using temporal information,” in

Proc. SPIE, 2010, vol. 7667, p. 76670L.

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

[2] A. Prakash, "A Biometric Approach for Continuous User Authentication by Fusing Hard and Soft Traits," International Journal of Network Security, Vol.16, No.1, PP.65-70, Jan. 2014.

[3] 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.

[4] 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.

[5] A. Bromme, "A risk analysis approach for biometric authentication technology," International Journal of Network Security, vol. 2, no.1, pp. 52-63, Jan. 2006.

[6]KoichiroNiinuma, UnsangParkand , Anil K. Jain, "Soft Biometric Traits for Continuous User Authentication," IEEE Transactions On Information Forensics And Security, Vol. 5, No. 4, December 2010.

[7] Klosterman AJ, Ganger GR (2000) Secure continuous biometric-enhanced authentication. Carnegie Mellon University, Tech. Rep. CMU-CS-00-134.

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

[9] YannisStylianou, YannisPantazis, Felipe Calderero, Pedro Larroy, Francois Severin, Sascha Schimke, Rolando Bonal, Federico Matta, and AthanasiosValsamakis. "GMM-Based Multimodal Biometric Verification", Enterface'05, MONS, Belgium -Final Project Report, 2005.

[10]Sunil Chawla and AashishOberoi, Robust algorithm for iris segmentation and normalization usinghough transform. Global Journal of Business Management and Information Technology, 1:69–76, 2011.

[11]DzatiAthiarRamli, Salina Abdul Samad, AiniHussain,"A Multibiometric Speaker Authentication System with SVM Audio Reliability Indicator", IAENG International Journal of Computer Science, 36:4, IJCS-3, 2008.

[12]Arun Ross and RohinGovindarajanb, "Feature Level Fusion Using Hand and Face Biometrics", SPIE Conference on Biometric Technology for Human Identification II, Volume, 5779, pp.196-204(Orlando, USA) March 2005.

[13] J.G. Daugman, "High Confidence Visual Recognition of Statistical Independence", IEEE Transactions on Pattern Analysis and Machine Intelligence 2011.

[14] HaryatiJaafar et al."A Review of multibiometric System with Fusion Strategies and Weighting Factor" / International Journal of Computer Science Engineering (IJCSE) ISSN: 2319-7323, vol. 2 No. July 2013.

[15] A. Ross and A. Jain, "Biometric sensor interoperability: A case study in fingerprints," in Proc. of International ECCV Workshop on Biometric Authentication (BioAW), LNCS, pp.

134–145, May 2004.

[16**]** Manvjeetkaur, Mukhwindersingh,AkshayGirdhar, and ParvinderS.Sandhu,'Fingerprint Verification System', International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:2, No:10, 2008

[17**]** Dinesh kumar Mishra, Dr. S.P Tripathi, DipakMisra,"A review of fingerprint image enhancement technique" Volume 2, Issue 2, March – April 2013

[18] Anil Jain, UmutUludag and Arun Ross Biometric Template Selection: A case study in fingerprints, Appeared in Proc. of 4th Int'l Conference on Audio- and Video-Based Person Authentication (AVBPA), LNCS 2688, pp. 335-342, Guildford, UK, June 9-11,2012.

[19] M. S. Ennis, R. K. Rowe, S. P. Corcoran, and K. A. Nixon, "Multispectral sensing for high-performance fingerprint biometric imaging," White Paper, Lumidigm Inc. (Available at http://www.lumidigm.com/lightPrint.html),2012.

[20] ChunxiaoRen, Yilong Yin, Jun Ma, and Gongping Yang, "Feature Selection for Sensor Interoperability: A Case Study in Fingerprint Segmentation", IEEE International Conference on Systems, Man, and Cybernetics San Antonio, TX, USA - October 2009.

[21] Dr.K.Rameshkumar Mrs.U.Latha, "A Study On Attacks And Security Against Fingerprint Template Database," International Journal Of Emerging Trends & Technology In Computer Science (Ijettcs), Vol. 2, No. 5, September 2013.

[22] Michael Kimwele, Stephen Kimani Joseph Mwema, "A Simple Review Of Biometric Template Protection Schemes Used In Preventing Adversary Attacks On Biometric Fingerprint Templates," International Journal Of Computer Trends And Technology (Ijctt), Vol. 20, No. 1, Feb 2015.

[23] Anil K. Jain, Arun Ross, And Umut Uludag, "Biometric Template Security: Challenges And Solutions," In 13the European Signal Processing Conference (Eusipco), Vol. 4, 2005, Pp. 1934-1937.

[24] D. Maio, A. K. Jain, And S. Prabhakar. D. Maltoni,.: Springer-Verlag London, 2003.