Continuous User Authentication Using Temporal Information

Koichiro Niinuma [a], Anil K. Jain [b]
[a] Fujitsu Laboratories, Kawasaki, Japan;
[b] Department of Computer Science & Engineering, Michigan State University, East Lansing, MI

ABSTRACT

Conventional computer systems authenticate users only at the initial log-in session, which can be the cause of a critical security flaw. To resolve this problem, systems need continuous user authentication methods that continuously monitor and authenticate users based on some biometric trait(s). We propose a new method for continuous user authentication based on a Webcam that monitors a logged in user's face and color of clothing. Our method can authenticate users regardless of their posture in front of the workstation (laptop or PC). Previous methods for continuous user authentication cannot authenticate users without biometric observation. To alleviate this requirement, our method uses color information of users' clothing as an enrollment template in addition to their face information. The system cannot pre-register the clothing color information because this information is not permanent. To deal with the problem, our system automatically registers this information every time the user logs in and then fuses it with the conventional (password) identification system. We report preliminary authentication results and future enhancements to the proposed system.

Keywords: biometrics, continuous authentication, secure log-in, face recognition, color histogram

1. INTRODUCTION

Most existing computer systems authenticate a user only at the initial log-in session. As a result, it is possible for another user, authorized or unauthorized, to access the system resources, with or without the permission of the signed-on user, until the initial user logs out. This can be a critical security flaw not only for high-security systems (e.g., the intellectual property office of a corporation) but also for low-security access control systems (e.g., personal computers in a general office environment). To deal with this problem, systems need methods for continuous user authentication where the signed-on user is continuously monitored and authenticated.

Biometric authentication [1] is useful for continuous authentication and several studies on this topic have been published [4, 5, 6, 7, 8, 9, 10]. For a continuous user authentication to be user friendly, passive authentication (e.g., face recognition) is desirable because the system should not require users' active cooperation to authenticate users continuously. In addition, a single biometric trait (unimodal technique) is not sufficient to authenticate a user continuously because the system sometimes cannot observe the biometric information. For example, the system will not be able to capture a user's face image if he turns his head away from the monitor. In general, to address the limitations of single biometrics, using multimodal biometrics (combining two or more single biometrics, e.g., face and iris) is a good solution.

In this application, the use of multimodal biometrics cannot resolve the problem, though it mitigates the problem. For example, the system cannot observe any biometric traits whenever the user takes a break to read a book or consults notes. This problem will persist as long as the system uses only primary biometric traits, like fingerprint, face, iris, etc. While these biometric traits contain strong discriminatory information about an individual, sometimes it is hard to observe them. On the other hand, there are soft biometric traits [2, 3], like gender, skin color, and hair color, which do not have sufficient discriminatory information about the individual, but they are nevertheless useful for identifying individuals in some cases such as continuous authentication.

In this paper, we propose a new method for continuous user authentication. Our method uses color information of users' clothing as an enrollment template in addition to their face information. The system cannot pre-register the clothing color information because this information is not permanent. To deal with the problem, our system automatically registers both clothing color and face information every time the user logs in and then fuses it with a conventional identification system.

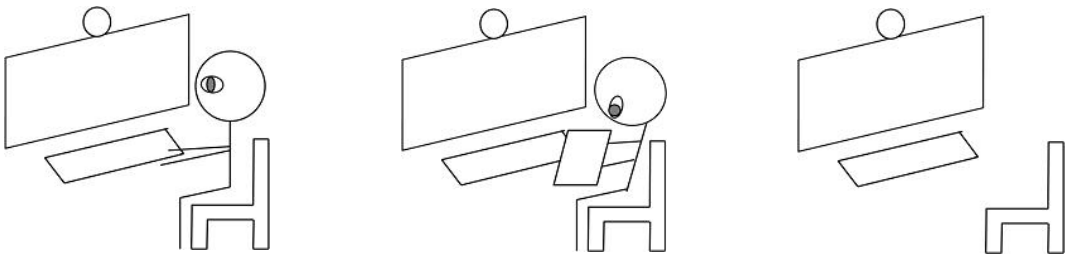
2. SYSTEM REQUIREMENTS

Continuous authentication is important not only for high-security systems (e.g., border control) but also low-security systems (e.g., home computing environment). For example, an average user typically walks away from the computer for short breaks without logging out of the system. This opens up an opportunity for unauthorized users to access the computing resources easily. It is desirable to develop a continuous authentication technique that is applicable to a wide range of log-in scenarios. We propose the following three criteria for continuous user authentication.

1. **Usability**: The system should not require active re-authentication of the users as long as the users are in front of the console, regardless of the users' posture, i.e., even if no biometric observations can be captured in any modality. For example, 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.
2. **Security**: The system should require active re-authentication of the user every time the user walks away from the console. This requirement will ensure that unauthorized users cannot access the resources after the legitimate user moves away.
3. **Cost**: The system should be implemented with commercial off-the-shelf (COTS) devices only. Cost is a very important factor in a low-security environment. For this reason, the authentication system should use only the standard devices (e.g. keyboard, mouse, and Web camera) and avoid the use of special devices.

To satisfy these criteria, the system needs to distinguish between scenario 1 and scenario 2 as discussed below and illustrated in Figure 1. The goal is to implement the continuous user authentication system, which does not require active re-authentication while the user is in front of the console (scenario 1) and requires active re-authentication every time the user moves away from the console (scenario 2).

1. Scenario1: The user is in front of the console.
   A) Case1: Biometric observations are available. For example, the user is in front of the console and his frontal facial view is available to the Webcam.
   B) Case2: There are no observations available in any biometric modality. For example, the user is sitting in front of the console, but is looking down.
2. Scenario2: The user has moved away from the console.



Scenario 1 case 1 Scenario 1 case 2 Scenario 2

Figure 1. Examples of two scenarios

3. RELATED WORK

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

Monrose and Rubin [4] proposed keystroke biometric technique for continuous authentication. Their method is based on a single biometric (unimodal technique), so in the absence of keystroke data, the system is not able to authenticate the user.

Altinok and Turk [5] proposed continuous authentication techniques using face, voice, and fingerprint. They claimed that a continuous biometric authentication system should be able to provide a meaningful estimate of authentication certainty at any given time, even in the absence of any biometric data. They presented a new temporal integration technique that satisfied this requirement. Each match score is modeled as a Gaussian random variable and, as expected, the authentication uncertainty increases over time. Surprisingly, even in the absence of any biometric data, Altinok and Turk were able to provide an estimate of the authentication certainty. However, in such a scenario, the authentication certainty must go down rapidly with time in order to maintain the system security, regardless of whether the user is in front of the console or not. This leads to a decrease in the system usability.

Sim and Zhang [6, 7] proposed a continuous authentication technique using face and fingerprint biometrics. They used a mouse with a built-in fingerprint sensor, which made fingerprint authentication a passive method for authentication. The authors proposed that a continuous biometric authentication should satisfy the following three criteria.

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

The authors presented a new Holistic Fusion method that satisfied the above criteria. Their technique was based on using the Hidden Markov Model. In addition, they proposed several new metrics to measure the performance of a continuous verification system. These include Time to Correct Reject, Probability of Time Correct Reject, Usability, and the Usability-Security Curve. However, Sim and Zhang’s technique had the same limitations as [5]; when no biometric observations are available, the authentication certainty must go down rapidly with time in order to protect the security, irrespective of whether the user is in front of the console or not.

Similar to Sim and Zhang [6, 7], Azzini and Marrara [8, 9] also proposed a continuous authentication technique using face and fingerprint biometrics. Their system checked the identity of the user only on the basis of face recognition. If the authentication certainty of face recognition falls below a threshold, then a new fingerprint acquisition is required. Again, the authentication certainty in this approach must go down rapidly with time in order to ensure the security, regardless of whether the user is in front of the console or not.

Kang and Ju [10] proposed a continuous authentication technique using face and behavioral biometrics. They used face trajectory and its pose as behavioral features. Because behavioral biometrics were used only for assisting face authentication, the authentication certainty must go down rapidly over time in the absence of face biometric data.

Table 1 shows a comparison of previous work. These methods satisfy security criteria, but do not satisfy usability criteria because they assume that the system requires re-authentication whenever any biometric observations are not available. These methods satisfy cost criteria because we classify fingerprint sensors as COTS devices. The method that Monrose and Rubin [4] proposed is not included in this table because they did not describe a practical system based on keystroke authentication.

Table 1. A comparison of previous work on continuous user authentication

	Usability	Security	Cost
Altinok and Turk [5]	No	Yes	Yes
Sim and Zhang [6, 7]	No	Yes	Yes
Azzini and Marrara [8, 9]	No	Yes	Yes
Kang and Ju [10]	No	Yes	Yes

None of the previous studies on continuous authentication distinguish between Scenario 1 and Scenario 2 shown in Figure 1. So, they cannot satisfy the three criteria of usability, security, and cost simultaneously as shown in Table 1. We classify these existing approaches into three types as follows.

1. Conventional authentication
   - The system authenticates the user based on a password or even biometrics only at limited time(s) (e.g., only at log-in time or, say, every 15 minutes if there has not been any activity at the console).
2. Continuous authentication A
   - The system authenticates the user only when biometric observations are available. The authentication certainty is not calculated in the absence of any biometric observations.
3. Continuous authentication B
   - The system authenticates the user when biometric observations are available. The system requests active re-authentication every time the biometric observations are not available. The authentication certainty is very low when there are no biometric observations.

Conventional authentication cannot distinguish the two scenarios in figure 1, and in general it does not request active re-authentication at all after log-in. So, while the conventional authentication satisfies criterion 1 (usability), it does not satisfy criterion 2 (security). Continuous authentication schemes A and B mentioned above also cannot distinguish between scenario 1 and scenario 2, but they can distinguish between “scenario 1 case 1” and “scenario 1 case 2 or scenario 2”. So, while continuous authentication A satisfies the usability criterion, it does not satisfy the security criterion. On the other hand, continuous authentication B satisfies the security criterion but does not satisfy the usability criterion. Table 2 and Figure 2 show a comparison of previous methods of continuous authentication and the proposed scheme. Table 1 and Figure 2 include only the usability and security criteria because the cost criterion depends on what devices are adopted for system implementation.

Table 2. A comparison of various continuous authentication schemes

	Usability	Security
Conventional authentication	Yes	No
Continuous authentication A	Yes	No
Continuous authentication B [5,6,7,8,9,10]	No	Yes
Proposed scheme	yes	Yes

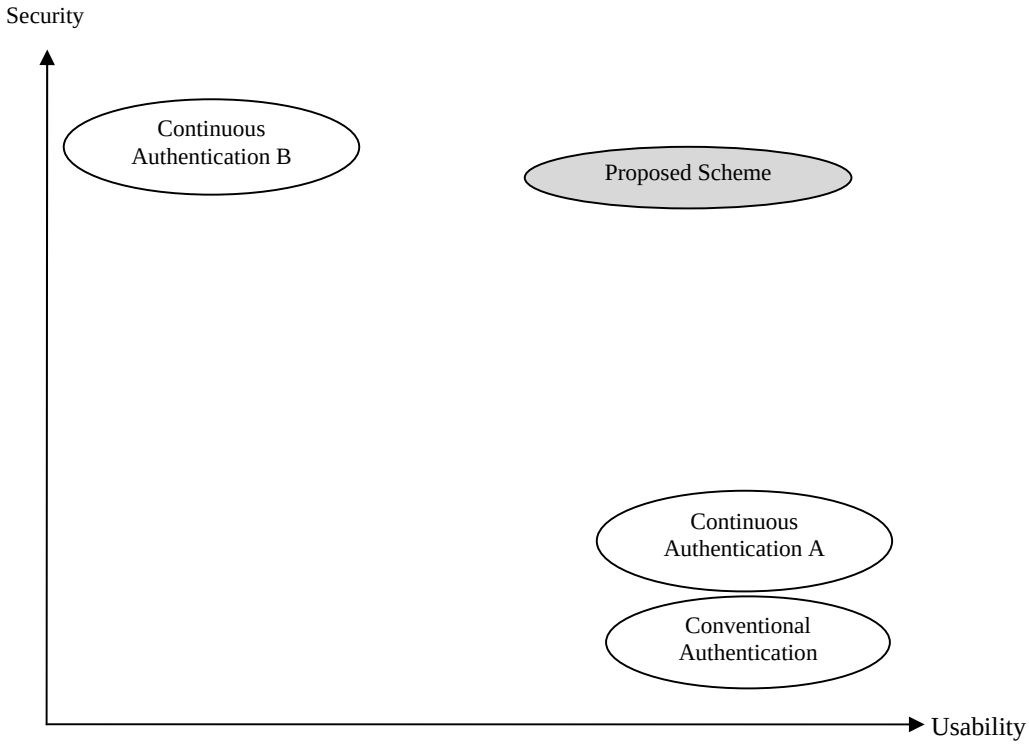


Figure 2. A comparison of various continuous authentication methods

4. PROPOSED FRAMEWORK

We propose a framework that combines continuous user authentication with a conventional identification method (such as password authentication or fingerprint authentication), which authenticates the user at the initial log-in session. In general, we need to pre-register our information as an enrollment template before we use a biometric system. But, the pre-registration is not suitable for distinguishing between scenario 1 and scenario 2, because it is difficult to pre-register the information that the system gets regardless of user's posture (even if no biometric observations are available in any modality). Instead of pre-registration, this method registers a new enrollment template every time a user logs in. This enables the use of temporal information, like color of user's clothing, as an enrollment template. The framework is composed of three modes as described below. Figure 3 shows an example of the sequence.

1. Mode1 (Enrollment): During log-in by conventional identification, the system registers an enrollment template automatically. We can assume that legitimate users are in front of the console during login. Therefore, the system can register the information that the system gets during login as an enrollment template of a legitimate user.
2. Mode2 (Identification): The system identifies whether the users are in front of the console or not. If the user moves away from the console, the status changes to termination status.
3. Mode3 (Termination): The system locks the console automatically, for example, log-out.

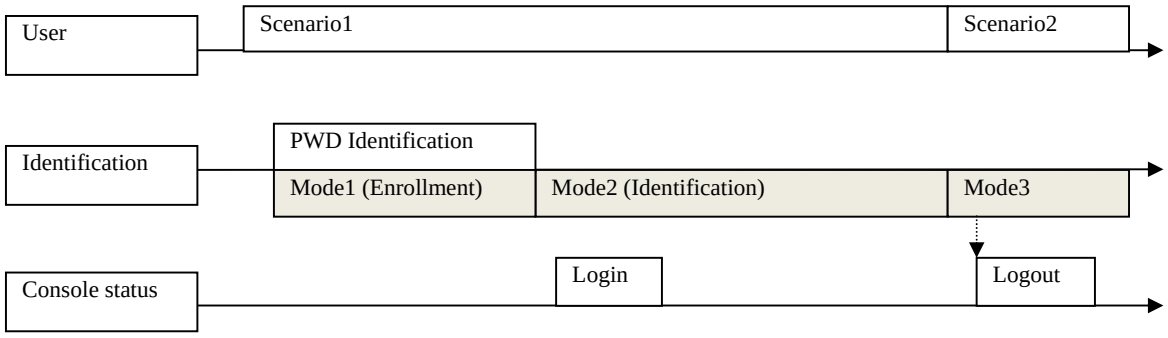


Figure 3. A sequence example of the proposed algorithm

5. PROPOSED ALGORITHM

We propose a continuous authentication algorithm that follows the framework. Our methods use color information of user's clothes as an enrollment template in addition to their face information. The method is similar to Jaffre and Joly [12], though their purpose is different from ours. They use the color distribution of person's clothing for automatic video content indexing.

5.1 Conditions

The algorithm we propose satisfies the following conditions. We assume that this algorithm is used for PC user identification, including laptop PCs, so these conditions are important for that specific purpose.

1. The algorithm works in real time on a PC.
2. The algorithm is robust to changes in user's posture.
3. The algorithm does not request user to undergo pre-registration of his biometric information.
4. The algorithm does not require a specific background scene.
5. The algorithm works correctly even if the background scene changes randomly.

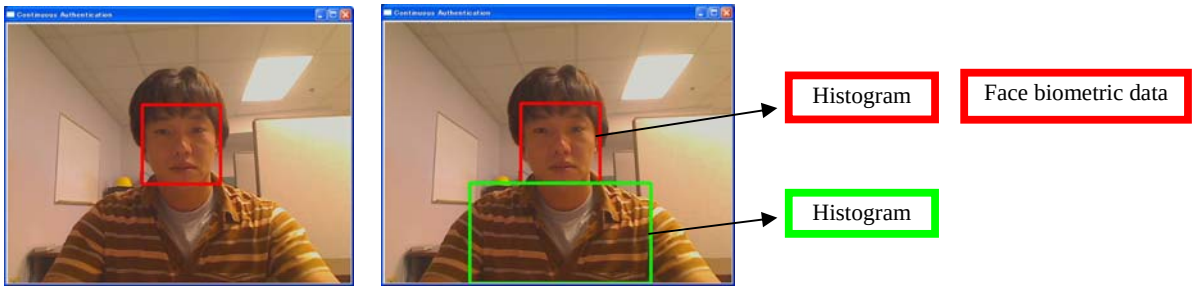
5.2 Enrollment (Mode 1)

The method of this mode is divided into 4 steps. Figure 4 shows an example of Mode 1.

1. Face detection
   - We use Haar classifier [11] as the face detection method, but any face detection method can be used. We can assume that user is typically looking in the frontal direction during Mode1 because of conventional identification, like password identification, and the system can detect a full view of the user's face during Mode 1.
2. Body localization
   - We follow Jaffre and Joly [12] to localize the body. We assume that the area under the face is always the user's body and the size of this area is proportional to the one of the face.
3. Registration of face and body histograms
   - The system calculates histograms of both the face and the body, and registers them as enrollment data.

4. Registration of face biometric data

   - The system registers face biometric data. We use PCA based face recognition, but any face recognition algorithm can be used instead. Because the system registers face biometric data every time a user logs in, the problem of the illumination difference between the time of enrollment and the time of identification is mitigated.



Mode1 (1) Face Detection Mode1 (2) Body Localization Mode1 (3) (4) registration

Figure 4. An example of Mode1

5.3 Identification (Mode 2)

The method of this mode is divided into 3 steps.

1. Face and body identification using histograms

   - The system tracks the face and the body separately based on the histograms registered in Mode1 (3) by applying the mean shift procedure [13, 14] and calculating the similarity S_{body} and S_{face} separately. We use the Bhattacharyya distance for calculating the similarity. We define the maximum size and the minimum size of the face and the body.

2. Face recognition

   - Face recognition is executed at regular intervals (e.g., once every 10 seconds). If it succeeds, T_{last}, which represents the last time the face recognition was successful, is updated. Face recognition is used only for assisting the identification using color histograms because the system cannot obtain the face information during scenario 1 case 2.

3. Calculating the final similarity

   - We define the final similarity S_{final} as below. If S_{final} is lower than a threshold, the status moves to Mode 3. Otherwise, the status returns to Mode 2 (1). T_{cur} means current time and T_{last} means the last time the face recognition was successful. **F**(t) is a monotone decreasing function and the range of **F**(t) is [0, 1]. The range of x is also [0, 1].

$$S_{final} = \mathbf{F}(T_{cur} - T_{last}) \ (x \, S_{face} + (1 - x) \, S_{body}) \quad (1)$$

5.4 Termination (Mode 3)

The method of this mode consists of only 1 step.

1. The system locks the console automatically.

6. EXPERIMENTS

6.1 System

Figure 5 shows our system, which consists of a laptop and a Webcam. We prepared several scenarios, including some challenging scenarios, and evaluated them in the experiments. The frame rate is 15 fps and the image size is 640 x 480 pixels.

Figure 5. System consisted of a laptop and a Webcam

6.2 Transition of Similarity

Figure 6 shows a result of an experiment and figure 7 shows a scenario used in the experiment. In figure 6, green line displays the transition of S_{body}, blue line displays the transition of S_{head} and blue line displays the transition of S_{final}. Figure 6 shows that the system works well. That is to say, the system keeps the similarity value high while the user is in front of the console regardless of user's posture (A-E), and the similarity value goes down rapidly after a user moves away from the monitor (F). On the other hand, it is hard for previous methods to authenticate a user in some cases in figure 7 (especially A, B and C) because the system cannot get any biometric information (e.g. face biometric data) from those postures.

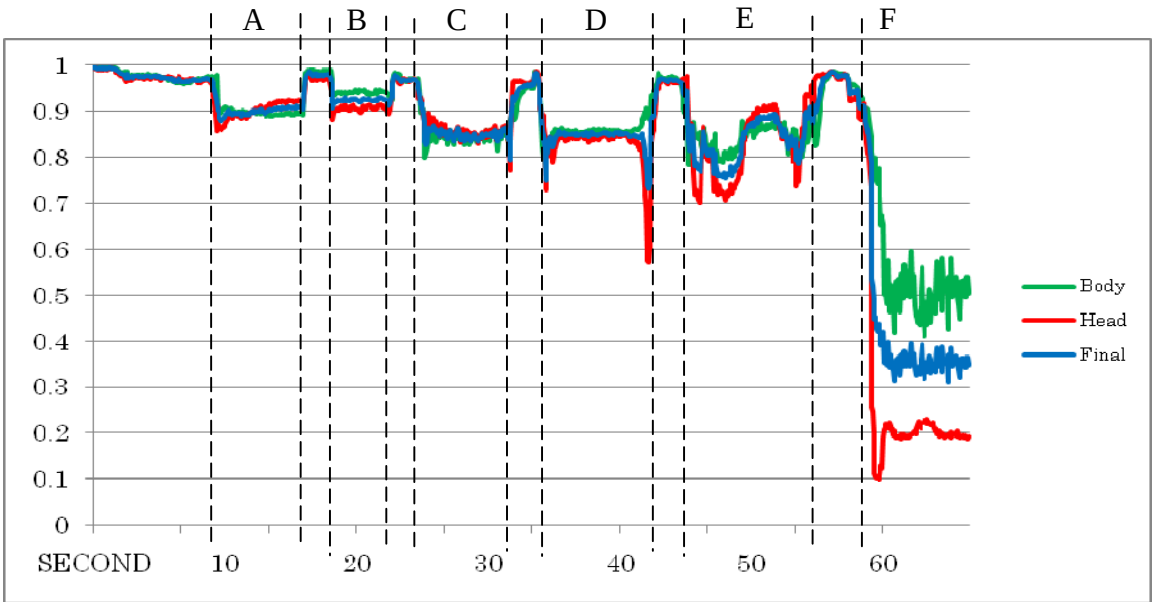
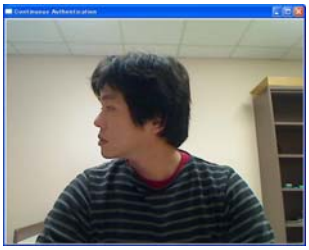
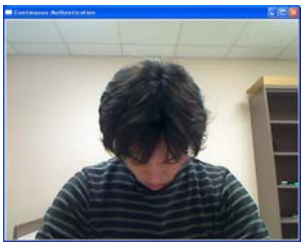


Figure 6. An example of transition of similarity

A. Turn head to left



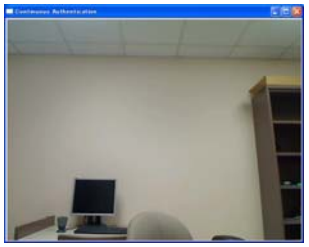
B. Turn head to right



C. Turn head down

D. Lean back in a chair

E. Stretch arms overhead



F. Move away

Figure 7. Scenarios

6.3 False Reject and False Accept/False Track

We define False Reject and False Accept/False Track as described below for continuous authentication.

1. 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 view of the camera. This problem lowers the usability of the system.
2. False Accept (FA) or False Track (FT): The system wrongly identifies a person that is not a legitimate user as the legitimate user. We call it false accept when the legitimate user is not in the camera's field of view anymore and call it false track when the legitimate user is still in the camera range. This problem lowers the security of the system.

To evaluate FR and FA/FT, we collected data from 12 users. In the experiments, the users were sitting in front of a Webcam and made some posture changes according to the same scenario as described in section 6.2. Figure 8 shows some examples of the experiments. In figure 8, the red ellipse indicates the face that the system tracked and the green ellipse shows the body that the system tracked.

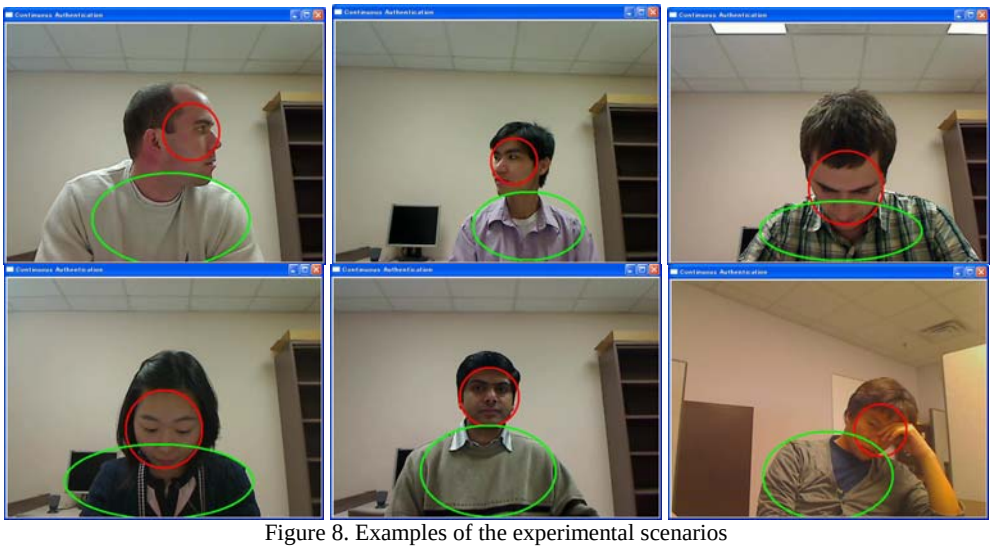


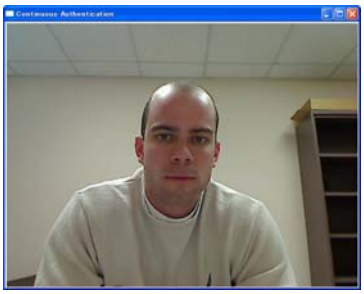
Figure 8. Examples of the experimental scenarios

Scenarios	False Reject Rate	False Accept Rate (False Track Rate)
A) Turn head to the left	0% (= 0 / 12)	-
B) Turn head to the right	0% (= 0 / 12)	-
C) Turn head down	0% (= 0 / 12)	-
D) Lean back in a chair	8.3% (= 1 / 12)	-
E) Stretch arms overhead	8.3% (= 1 / 12)	-
F) Move away	-	0% (= 0 / 12)

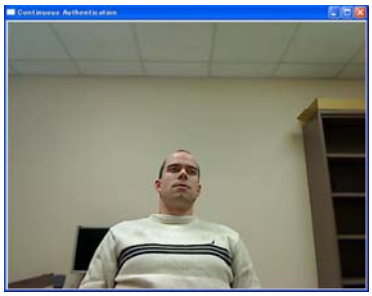
Table 3. False Reject and False Accept/False Track

Table 3 shows the results. The table shows good performance though there is a false reject in situations D and E). These false rejects happened because of the variations in the angle of illumination. In these cases, the color of user's clothing is white which is susceptible to the change of illumination. Figure 9 shows the images when false reject occurred. The system worked well in A, B and C regardless of the color of user's clothing, because the angle of illumination did not change widely in these cases.

These error rates are influenced by scenarios or recording conditions (e.g. the color of clothing). So we believe it would be necessary to design standard scenarios and/or standard databases in order to evaluate the systems for continuous authentication.



A. Enrollment



B. Identification

Figure 9. An example of False Reject

7. CONCLUSIONS

We propose three criteria for continuous authentication: usability, security, and cost. These criteria are important not only for high-security systems but also for low-security systems. In addition, we propose a new framework for continuous authentication to satisfy these criteria and a new algorithm that authenticates users regardless of their posture in front of the workstation (laptop or PC). Many studies on continuous authentication use multimodal biometrics, but none of these studies can identify the user in the absence of biometric observation. To alleviate this requirement, our method enrolls the user's face as well as the color of his clothing as an enrollment template every time the user logs in.

Overall, the method shows promise. Preliminary tests demonstrate that the system is able to continuously authenticate a user despite posture changes and the presence of other individuals in the camera`s field of view. Future improvements will include implementing the following functionalities:

1. A function to recalculate histograms in order to deal with dramatic illumination changes.
2. A function to use the information besides the color information (e.g. the relative position and size between the face and the body, or their shape information) in order to deal with heavy occlusion or false accept/false track.

In addition, we will evaluate both the usability and security of the system under real operating environments (e.g. evaluation under a daily business transaction environment for an extended period of time).

REFERENCES

[1] Anil K. Jain, Patrick Flynn and Arun A. Ross (eds.), Handbook of Biometrics, Springer, 2007.

[2] 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.

[3] Anil K. Jain, Sarat C. Dass and Karthik Nandakumar, "Soft Biometric Traits for Personal Recognition Systems," Proceedings of International Conference on Biometric Authentication, LNCS 3072, pp. 731-738, 2004.

[4] Fabian Monrose and Aviel D. Rubin, "Keystroke Dynamics as Biometrics for Authentication," Future Generation Computer Systems 16, pp. 351-359, 2000.

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

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

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

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

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

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

[11] Rainer Lienhart and Jochen Maydt, "An Extended Set of Haar-like Features for Rapid Object Detection," Proceedings of the 2002 IEEE International Conference on Image Processing, vol.1, pp. 900-903, 2002.

[12] Gael Jaffre and Philippe Joly, "Costume: A New Feature for Automatic Video Content Indexing," Proceedings of RIAO2004, pp. 314-325, 2004.

[13] Dorin Comaniciu and Peter Meer, "Mean Shift: A Robust Approach Toward Feature Space Analysis," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, pp. 603-619, 2002.

[14] Dorin Comaniciu, Visvanathan Ramesh and Peter Meer, "Kernel-Based Object Tracking," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol.25, no.5, pp. 564-577, 2003.