Soft Biometric Traits for Continuous User Authentication

Koichiro Niinuma, Unsang Park, *Member, IEEE*, and Anil K. Jain, *Fellow, IEEE*

***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. To address this security flaw, we propose a continuous authentication scheme that continuously monitors and authenticates the logged in user. Previous methods for continuous authentication primarily used hard biometric traits, specifically fingerprint and face to continuously authenticate the initial logged in user. However, the use of these biometric traits is not only inconvenient to the user, but is also not always feasible due to the user's posture in front of the sensor. To mitigate this problem, we propose a new framework for continuous user authentication that primarily uses soft biometric traits (e.g., color of user's clothing and facial skin). The proposed framework automatically registers (enrolls) soft biometric traits every time the user logs in and fuses soft biometric matching with the conventional authentication schemes, namely password and face biometric. The proposed scheme has high tolerance to the user's posture in front of the computer system. Experimental results show the effectiveness of the proposed method for continuous user authentication.**

***Index Terms*—Biometrics recognition, color histogram, 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 [2], [3]. In addition, most users prefer to use very simple passwords (e.g., their first name, "123456," or "password") and use the same password across different applications [4]. This is because complex passwords are difficult to remember, even though they are more secure. Similarly, smart cards can be shared, stolen, duplicated, or lost. To circumvent these issues, a number of login authentication methods, including textual and graphical passwords [5], public key infrastructure (PKI), and biometric authentication [6], 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 or there is a substantial time interval between user's activities on the workstation. This could pose a critical security weakness not only for high-security systems, but also for personal computers in a general office environment. 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. 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. We believe that biometric traits [6] that 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 [7]–[14]. These schemes typically use one or more primary (hard) biometric traits (e.g., fingerprint or face). Sim *et al.* [9] and Kwang *et al.* [15] 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, she often needs to turn her head away from the camera. Another situation where face image is not properly captured is when the user takes a break from typing to read paper documents and 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.

To address the above problems, we propose a new method for continuous user authentication that continuously collects soft biometric information. In particular, we use the colors of user's clothing and face as the soft biometric traits. In addition, we

Manuscript received February 23, 2010; revised September 01, 2010; accepted September 02, 2010. Date of publication September 13, 2010; date of current version November 17, 2010. An earlier version of this work appeared in the *Proc. SPIE*, vol. 7667, p. 76670L, 2010. The work of A. K. Jain was supported in part by the World Class University (WCU) program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (R31-2008-000-10008-0). The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Davide Maltoni.

K. Niinuma is with Fujitsu Laboratories Ltd., Kawasaki 211-8588, Japan (e-mail: niinuma.k@jp.fujitsu.com).

U. Park and A. K. Jain are with the Computer Science and Engineering Department, Michigan State University, East Lansing, MI 48824 USA (e-mail: parkunsa@cse.msu.edu; jain@cse.msu.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2010.2075927

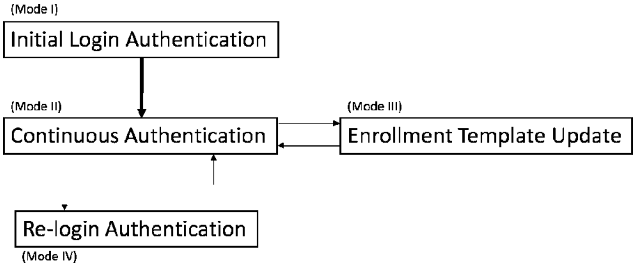

(Mode I)
Initial Login Authentication
(Mode II)
Continuous Authentication
(Mode III)
Enrollment Template Update
Re-login Authentication
(Mode IV)

Fig. 1. Proposed framework for continuous user authentication. At the initial login time (Mode I), any authentication scheme can be used.

TABLE I
SUMMARY OF DIFFERENCES BETWEEN THE CONTINUOUS AUTHENTICATION SYSTEMS USING HARD AND SOFT BIOMETRICS. Ω_{intra} AND Ω_{inter} REPRESENT THE INTRACLASS AND INTERCLASS MATCHING SCORE DISTRIBUTIONS, RESPECTIVELY

	Hard biometrics	Soft biometrics
Confidence of decision with each observation	High to medium	Medium to low
Frequency of observation	Medium to low	High
Pre-registration	Required	Not required
Ω_{intra} and Ω_{inter}	Available	Not available

also use PCA-based face features for conventional face recognition for relogin authentication. To the best of our knowledge, the proposed method is the first to use soft biometric traits for continuous authentication. Use of soft biometrics in a continuous authentication system has the following advantages: 1) user can be authenticated continuously even when either no hard biometric data or incomplete hard biometric data are available and 2) no preregistration of the soft biometric traits is required; the soft biometric traits are automatically enrolled every time the user logs in. Our method automatically registers the user every time the user logs in by combining the soft biometric traits with the conventional password or face recognition authentication method. We also extend published continuous authentication methods [9], [15] by addressing the issues concerning 1) relogin authentication which handles short absence of the user or incomplete biometric data capture of the user due to occlusion and 2) template update. Fig. 1 shows the block diagram of the proposed continuous user authentication system. The arrow from Mode I to Mode II represents process flow and all other arrows represent possible transitions when appropriate conditions are met.

The rest of this paper is organized as follows: Section II describes the overall approach, Section III introduces the proposed framework, Section IV presents the experimental results and discussion, and Section V provides conclusions and future work.

II. 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" [16]. These traits include gender, ethnicity, 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.) [16], [17]. 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.

Sim *et al.* [9] 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. Sim *et al.* proposed a system based on the genuine and imposter matching score densities of face and fingerprint, Ω_{intra} and Ω_{inter}. The decision criterion for a user being genuine or equivalently a system being safe is $P(x_t = \text{safe}|Z_t) > P(x_t = \text{compromised}|Z_t)$, where $Z_t = \{z_0, \ldots, z_t\}$ denotes the set of biometric observations until time t and x_t denotes the system state (safe or compromised) at time t. Sim *et al.* introduced a decaying function $p = e^{k\Delta t}$ to control the influence of a biometric trait, where k $(k < 0)$ is a constant governing the decaying speed and t is the elapsed time since the last observation. Some of the drawbacks of this system are: 1) Intraclass and interclass score distributions (Ω_{intra} and Ω_{inter}) of both face and fingerprint biometrics are required. 2) A decaying function is needed because continuous stream of hard biometric traits may not always be available. While the decaying function indeed enables continuous authentication, it comes at the expense of sacrificing the system security. While the authentication decisions can be made to accept the user based on the decaying function p, the system may already have been compromised. 3) The assumption $P(x_0 = \text{safe}|Z_0) = 1$ (i.e., user is genuine at the login time) is not valid. By using hard biometric traits, the user's identity can be verified, but it is indeed possible that the initial state is not safe $(P(x_0 = \text{safe}|Z_0) = 0)$ in case an attacker tries to login with a stolen password. Using soft biometrics, we achieve the following advantages over continuous authentication systems that only rely on hard biometrics: 1) Ω_{intra} and Ω_{inter} are neither available nor required. 2) The role of the decaying function p is diminished because soft biometric traits enable richer observations (Z_t). 3) The condition $P(x_0 = \text{safe}|Z_0) = 1$ is now true since soft biometric template enrollment occurs at each login time. This does not necessarily mean that soft biometrics provide higher security (i.e., a stolen password can still be used) at the login time. However, our problem formulation starts with correct assumptions. Table I summarizes the differences between continuous authentication systems using hard and soft biometrics.

Our system also meets the three criteria for continuous authentication introduced by Sim *et al.*: 1) We used reliability factor of the different modalities. 2) We use time decaying function in relogin authentication mode to make older observations increasingly uncertain. 3) Our system can determine authentication certainty at any point of time. In continuous authentication, the soft biometric is always available. When the soft biometric is not available, system enters relogin authentication mode where a combination of time decay function and hard and soft biometrics is used. The third criterion is more critical for the hard-biometric-based continuous authentication system (CAS) because the hard biometric trait is often unavailable. It is not as important in our system due to the high availability of soft biometric traits.

Even though we can obtain Ω_{intra} and Ω_{inter} by running continuous authentication sessions with a number of subjects, we did not use Ω_{intra} and Ω_{inter} in our system design to make the system more flexible since no preregistration is required. Instead, we make the authentication decision based on the similarity scores. We use the color histogram of user's clothing (on the upper part of the body visible to the webcam) and face color as soft biometrics and the PCA-based face features [18] as a hard biometric for relogin authentication. Let z_t^{sf}, z_t^{hf}, and z_t^{c} denote the set of observations of soft-face, hard-face, and clothing color, respectively, at time t and z_0 be the observation at the login time. The similarity scores for the three types of biometric information are calculated by comparing z_t and z_0 as

$$S_{\text{softface}} = s\left(z_t^{\text{sf}}, z_0^{\text{sf}}\right) \tag{1}$$

$$S_{\text{hardface}} = s\left(z_t^{\text{hf}}, z_0^{\text{hf}}\right) \tag{2}$$

and

$$S_{\text{clothes}} = s\left(z_t^{c}, z_0^{c}\right) \tag{3}$$

where $s(.,.)$ denotes the similarity score based on the Bhattacharyya coefficient [19]. The hard face feature f_{hardface} is a set of Eigen vectors $(\text{length} = l_{\text{eig}})$ with each Eigen vector of length l_{hardface}. The features of soft face and clothes, f_{softface} and f_{clothes}, are the three-dimensional color histograms of red, green, and blue channels with each dimension of length l_{soft}. Therefore, the dimensions of feature vectors of f_{hardface} are $l_{\text{eig}} \times l_{\text{hardface}}$ and those of both f_{softface} and f_{clothes} are $l_{\text{soft}} \times l_{\text{soft}} \times l_{\text{soft}}$. All feature values are transformed to a one-dimensional vector to calculate the similarity using the Bhattacharyya coefficient. The Bhattacharyya coefficient between two feature vectors a and b of length D_1 is given as $\sum_{i=1}^{D_1} \sqrt{a_i b_i}$. The total soft biometric score S_{cont} is calculated as the weighted sum

$$S_{\text{cont}} = wS_{\text{softface}} + (1-w)S_{\text{clothes}} \tag{4}$$

where w is the weighting factor in combining soft biometric traits of face and clothing. Now, the decision criterion for a user being genuine is simply $S_{\text{cont}} \geq t_{\text{cont}}$, where t_{cont} is a threshold value. Using only the soft biometric in the continuous authentication mode is the main idea of the proposed method. If we use the hard biometric in the continuous authentication mode, we will experience the same problem as faced by Sim *et al.*, namely the hard biometric trait is often unavailable. We do not try to identify each subject at every single instance, but continuously monitor the user to determine whether he is the same person who initially logged in. The similarity score of the hard face biometric S_{hardface} is only used in the relogin authentication stage as

$$S_{\text{relogin}} = F(T_{\text{cur}} - T_{\text{reject}})S_{\text{cont}} \tag{5}$$

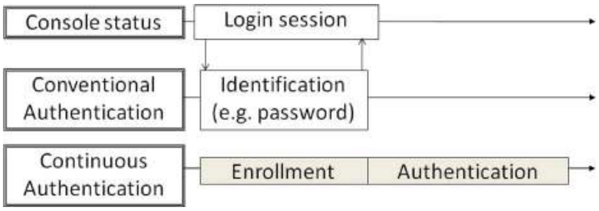

Console status
Login session
Conventional Authentication
Identification (e.g. password)
Continuous Authentication
Enrollment
Authentication

Fig. 2. Schematic showing the difference between conventional and continuous authentication systems.

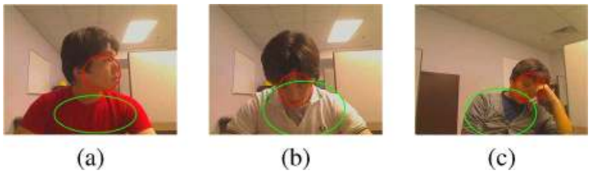

(a) (b) (c)

Fig. 3. Examples of user's posture. The two ellipses in each image denote the facial and clothing regions used to compute the color histograms.

where $F(\Delta t) = e^{k\Delta t}$ denotes a time decaying function with k deciding the decay rate $(k < 0), T_{\text{cur}}$ denotes the current time when S_{hardface} is above a threshold, t_{hardface}, and T_{reject} denotes the time when a user was rejected in the continuous authentication mode. We consider both hard and soft biometric traits in S_{relogin} to make the relogin process more secure. If $T_{\text{cur}} - T_{\text{reject}}$ is large, S_{relogin} becomes small. This will make the system enter the initial login authentication mode (mode I). On the other hand, if the user is absent for only a short time, it is more likely that he will be accepted given valid soft and hard biometric traits. In the continuous authentication mode, S_{cont} is used as the criterion to accept the user instead of S_{relogin}, where T_{reject} or T_{cur} is not considered. Therefore, the following three conditions must be satisfied for relogin authentication:

$$S_{\text{hardface}} \geq t_{\text{hardface}} \tag{6}$$

$$T_{\text{cur}} - T_{\text{reject}} \leq t_{\text{delay}} \tag{7}$$

and

$$S_{\text{relogin}} \geq t_{\text{relogin}} \tag{8}$$

where t_{delay} and t_{relogin} are threshold values. The necessary conditions for relogin are 1) S_{hardface} is large [unlike continuous authentication mode, relogin requires the use of hard biometric (6)], 2) the time when the user was last rejected is not too long (7), and 3) final relogin score that is the combination of the hard and soft biometric should be large (8). Equation (5) incorporates all the conditions in (6)–(8). Fig. 2 shows a comparison of conventional and continuous authentication systems. During the login session, the user inputs his identifying information (e.g., password or hard biometric information) to login to the system. Then, the system registers soft biometric traits, such as color of user's clothing, as a "one-time" enrollment template during the login session, and finally, the system identifies the user continuously using the enrolled soft biometric template.

Fig. 3 shows example images of user's posture, where the system cannot automatically and reliably capture any hard biometric information (e.g., hard facial biometric information). As a result, a continuous authentication system using only hard biometric traits cannot identify the user in such cases. However, some of the soft biometric traits (e.g., clothing and facial color histogram marked as red and green ellipses in Fig. 3) can be continuously observed and used for authentication. We will explain

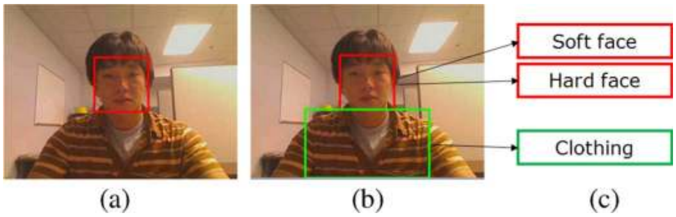


Fig. 4. Initial enrollment mode. (a) Face detection, (b) body localization, and (c) registration.

the four different modes (Fig. 1) in the proposed continuous authentication system in the following sections.

III. Continuous Authentication System

We propose a versatile framework combining continuous authentication with conventional authentication. Our framework registers a new enrollment template (color histogram of a user's clothing and face) every time the user logs in through a conventional login authentication process. Then, the soft biometric traits are used for identifying the user in the continuous authentication mode. The enrollment templates are used not only for continuous authentication, but also for relogin authentication. Hard biometric trait (i.e., face) is used in addition to the soft biometrics for relogin authentication to achieve both high usability and security. The proposed framework consists of four modes as described in Fig. 1.

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 is currently used in our system. However, any authentication method mentioned earlier can be used. 2) Face detection: Haar classifier [20], [21] 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 based on the method of Jaffre and Joly [22]. 4) Template enrollment: Histogram of the face color (soft face), histogram of the clothing color, and the Eigenface representation [18] of the face (hard face) are computed and stored as enrollment templates. We quantize the RGB color space into $16 \times 16 \times 16$ bins in order to generate the color histograms of face and clothing. Top 100 Eigenfaces are used to construct the template of hard face. Fig. 4(a), (b), and (c) depict the intermediate processes of steps 2), 3), and 4), respectively.

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 continuous authentication mode consists of the following three steps.

1) Face and body identification using color histograms: the system tracks the face and the body separately based on the histograms registered in Mode I by applying the mean shift algorithm [23], [24] and calculating the similarities S_{softface} and S_{clothes} separately. The Bhattacharyya coefficient [19] is used for calculating the similarity between two histograms. 2) Face recognition: A PCA-based face recognition technique (Eigenface) [18] is used in our system to extract facial features. Face recognition is executed at regular intervals (1 second). S_{hardface} is not directly used in continuous authentication but it is stored for use in relogin authentication. 3) Computing the final similarity: the system calculates the final similarity S_{cont} defined in (4). If S_{cont} is below a threshold (t_{cont}), 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.

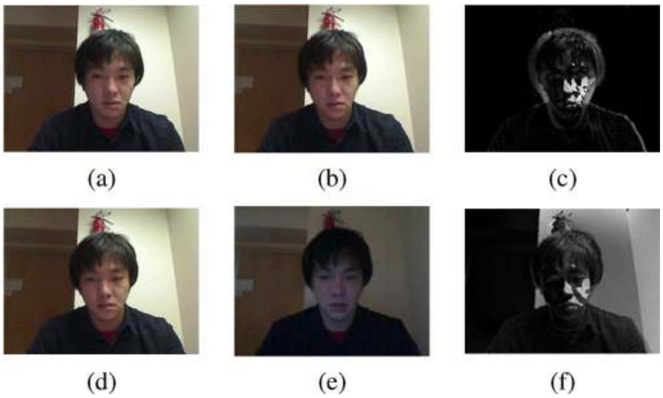


Fig. 5. Example of image subtraction for illumination change detection. The difference image in (f) shows an illumination change between (d) and (e), but the difference image in (c) does not show change in illumination between (a) and (b).

C. *Enrollment Template Update (Mode III)*

The system status enters Mode III whenever the similarity S_{cont} falls below t_{cont}. This mode is introduced to reduce the false rejects caused by illumination changes. This process consists of two steps.

1) Illumination change detection: when S_{cont} is lower than t_{cont} in Mode II, 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 when $S_{\mathrm{cont}} \leq t_{\mathrm{cont}}$ 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. Fig. 5 shows two image subtractions results; there is an illumination change between Fig. 5(d) and (e), but no change between Fig. 5(a) and (b). 2) Enrollment template update: when an illumination change is detected, we update the user's biometric template [z_0 in (1)–(3)] 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

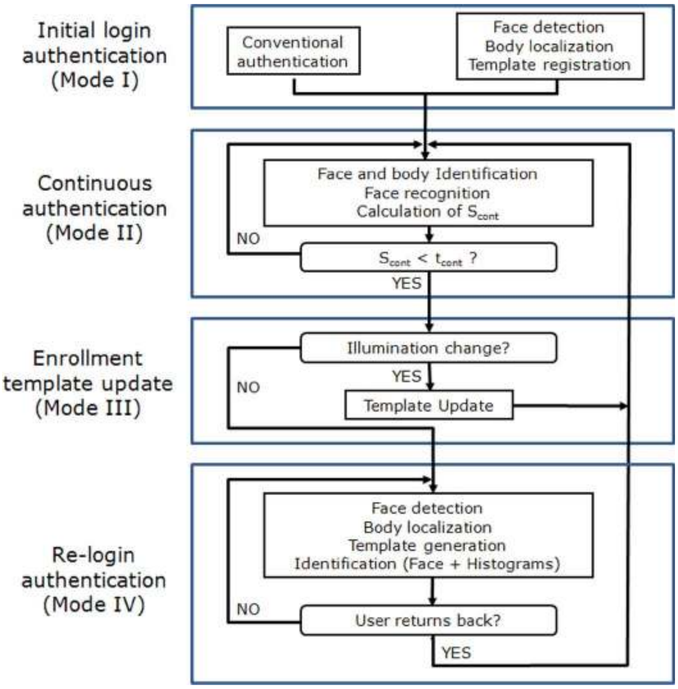

Initial login authentication (Mode I)
Conventional authentication
Face detection
Body localization
Template registration
Continuous authentication (Mode II)
Face and body Identification
Face recognition
Calculation of S_{cont}
NO
$S_{cont} < t_{cont}$?
YES
Enrollment template update (Mode III)
Illumination change?
YES
NO
Template Update
Re-login authentication (Mode IV)
Face detection
Body localization
Template generation
Identification (Face + Histograms)
NO
User returns back?
YES

Fig. 6. Flowchart of the proposed algorithm.

reauthenticates the user as genuine, the status moves to Mode II again. The relogin 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 III-A. In step 4), the user is authenticated using both soft (color histograms) and hard biometrics (face). The similarity score, S_{relogin}, shown in (5) is used for relogin authentication.

Fig. 6 shows the detailed flowchart of the proposed algorithm. We address the "session hijacking[1]" 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 relogin authentication mode. In the relogin authentication mode, the user must provide valid soft and hard biometrics. Imposters may be wearing similar clothes and face color, but it is highly unlikely that he will have similar hard biometric traits. Therefore, the relogin authentication is the method of deterring session hijacking in our system.

IV. Experimental Results

A. System Configuration

Fig. 7 shows the system setup used in our experiments, which consists of a laptop and a webcam. The system has the following characteristics that are conducive, especially for PC or laptop users

- Real-time continuous user authentication capability.
- Robustness to changes in user's posture.
- No requirement for user to preregister.

Fig. 7. Continuous authentication system setup: laptop with a webcam.

- No requirement for a specific background (robust to cluttered background).

B. Database

We have collected videos of 20 subjects using the system shown in Fig. 7 to evaluate the proposed continuous authentication scheme. Each user was asked to perform the following set of actions while seated in front of the webcam.

- Scenario A: turning head to the left;
- Scenario B: turning head to the right;
- Scenario C: turning head down;
- Scenario D: lean back in chair;
- Scenario E: stretch arms;
- Scenario F: walk away.

The duration of videos ranges from 54 to 143 s with a frame rate of 15 frames/s and frame size of 640 × 480 pixels. Fig. 8 shows some example screen shots of the videos with red and green ellipses indicating the face and body regions automatically detected by the system.

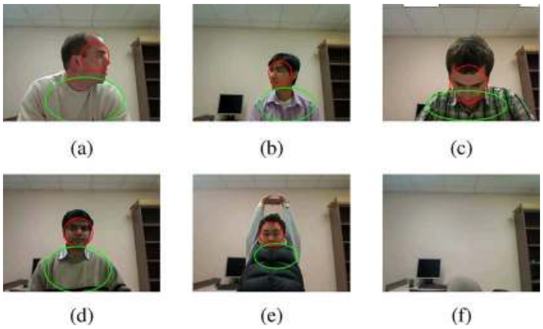
C. Performance Evaluation

Sim *et al.* [9] proposed a number of performance metrics such as Time to Correct Reject (TCR), Probability of Time to Correct Reject (PTCR), Usability, and Usability-Security Characteristic Curve (USC). While it is reasonable to use these performance evaluation metrics in a continuous authentication system using the hard biometric, they are not suitable to evaluate the continuous authentication system using soft biometrics. The proposed soft-biometrics-based continuous authentication system gathers more frequent observations on user's biometric traits. Therefore, our system's performance can be measured based on false accept (FA) and false reject (FR) for each event (e.g., turning head away) rather than the delayed time until a correct decision is made. The continuous and frequent soft biometric observations available in our system enables immediate decision making. Our database also contains a variety of events (i.e., change in user's posture). We define the FR and FA below for continuous user authentication.

- False Reject (FR): The system identifies incorrectly that a user is not in the camera's field of view even though the user is still in front of the camera. False rejects lower the usability of the system.
- False Accept (FA): The system wrongly identifies an impostor as the legitimate user. False accepts lower the security of the system.

Table II shows our experimental results based on data collected on 20 users. We have tried several different threshold values and selected those providing the smallest FR and FA rates

[1] Session hijacking means that the legitimate user has successfully logged in, but an imposter forcibly takes over the system (e.g., by threatening the legitimate user) during the current session (the legitimate user has not logged out). This terminology is recommended by one of the reviewers.



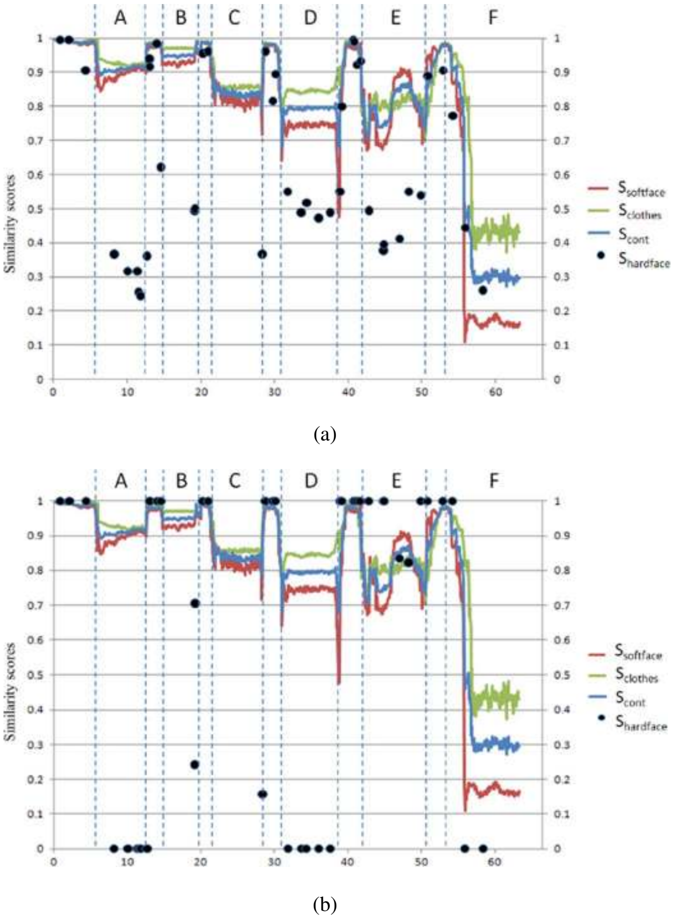
(a) (b) (c)

(d) (e) (f)

Fig. 8. Example video frames with automatically detected face and body regions for color histogram computation. (a) Turn head to left; (b) turn head to right; (c) turn head down; (d) lean back in chair; (e) stretch arms; and (f) walk away.

TABLE II
PERFORMANCE EVALUATION OF THE CONTINUOUS AUTHENTICATION SYSTEM

Scenario	False Reject Rate	False Accept Rate
A) Turn head to the left	0% (= 0 / 20)	0% (= 0 / 20)
B) Turn head to the right	0% (= 0 / 20)	0% (= 0 / 20)
C) Turn head down	10% (= 2 / 20)	0% (= 0 / 20)
D) Lean back in a chair	5% (= 1 / 20)	0% (= 0 / 20)
E) Stretch arms over-head	10% (= 2 / 20)	0% (= 0 / 20)
F) Walk away	0% (= 0 / 20)	0% (= 0 / 20)



(a)

(b)

Fig. 9. Example 1 of similarity score versus time graph using (a) Eigenface and (b) FaceVACS [25].

($w = 0.5$, $t_{\text{cont}} = 0.6$, $t_{\text{hardface}} = 0.8$, and $t_{\text{relogin}} = 0.6$). The main factors that explain the small number of false rejects are:

- The color histogram of the user's clothing changed significantly because of the illumination variations. This problem is typically observed when the color of the user's clothing is white (see Fig. 15), which is more susceptible to change in illumination compared to other colors, especially in scenarios D and E.
- The user's face is completely occluded, so no color histogram of the face could be computed [Fig. 14(c)].

Fig. 9(a) shows the changes in various similarity values (S_{clothes}, S_{softface}, S_{hardface}, and S_{cont}) as the user performs various actions in front of the webcam over time. Green, red, and blue lines represent the transition of S_{clothes}, S_{softface}, and S_{cont} similarity values, respectively, while black dots represent S_{hardface}. Recall that hard face authentication is only performed every 1 second. The range of similarity scores (S_{clothes}, S_{softface}, S_{hardface}, and S_{final}) is [0, 1]; a higher score represents a better matching. In Figs. 9 and 11 (corresponding video frames are shown in Figs. 10 and 12), the similarities, S_{clothes}, S_{softface}, and S_{cont} remain high regardless of the user's posture (scenarios A–E), but they go down rapidly after the user walks away from the console (scenario F). On the other hand, the hard face similarity S_{hardface} is not very stable depending on the user's posture. This demonstrates the advantage of using soft biometric traits for continuous authentication. Fig. 9(b) shows a plot similar to Fig. 9(a), but with S_{hardface} obtained by using a leading commercial face recognition engine FaceVACS [25]. Since both Eigenface and FaceVACS show similar performance, we used Eigenface in the remaining experiments (Figs. 11, 13, 16, 18, and 24). Fig. 13 (corresponding video frames are shown in Fig. 14) shows an example of FR during scenario C. This is because as the user was looking down, the system failed to track both the face and body correctly. Fig. 14(c) shows the corresponding input video frames leading to FR.

To further demonstrate the robustness of the proposed system, we also conducted the following additional evaluations: 1) illumination change detection, 2) relogin authentication, 3) occlusion, and 4) evaluation on a laptop with a built-in camera (as opposed to externally mounted web cam).

1) Illumination Change Detection: Consider two frames of a user in Fig. 17 where an illumination change is observed. Fig. 16 shows the results of various similarity computation over time without and with enrollment update, respectively, for the scenario in Fig. 17. In Fig. 16(a), the soft biometrics similarity values decrease rapidly as soon as the illumination change occurs, while in Fig. 16(b) due to template update these similarity values remain high even after the illumination change. On the other hand, the scores of face recognition go down after

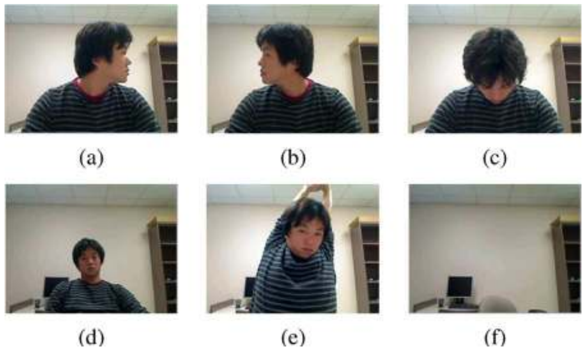


Fig. 10. Images used to construct the graphs in Fig. 9. (a) Turn head to left; (b) turn head to right; (c) turn head down; (d) lean back in chair; (e) stretch arms; and (f) walk away.

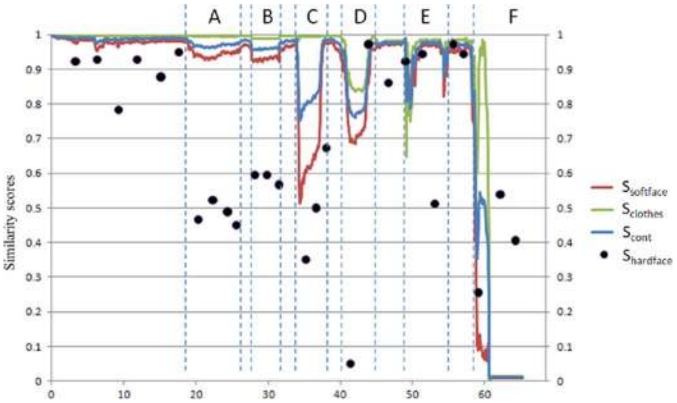


Fig. 11. Example 2 of similarity score versus time graph.

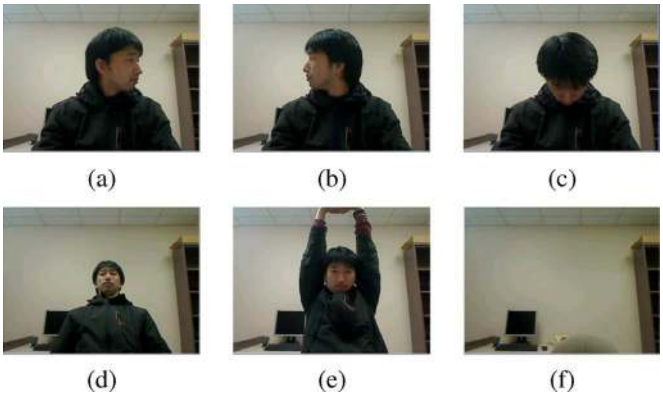


Fig. 12. Images used to construct the graph in Fig. 11. (a) Turn head to left; (b) turn head to right; (c) turn head down; (d) lean back in chair; (e) stretch arms; and (f) walk away.

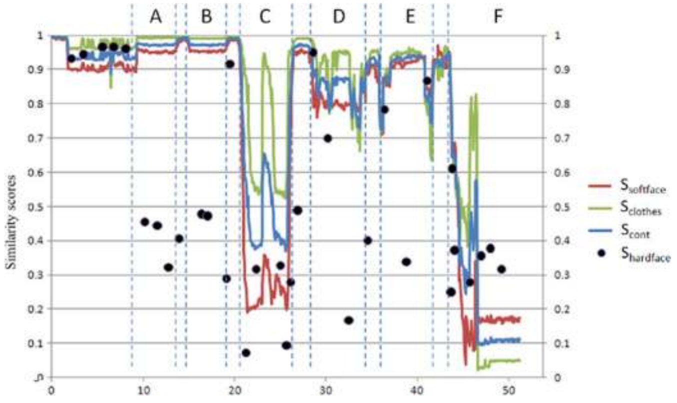


Fig. 13. Example 3 of similarity score versus time graph.

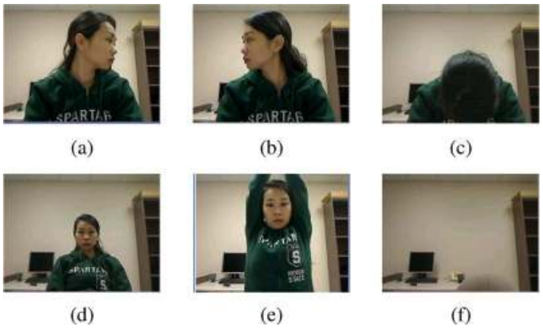


Fig. 14. Images used to construct the graph in Fig. 13. (a) Turn head to left; (b) turn head to right; (c) turn head down; (d) lean back in chair; (e) stretch arms; and (f) walk away.

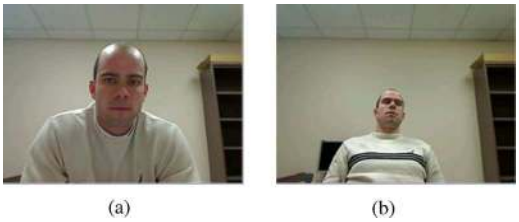


Fig. 15. Example of FR. (a) Enrollment. (b) Authentication.

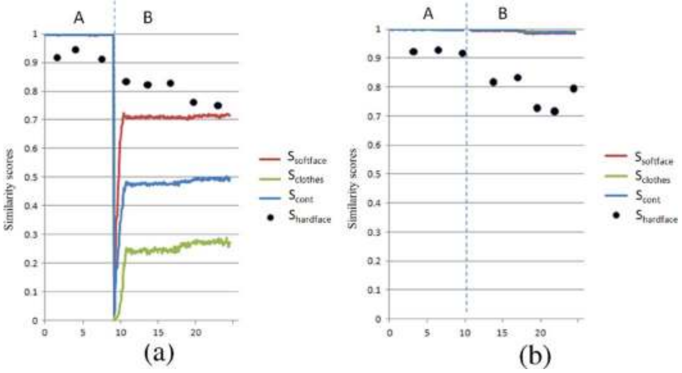


Fig. 16. Example 1 of similarity score versus time graphs with and without enrollment update. (a) Without enrollment update. (b) With enrollment update.

the illumination change. While a more advanced face recognition engine is likely to be more robust to moderate illumination changes, it will still fail with large pose variations, as shown in Fig. 9(b). Fig. 18 (corresponding video frames are shown in Fig. 19) shows another example video where the user also shifted his position along with the illumination change. Fig. 18(a) and (b) shows the transition of S_{cont} values without and with enrollment update, respectively. Fig. 18(b) shows that the system is able to successfully recognize the user after the illumination change with only slight fluctuations in the similarity scores. Table III shows the false illumination detection rate using the same data used in Section IV-C. No false detection due to illumination change was observed in the test.

2) Relogin Authentication: The proposed relogin authentication method is evaluated using video clips where an authorized user logs in, the user leaves the work environment (without logging out) and then, another user (an impostor) appears in the field of view of the webcam. Fig. 20 shows this scenario. The system successfully detects an impostor in Fig. 20(c) and permits relogin to the initial logged in user in Fig. 20(e). The colored ellipses in Fig. 20(a) and (e) indicate that the system correctly recognized the valid user in front of the console, while

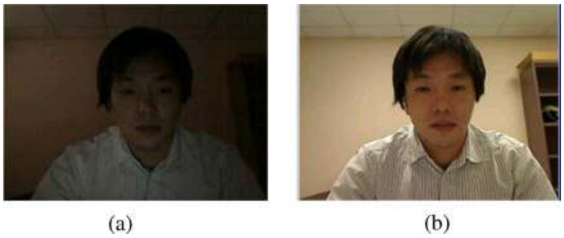


Fig. 17. Images before and after the illumination change used for plots in Fig. 16. (a) Dark room. (b) Bright room.

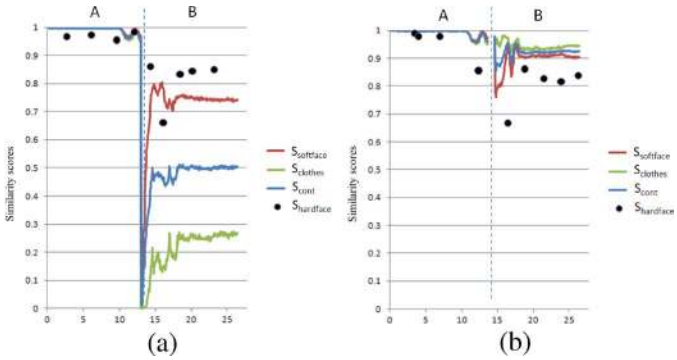


Fig. 18. Example 2 of similarity score versus time graphs with and without enrollment update. (a) Without enrollment update. (b) With enrollment update.

TABLE III
FR RATES IN THE PRESENCE OF ILLUMINATION CHANGE

Scenario	False Reject Rate
A) Turn head to the left	0%
B) Turn head to the right	0%
C) Turn head down	0%
D) Lean back in a chair	0%
E) Stretch arms overhead	0%
F) Walk away	0%

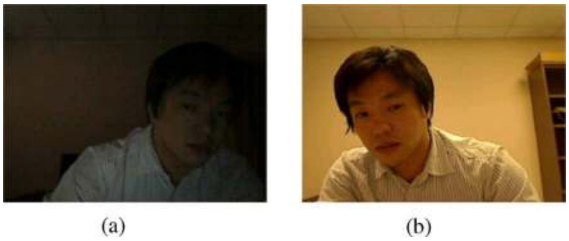


Fig. 19. Images before and after the illumination change used for plots in Fig. 18. (a) Dark room. (b) Bright room.

black-and-white images in Fig. 20(b), (c), and (d) indicate that the system correctly recognized the absence of the valid user in front of the console.

3) Occlusion: Even though occlusion was partly evaluated in earlier experiments (turn head down to occlude both face and clothing in Figs. 9, 11, and 13), we performed a test with a more explicit occlusion by a paper file. Figs. 21 and 22 show the results of successful continuous authentication with occlusion event. The system enters relogin authentication mode and then accepted the user when his face and clothes become available after the occlusion. In the current system, if the occlusion occurs for a long time ($> t_{\mathrm{relogin}}$), then the user will not be accepted to the system. In this case, the user needs to start over from the initial login mode. In Fig. 21, the hard face biometric has similar performance as the soft biometrics because the face appears in the frontal pose in most of the video frames. However, the similarity score of hard face drops with facial pose variations as shown in Fig. 9.

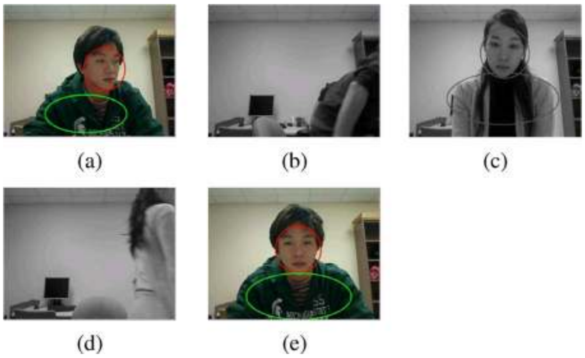


Fig. 20. Example results of relogin authentication experiments. (a) Authentic user; (b) authentic user walks away; (c) imposter user; (d) imposter user walks away; and (e) authentic user returns.

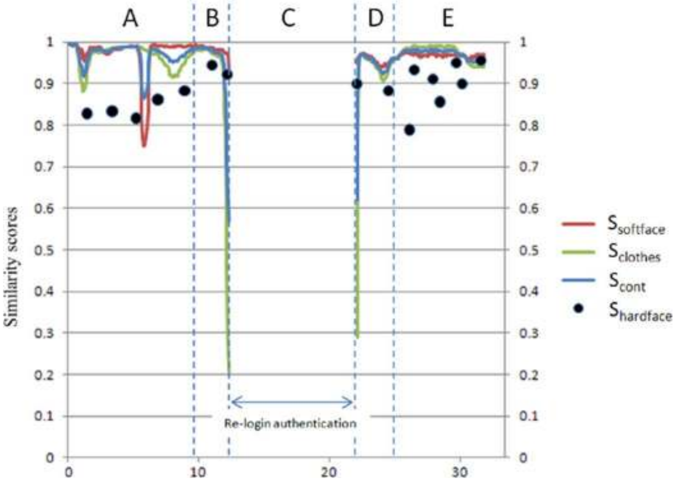


Fig. 21. Example of similarity score versus time graph with occlusion.

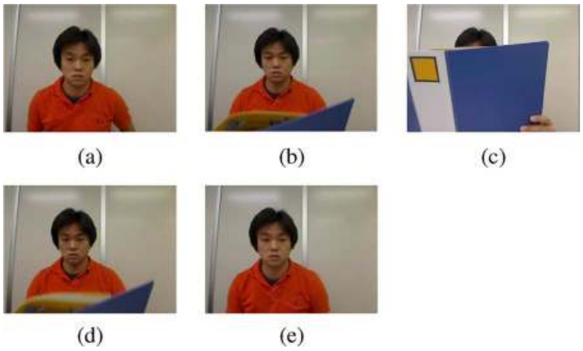


Fig. 22. Images used to construct the graph in Fig. 21. (a), (b), (c), (d), and (e) correspond to time instants A, B, C, D, and E in Fig. 21.

4) Laptop With Built-In Webcam: We have also evaluated our system using a built-in webcam as opposed to a webcam externally mounted on the laptop/desktop screen. Fig. 23 shows the laptop with a built-in camera (red ellipse). The built-in webcam provides a frame rate of 15 frames/s and an image size of 640 × 480 pixels. The images captured from the built-in webcam are a little blurry and show low saturation. In spite of that,

Fig. 23. (a) Laptop with a built-in webcam and (b) close up view of the built-in camera.

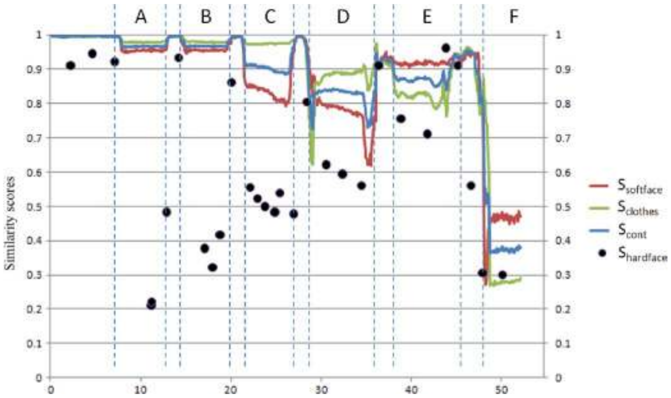


Fig. 24. Example of similarity score versus time graph for the built-in webcam.

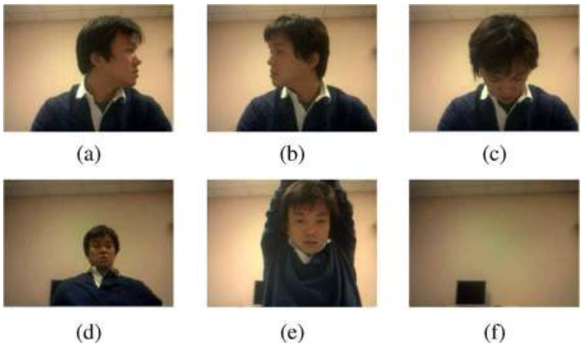


Fig. 25. Images from built-in webcam used to construct similarity score versus time graph of Fig. 24. (a) Turn head to left; (b) turn head to right; (c) turn head down; (d) lean back in chair; (e) stretch arms; and (f) walk away.

Figs. 24 and 25 show the result of successful continuous authentication using the built-in webcam.

D. System Attacks

We now analyze the points of vulnerability in the proposed system and provide possible approaches to reduce the systems vulnerabilities. The major points of attacks are in the: 1) initial login time with stolen password, 2) continuous authentication mode, and 3) relogin authentication mode. First, an effective method to prevent the system attack in case the password is stolen is by incorporating the hard biometric in the login process. However, this does not prevent all the attacks because the hard biometric trait itself can be compromised. Second, an attacker can have very similar soft biometric traits with the authentic user and breach the system. However, we minimized the risk of this type of attack by introducing the relogin authentication mode. Whenever the system fails in authenticating the user by his soft biometric traits, it enters the relogin authentication mode where the user needs to be authenticated both by hard and soft biometrics. When there is a sudden lighting change, for example, the system first checks whether it is due to the lighting change or the change in the soft biometric trait (e.g., clothing change or absence of the user). We explained how we distinguish between changes in lighting and user absence in Section IV-C. If the change is due to the change of user, the system enters relogin authentication mode, else if the change is due to the lighting the system updates the soft and hard biometric traits and stays in the continuous authentication mode. Third, system can be breached at the relogin authentication mode when the user has very similar soft biometrics (i.e., clothing and face color) and face appearance. We utilize the time decaying function in the relogin authentication step to block an unauthorized user after a certain time lapse.

V. Conclusion and Future Work

We have proposed a new framework that uses soft biometric traits for continuous user authentication. This framework registers a new enrollment 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 system is robust with respect to user's posture in front of the workstation and it also has the capability for enrollment template update and relogin authentication. Soft biometrics for continuous authentication offers high usability and, using both soft and hard biometrics (face recognition) for relogin 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 high tolerance to the user's posture. In our ongoing work, we are considering introducing additional soft biometric traits (e.g., relative position and size between the face and the body and their shape attributes) to further improve the system's robustness against illumination changes and cluttered background. The use of two cameras to capture depth information through stereography is also being evaluated. We are also evaluating the proposed system in routine operating environments.

Acknowledgment

Usang Park is the corresponding author.

References

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

[2] 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.

[3] 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.

[4] A. Vance, "If your password is 123456, just make it HackMe," *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., *Handbook 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] A. 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] A. 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.

[11] A. Azzini and S. Marrara, "Impostor users discovery using a multimodal biometric continuous authentication fuzzy system," *Lecture Notes in Artificial Intelligence*, vol. 5178, pp. 371–378, 2008.

[12] H.-B. Kang and M.-H. Ju, "Multi-modal feature integration for secure authentication," in *Proc. Int. Conf. Intelligent Computing*, 2006, pp. 1191–1200.

[13] C. Carrillo, "Continuous Biometric Authentication for Authorized Aircraft Personnel: A Proposed Design," Master's thesis, Naval Postgraduate School, Monterey, CA, 2003.

[14] A. Klosterman and G. Ganger, Secure Continuous Biometric-Enhanced Authentication Carnegie Mellon University, Tech. Rep. CMU-CS-00-134, 2000.

[15] G. Kwang, R. H. Yap, T. Sim, and R. Ramnath, "A usability study of continuous biometrics authentication," *LNCS*, vol. 5558, pp. 828–837, 2009.

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

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

[18] M. Turk and A. Pentland, "Eigenfaces for recognition," *Int. J. Cognitive Neurosci.*, vol. 3, no. 1, pp. 71–86, 1991.

[19] A. Bhattacharyya, "On a measure of divergence between two statistical populations defined by their probability distributions," *Bull. Calcutta Math. Soc.*, vol. 35, pp. 99–109, 1943.

[20] R. Lienhart and J. Maydt, "An extended set of Haar-like features for rapid object detection," in *Proc. IEEE Int. Conf. Image Processing*, 2002, vol. 1, pp. 900–903.

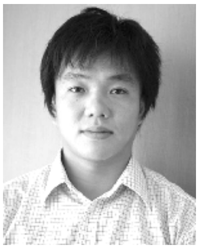
[21] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in *Proc. IEEE Computer Vision and Pattern Recognition*, 2001, pp. I-511–I-518.

[22] G. Jaffre and P. Joly, "Costume: A new feature for automatic video content indexing," in *Proc. Adaptivity, Personalization and Fusion of Heteogeneous Information (RIAO)*, 2004, pp. 314–325.

[23] D. Comaniciu and P. Meer, "Mean shift: A robust approach toward feature space analysis," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 5, pp. 603–619, May 2002.

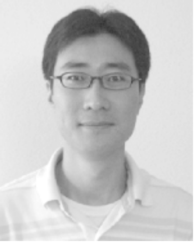
[24] D. Comaniciu, V. Ramesh, and P. Meer, "Kernel-based object tracking," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 5, pp. 564–577, May 2003.

[25] FaceVACS Software Developer Kit, Cognitec Systems GmbH [Online]. Available: http://www.cognitec-systems.de



Koichiro Niinuma received the B.S. degree in electrical and electronic engineering and the M.S. degree in intelligence science and technology from Kyoto University, Japan, in 2001 and 2003, respectively.

He is a researcher at Fujitsu Laboratories Ltd., Kawasaki, Japan. He was a visiting scholar at the Pattern Recognition and Image Processing Laboratory, Michigan State University, from 2009 to 2010. His research interests include biometrics, computer vision, and image processing.



Unsang Park (S'08–M'08) received the B.S. and M.S. degrees from the Department of Materials Engineering, Hanyang University, South Korea, in 1998 and 2000, respectively. He received second M.S. and Ph.D. degrees from the Department of Computer Science and Engineering, Michigan State University, in 2004 and 2009, respectively.

From 2009, he was a Postdoctoral Researcher in the Pattern Recognition and Image Processing Laboratory, Michigan State University, East Lansing. His research interests include biometrics, video surveillance, image processing, computer vision, and machine learning.

Anil K. Jain (S'70–M'72–SM'86–F'91) is a university distinguished professor in the Department of Computer Science and Engineering, Michigan State University, East Lansing. His research interests include pattern recognition and biometric authentication.

Dr. Jain received the 1996 IEEE TRANSACTIONS ON NEURAL NETWORKS Outstanding Paper Award and the Pattern Recognition Society best paper awards in 1987, 1991, and 2005. He served as the editor-in-chief of the IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE (1991–1994). He is a fellow of the AAAS, ACM, IAPR, and SPIE. He has received Fulbright, Guggenheim, Alexander von Humboldt, IEEE Computer Society Technical Achievement, IEEE Wallace McDowell, ICDM Research Contributions, and IAPR King-Sun Fu awards. The holder of six patents in the area of fingerprints, he is the author of a number of books, including *Handbook of Fingerprint Recognition* (2009), *Handbook of Biometrics* (2007), *Handbook of Multibiometrics* (2006), *Handbook of Face Recognition* (2005), *BIOMETRICS: Personal Identification in Networked Society* (1999), and *Algorithms for Clustering Data* (1988). ISI has designated him a highly cited researcher. According to Citeseer, his book *Algorithms for Clustering Data* (Prentice-Hall, 1988) is ranked #93 in most cited articles in computer science. He served as a member of the Defense Science Board and The National Academies committees on Whither Biometrics and Improvised Explosive Devices.