ISSN : 2494-9150 Vol-01, Issue 12, Mar 2016.

Continuous User Authentication using Soft Biometric Peculiarity

[1]Ankita Shinde, [2]Roshni Singh
[1,2]Smt. Indira Gandhi College of Engineering, Mumbai, Maharashtra, India.
[1]ankitashindeas.11@gmail.com, [2]roshni1893@gmail.com

Abstract- In the existing computer systems, user authentication is done only in the initial stage of login process which can prove to be a critical security issue. In such scenario an imposter can access the important resources of the user if the user has not logged out. This situation mostly occurs when the user forgets to log out or take a short break without logging out. To solve this problem we propose a continuous authentication scheme that continuously monitors and authenticate the logged in user. The previous methods of continues authentication uses only hard biometric traits (face, fingerprint, etc.) for authentication purpose. However the use of these peculiarities is not only inconvenient to user but is also not feasible due to changing user posture. To overcome this problem we propose a new method of continuous user authentication which uses combination of hard and soft biometric traits (e.g. face color, clothes color). The proposed framework automatically registers soft biometric qualities every time the user logs in and fuses soft biometric matching with the conventional authentication schemes, namely password and face biometric.

***Keywords — Biometrics recognition, continuous user authentication, face recognition, fusion, soft 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. Similarly, smart cards can be shared, stolen, duplicated, or lost. 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. But all of the above login methods have a common problem that is they have one-time authentication process. They authenticate a user only at the initial log-in session and do not re-authenticate a user until the user logs out or there is a substantial time interval between user's activities on the workstation. This could pose a critical security weakness since any intruder can access the users system when user leaves the system for some time or does not properly log out.

To solve the above problems, we propose a new method for continuous user authentication that continuously collects soft biometric information. We use the colors of user's clothing and face as the soft biometric traits. In addition, we also use PCA-based face features for conventional face recognition for re-login authentication. Also we use concept of histogram matching for eliminating the clustered background. We automatically register the user every time the user logs in by combining the soft biometric traits with face recognition authentication method. This helps us to authenticate the user continuously and re-authenticate when the system logs out after failing to detect the user.

II. LITERATURE SURVEY

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

Biometrics is the science of automatically recognizing people based on physical or behavioral 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.

III. SCOPE OF THE PROJECT

This type of continuous authentication method is used to authenticate the users during the login process into military applications, banking accounts, personal computers, high security dataset,etc.

IV. MODULES

The system is being divided into following 4 modules:

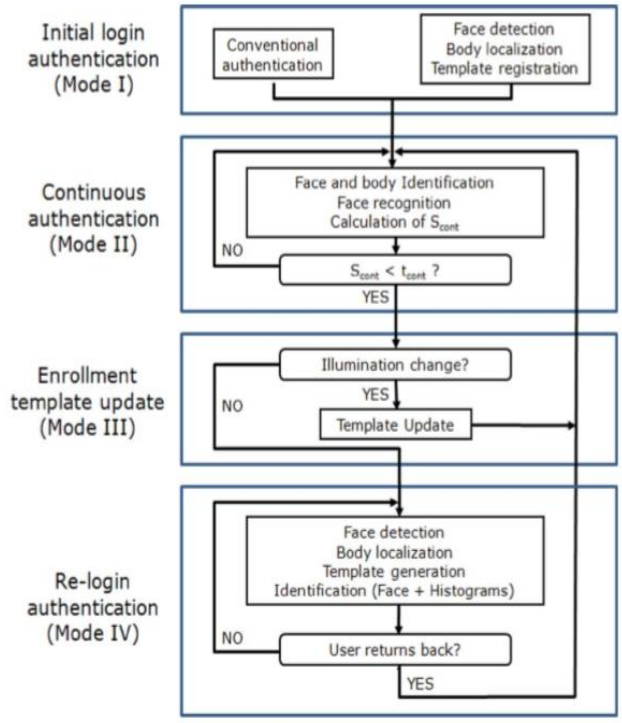

Fig .01 – Modes of proposed system

A. Initial Login Authentication (Mode I)

This is the first mode and consists of the following four main steps.

1) Initial authentication: A password-based authentication has been currently used in our system. However, any authentication method mentioned earlier can be used.
2) Face detection: Haar classifier is used for face detection. We assume that 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 to type in the login password and the user wants to be authenticated.
3) Body localization: Location and size of the user's body with respect to his face are estimated.
4) Template enrolment: Images of the face (Hard face) and of the clothing in both colour and grey format are computed and stored as enrolment templates in an array.

(a) (b)

Fig: 02– Initial enrolment mode. (a) Face detection, (b) body localization, and (c) registration.

B. Continuous Authentication (Mode II)

Continuous authentication starts after mode I. The system registers the histograms of face and colour from the images saved in mode I. The system continuously authenticates the user by using the "soft face" and "clothing" enrolment templates registered. 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). The continuous authentication mode consists of the following three steps:

1) Face and body identification using colour histograms: the system tracks the face and the body separately based on the histograms registered in Mode I.
2) Face recognition: A PCA-based face recognition technique (Eigen face) is used in our system to extract facial features.
3) Cloth recognition: After detecting the face, cloth is recognized.

Fig: 03 –Examples of user's posture. The two rectangles in each image denote the facial and clothing regions used to compute the colour histograms.

C. Enrolment Template Update (Mode III)

The system status enters Mode III. This mode is introduced to reduce the false rejects caused by illumination changes. This process consists of two steps:

1) Illumination change detection: The system checks whether:
   i) user is no longer in front of the console or
   ii) there has been a change in the ambient illumination. We use 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 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) Enrolment template update: when an illumination change is detected, we update the user's biometric template to maintain successful continuous authentication in the modified operating environment.

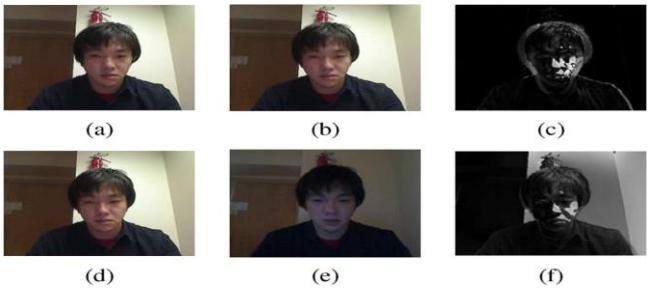

Fig: 04-Example results of re-login authentication experiments. (a) Authentic user; (b) authentic user walks away; (c) imposter user; (d) imposter user walks away; and (e) authentic user returns.

D. Re-login 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 re-authenticate him automatically. If the system detects a user and re-authenticates the user as genuine, the status moves to Mode II again. The re-login authentication mode consists of four steps. Steps 1), 2), and 3) use the same procedures as used in steps 2), 3), and 4) in Section IV-A. In step 4), the user is authenticated using both soft (colour histograms) and hard biometrics (face).

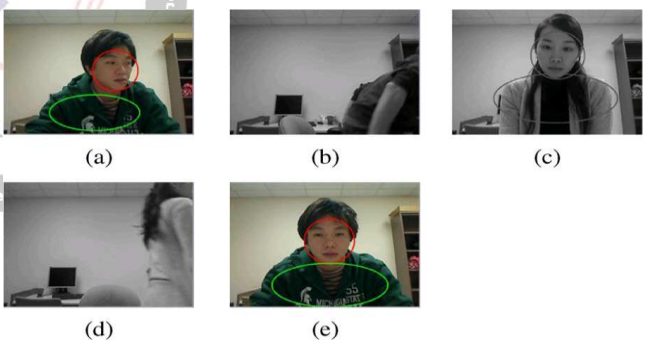

Fig: 06-Example results of re-login authentication experiments. (a) Authentic user; (b) authentic user walks away; (c) imposter user; (d) imposter user walks away; and (e) authentic user returns.

Fig. 07 shows the detailed flowchart of the proposed algorithm. We address the "session hijacking1" problem by using both the soft and hard biometrics. There will be a small discontinuity in the values of soft biometrics when the imposter tries to replace the legitimate 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. Imposters may be wearing similar clothes and face colour, but it is highly

V. OVERVIEW OF THE PROPOSED WORK

As said earlier we combine the hard and soft features of user to continuous authenticate it. Our system works for different user postures so it becomes more convenient to user. Also we overcome the problem of background color changes which proves obstacle in continuous authentication phase by using the concept of histogram matching.

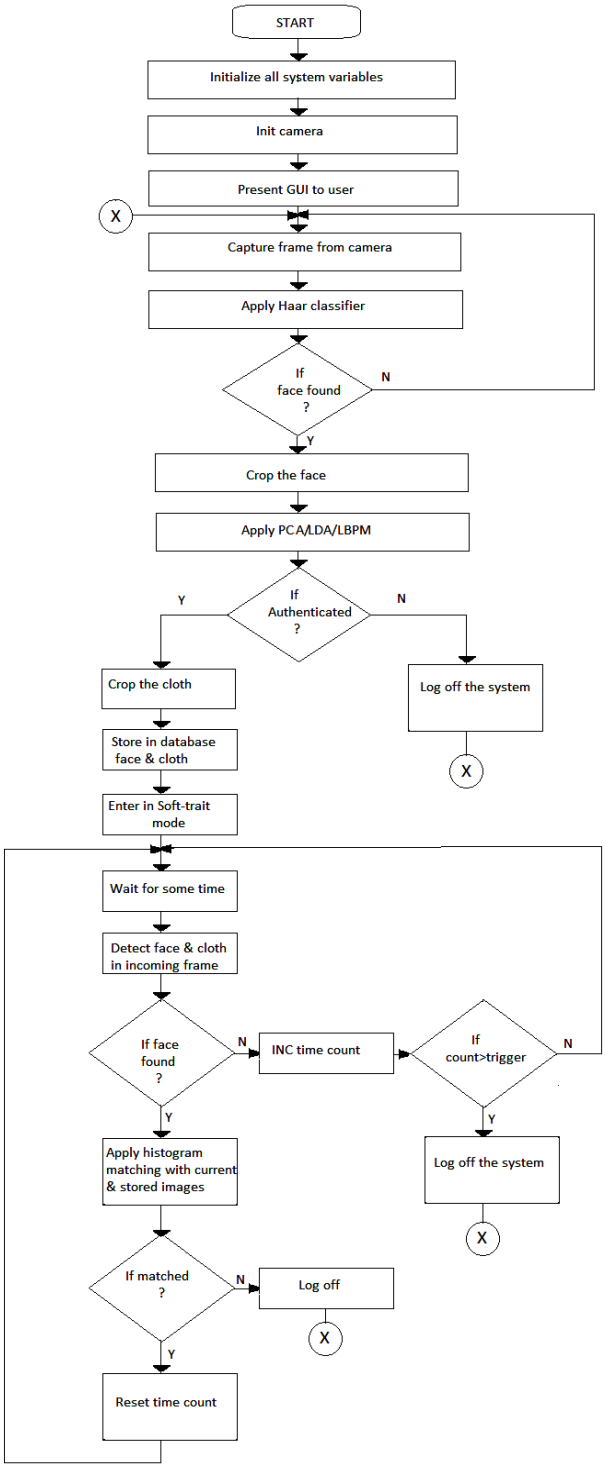

Fig: 07 – Flowchart of proposed system

The proposed model is depicted in fig 01. The overview of the proposed model is as follows:

1. We initialize all the variables of the system.
2. After initializing the camera and presenting the GUI to user, we capture an image and display it on screen.
3. Now the initial log in stage of user starts or he enters the hard biometric mode.
4. We apply Haar classifier so as to detect the face in an image.
5. After the face is detected we need to crop it to remove the background noise.
6. For that we use PCA, LDA or LBPH algorithms.
7. The cropped face and cloth is stored in database. The system now enters into soft biometric mode.
8. When user goes into continuous authentication mode, the time counter starts immediately.
9. If face is found we apply histogram matching for current and stored images.
10. If the match is done then counter is reset, and if not the system logs off.
11. Or else if no face is detected for the specified counter time the system logs off.

The image processing techniques that are used in the proposed system has been explained in the following sections.

A. Haar classifier

Object Detection using Haar feature-based cascade classifiers is an effective object detection method proposed by Paul Viola and Michael Jones in their paper, "Rapid Object Detection uses a Boosted Cascade of Simple Features" in 2001. It is a machine learning based approach where a cascade function is trained from a lot of positive and negative images. It is then used to detect objects in other images. A window of the target size is moved over the input image, and for each subsection of the image the Haar-like feature is calculated. This difference is then compared to a learned threshold that separates non-objects from objects.

ISSN : 2494-9150 Vol-01, Issue 12, Mar 2016.

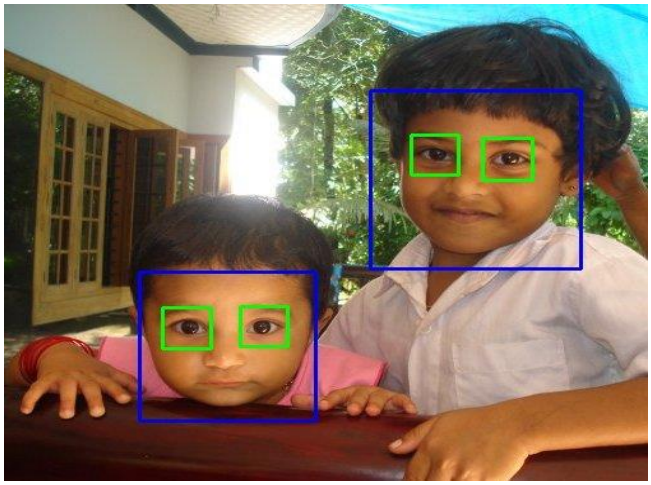

Fig: 08 – Haar Classifier

B. PCA algorithm

After we obtain an image of face of user, we crop it. And accordingly we crop the cloth part.

Now in recognition process we need to train the Eigen engine. Principal Component Analysis (PCA) is then used which is a statistical procedure that extracts the most important features of a dataset.

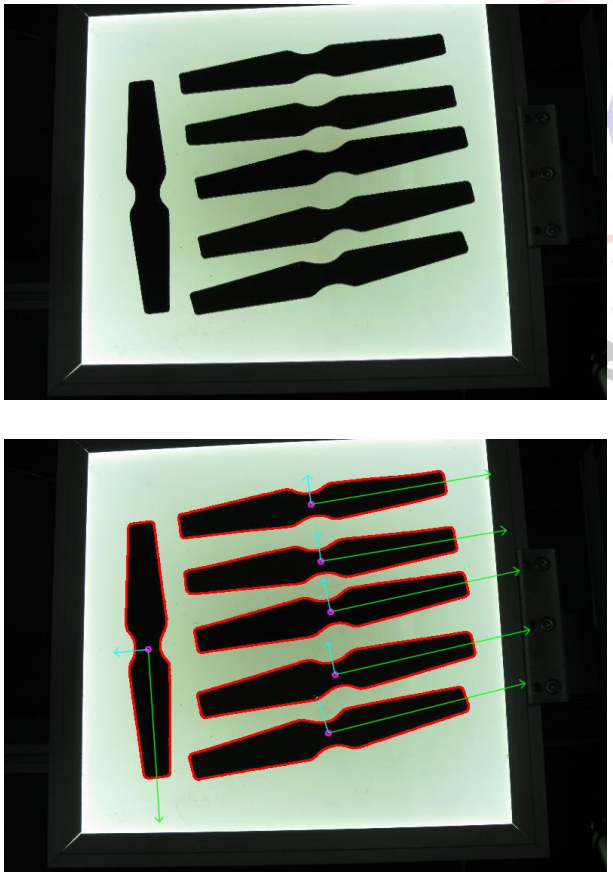

Fig: 09 – PCA test results

C. Histogram Matching

It loads a *base image* and 2 *test images* to be compared with it. Convert the images to HSV format. Calculate the H-S histogram for all the images and normalize them in order to compare them. Compare the histogram of the *base image* with respect to the 2 test histograms, the histogram of the lower half base image and with the same base image histogram. Finally it display the numerical matching parameters obtained.

VI. CONCLUSION

We have proposed a new framework that uses soft biometric traits for continuous user authentication. This framework registers a new enrolment template every time the user logs in, which enables the system to effectively use soft biometric traits for continuous authentication; the proposed system uses face color information as well as clothing color (soft biometric) to continuously authenticate the user. The user has to register just once before using the system. Because it would be inconvenient for the user to meet the requirement of entering a password or provide his fingerprint whenever he takes a break to read a book or consult notes. Hence, the system reduces the user's task and increase usability. The system is robust with respect to user's posture in front of the workstation and it also has the capability for enrolment template update and re-login authentication. 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. The use of the soft biometric also circumvents the situation when the availability of hard biometric traits is limited due, for example, to user inactivity. Experimental results demonstrate that the system is able to successfully authenticate the user continuously with tolerance to the user's posture. Also the authentication system uses only the standard devices (e.g. keyboard, mouse, and Web camera) and avoids the use of special devices. Hence, system can be implemented with commercial off-the-shelf (COTS) devices only which are a very important factor in a low-security environment.

REFERENCES

[1] K. Niinumaand A.K. Jain, "Continuous user authentication using temporal information," in Proc. SPIE, 2010, vol. 7667, p. 76670L.

[2] 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.

[3] 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.

[4] Vance, "If your password is 123456, just make it Hack Me," The New York Times [Online]. Available: http://www.nytimes.com/2010/01/21/ technology/21password.html

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

[6] A.K. Jain, P. Flynn, and A. A. Ross, Eds., Hand book of Biometrics. New York: Springer, 2007.

[7] F. Monrose and A. D. Rubin, "Keystroke dynamics as biometrics for authentication," *Future Generation Comput. Syst.*, vol. 16, pp. 351–359, 2000.

[8] Altinok and M. Turk, "Temporal integration for continuous multimodal biometrics," in *Proc. Workshop on Multimodal User Authentication*, 2003, pp. 131–137.

[9] 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.

[10] Azzini, S. Marrara, R. Sassi, and F. Scotti, "A fuzzy approach to multimodal biometric continuous authentication," *Fuzzy Optimal Decision Making*, vol. 7, pp. 243–256, 2008.

