ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

Continuous User Authentication Using Soft Biometric Traits for E-Learning

Kalyani Tukaram Bhandwalkar, P.S.Hanwate

ME(I), Computer Engg, G.H.Raisoni College of Engg, Ahmednagar, Maharashtra, India.

Assistant Professor, Computer Engg, G.H.Raisoni College of Engg, Ahmednagar, Maharashtra, India.

Abstract: E-learning institutions are currently facing two key challenges related to identity management. The traditional static authentication at login time whether it is based on a simple password scheme or a strong password is inadequate for two reasons. Firstly, in the current e-learning environments, a student can easily perform the initial authentication (in case of strong authentication such as biometric) or share their password with an expert, and have that expert take an online exam on their behalf without being caught, which is a serious threat to the integrity of the degrees offered by e-learning institutions. Secondly, students can share their accounts with other fellows, who will be able to take online lectures without ever registering, which represent loss in tuition fees for e-learning institutions. To prevent students from e-cheating soft biometric traits are used for continuous user authentication.

Keywords: — Soft Biometric, Continuous User Authentication, Face Recognition

I. Introduction

E-Learning is becoming increasingly popular in higher education because it can alleviate time and space restrictions. E-leaming systems represent a new form of learning and are becoming more and more popular everyday. Hence security in e-Learning has become a fundamental requirement. e-Testing in the form of web based exams is effective for reducing the constraints of regular examinations, as it is possible to take exams at home rather than at a testing center. However, most e-testing systems perform user authentication using only a user name and password which are entered at login, making it easy to cheat. Passwords can be easily shared with the expert, and have that expert take an online exam on their behalf without being caught, which is a serious threat to the integrity of the degrees offered by e-learning institutions.

By continuous verification we mean that the identity of the human operating the computer is continually verified. Verification is computationally simpler than identification and attempts to determine how "close" an observation is to a known value, rather than finding the closest match in a set of known values. 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.

II. Literature survey

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 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. A number of studies on continuous user authentication have been published. These schemes typically use one or more primary (hard) biometric traits (e.g., fingerprint or face). *Sim et al.* and *Kwang et al.* captured the user's face and fingerprint with a camera and a mouse with a built-in fingerprint sensor, respectively. While they showed promising authentication results, their system suffered from low availability of the biometric traits. For example, when a user is typing or entering a document, he often needs to turn his head away from the camera. Face image is not properly captured is when there is change in user posture and he does not look directly at the camera. Similarly, fingerprint can only be authenticated when the user keeps his finger on the reader embedded in the mouse [2].

III. BIOMETRICS

Biometrics is defined as the identification of an individual based on physiological and behavioral characteristics [4]. 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. Some researchers have coined the term behaviometrics to describe the latter class of biometrics. Biometrics is used to refer to the field of technology devoted to identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, or face recognition. Biometrics provides a convenient and low-cost additional tier of security. It eliminates problems caused by shared passwords by using physiological attributes. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.

IV. 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 [5]. These traits include gender, ethnicity, and color of eye/skin/hair, height, weight, and SMT (scars, marks, and tattoos) [5]. 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.

V. PROPOSED SCHEME

To address the security problems, a method for continuous user authentication is proposed that continuously collects soft biometric information. In particular, in this method the colors of user's clothing and face as the soft biometric traits are used. Also use conventional face recognition for relogin authentication.

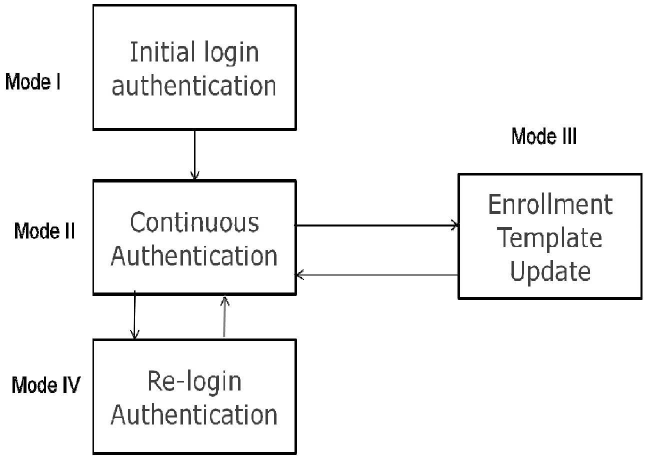
Mode I
Initial login authentication
Mode II
Continuous Authentication
Mode III
Enrollment Template Update
Mode IV
Re-login Authentication

Fig. 1 Proposed System

The method automatically registers the user every time the user logs in by combining the soft biometric traits with the conventional face recognition authentication method [2]. Relogin authentication which handles short absence of the user or incomplete biometric data.

A. Initial Login Authentication (Mode I)

This is the first mode and consists of the following four main steps.
Initial authentication: Biometric face recognition authentication method can be used.
Face detection: A user is typically looking in the frontal direction during the login session. This is a reasonable assumption because the user typically looks at the monitor at the login time as the user wants to be authenticated.
Body localization: Location and size of the user's body with respect to his face are estimated.
Template enrollment: Histogram of the face colour (soft face), histogram of the clothing colour, and the eigenface representation of the face (hard face) are computed and stored as enrollment templates.

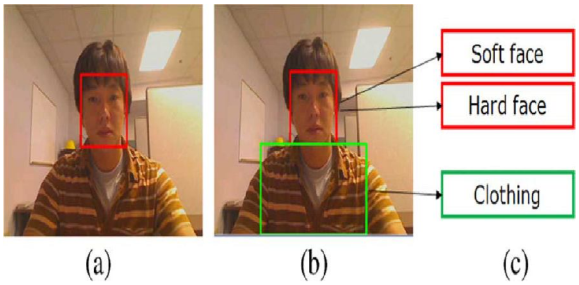

Fig. 2 Initial Enrollment Mode: (a) Face Detection,(b)Body Localization;(c) Registration

B. Continuous Authentication (Mode II)

Continuous authentication starts after mode I. The system continuously authenticates the user by using the "soft face" and "clothing" enrollment templates registered in Mode I (initial login authentication). Any time the system recognizes that the user is no longer present in front of the console, the system status changes to Mode III (enrollment template update). The system tracks the face and the body separately based on the histograms registered in Mode I. Face recognition is executed at regular intervals (1 second). Hard face recognition is not directly used in continuous authentication but it is stored for use in relogin authentication [2]. If similarity is below a threshold, the system enters Mode III to check whether it is due to the change in the ambient illumination or user's absence in front of the console.

C. Enrollment Template Update(Mode III)

The system status enters Mode III whenever the similarity falls below threshold. This mode is introduced to reduce the false rejects caused by illumination changes. This process consists of two steps.
Illumination change detection: When similarity is lower than threshold in Mode II, the system checks whether:

- User is no longer in front of the console or
- There has been a change in the ambient illumination.

The well-known and simple method of image subtraction to detect the illumination change. A pair of images, one just before and one immediately after the time when Similarity ≤ threshold is used for image subtraction; the number of pixels that show a large difference in brightness between the two images is counted. If the difference image shows intensity differences all over the image, it is decided that there has been an illumination change.

2. Enrollment template update: When an illumination change is detected, the user's biometric template is updated to maintain successful continuous authentication in the modified operating environment.

D. Relogin Authentication (Mode IV)

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 reauthenticate him automatically. If the system detects a user and reauthenticates the user as genuine, the status moves to Mode II again. The relogin authentication mode consists use the same procedures as used in section III. Here, the user is authenticated using both soft (colour histograms) and hard biometrics (face). The similarity score is used for relogin authentication. Fig. 1 shows flowchart of the proposed algorithm.

The fig. 3 shows successful detection of unauthorized user who replaced the authenticated student during e-test. The colour ellipses in fig.3 (a) and (e) indicate that the system correctly recognized the valid user in front of the console, while black-and-white images in Fig. 3(b), (c), and (d) indicate that the system correctly recognized the absence of the valid user in front of the console.

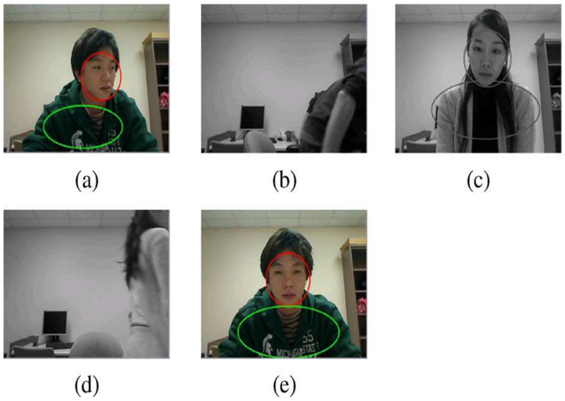

Fig. 3 Example showing detection of e cheating (a)Authenticated Student; (b) Authenticated Student walked away; (c) Unauthenticated person is detected;(d) Unauthenticated user walked away;(e) Authenticated user returns.

There will be a small discontinuity in the values of soft biometrics when the unauthenticated person tries to replace the student. When there is a discontinuity in the similarity scores based on the soft biometric, the system enters relogin authentication mode. In the relogin authentication mode, the user must provide valid soft and hard biometrics. Person replacing the student may be wearing similar clothes and face colour, but it is highly unlikely that he will have similar hard biometric traits. Therefore, the relogin authentication is the method of successfully identify e cheating .

VI. CONCLUSION

The main purpose of this paper is to present a new e-learning model used for identification, authentication and tracking the student. The system is robust with respect to user's posture in front of the workstation. Soft biometrics for continuous authentication offers high usability and, using both soft and hard biometrics (face recognition) for relogin authentication, leads to higher security. Also no additional hardware required for soft biometric.

REFERENCES

[1] 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*

[2] Koichiro Niinuma, Unsang Parkand , Anil K. Jain, "Soft Biometric Traits for Continuous User Authentication," *IEEE Transactions On Information Forensics And Security, Vol. 5, No. 4, December 2010*

[3] Mohsen Khademi Dehnavi, Sayed Mehran Sharafi, Naser Nematbakhsh," Developing A E-Learning Model For Tracking The Continuous Attendance Of The Students" *Journal of Theoretical and Applied Information Technology 2005-2011 JATIT & LLS*

[4] Qinghai Gao,"Online teaching: Do you know who is taking the final exam?", *Fall 2010 Mid-Atlantic ASEE Conference, October 15-16, 2010, Villanova University*

[5] Anil K. Jain, Sarat C. Dass and Karthik Nandakumar," Can soft biometric traits assist user recognition" *Proceedings of SPIE Vol. 5404, pp. 561-572, 2004*

[6] A. Dantcheva, C. Velardo, A. D'Angelo, and J.-L. Dugelay." Bag of soft biometrics for person identification: New trends and challenges." *Multimedia Tools and Applications, 51(2):739–777,2011.*

[7] Sandeep Kumar ,Terence Sim, Rajkumar Janakiraman, Sheng Zhang, "Using Continuous Biometric Verification to Protect Interactive Login Sessions "

[8] http://en.wikipedia.org/wiki/Biometrics

[9] http://en.wikipedia.org/wiki/Soft_biometrics