USER AUTHENTICATION USING TEMPORAL INFORMATION

Nida Jawre, Kiran Bhandari
Thakur College of Engg. & Technology, Kandivali (E), Mumbai, M.S., India

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. No pre-registration of biometric features are required as they are captured and saved every time the user logs in.

GENERAL TERMS: *Image processing*

KEYWORDS: *Biometrics, continuous authentication, secure log-in, face recognition, color histogram.*

I. 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 faces information every time the user logs in and then fuses it with a conventional identification system.

II. 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 the behavioral biometrics was used only for assisting face authentication, the authentication certainty must go down rapidly over time in the absence of face biometric data.

III. PROPOSED WORK

We propose a framework that combines continuous user authentication with a conventional identification method (such as password authentication or fingerprint authentication), which authenticates users 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 users' 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 colors of users' clothes, as an

enrollment template. The framework is composed of three modes as described below. Figure 1 shows an example of the sequence using following scenarios.

1. Scenario1: The user is in front of the console. 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.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.

- 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. From the captured frame face and the upper body is localized according.
- Mode2 (Identification):
- Mode 2:Continuous authenticate user based on captured skin and clothing color
- Mode 3: This mode has two part :
  Identify Illumination changes
  Remove false reject.
- Mode 4: Terminate

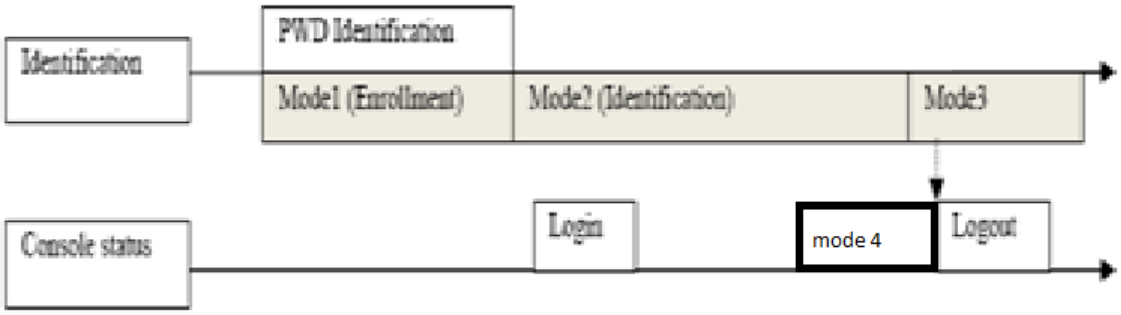

Fig.1 Outline of the proposed method

IV. PROPOSED ALGORITHM

We propose a continuous authentication algorithm that follows the framework. Our methods use color information of users' 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 persons' clothes for automatic video content indexing.

- **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 strong for the change of users' posture.
3. The algorithm does not request users to undergo pre-registration of their biometric information.
4. The algorithm does not require a specific background scene.
5. The algorithm works correctly if a background scene is changed randomly.

- **Enrollment (Mode 1)**

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

1.Face detection: The system uses Haar classifier[11] as the face detection method, The system assumes that users usually face front 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: Once the face is detected Jaffre and Joly[12] method is used to localize the body, which assumes 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. The enrollment template is saved in two folders maintained, in this system two folders are maintained one for face and one for clothing region.

4.Registration of face biometric data: The system registers face biometric data. System uses 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 one of identification is mitigated

- **Identification (Mode 2)**

The method of this mode is divided into 3 steps.

1. Face and body identification using haar classifier:

If the user is sitting in frontal pose the face is detected using haar classifier, as the face is detected the body is localized. The detected face and clothing region is cropped from the captured frame and is used for calculating color histogram of the current detected and previously saved face and clothing region, bhattacharyya distance for calculating the similarity between the histograms is used.

2. Face and body identification using histogram based tracker:

If the user is not sitting in frontal pose the haar classifier cannot detect face, hence body cannot be localized. In this situation the system tracks user using histogram based tracker. The tracker is applied on two frame a previous frame and current frame, previous frame is the frame on which haar classifier was able to detect face and current frame is frame on which haar classifier could not detect face.

3. Calculating the final similarity

The final similarity S_{final} is calculated as below. x=[0,1]

$$S_{final} = (x\, S_{face} + (1 - x)\, S_{body}) \quad (1)$$

- **Mode 3**

To check if there have been an illumination change the sytem perform image subtraction between frame captured before the S_{final} value was below threshold and current frame.The frames for consideration include only the background pixels as the users face and clothing region is filled with black color. If the number of pixel having considerable changes in intensity value is identified then an illumination change is detected and the new cropped face and clothing region is saved in their respective enrollment folders.

If the illumination change is not identified then the checks for user's hard biometric features using PCA based face recognition. This mode is used in system to avoid false reject of an authenticated user if the user has intentionally brought some changes in his clothing. If the match scores count falls below a threshold the system increment a count value which is kept to change the mode of the system to mode 4.

- **Mode 4**

This mode is implemented to avoid session hijacking. Many times it happens that if user forgets log-out of the system an intruder may come and have illegal access to the system. In this system it is assumed that for a user to get up from his place and for an intruder to occupy his place our system will have 10 captured frame to work on, a count value is incremented each time the absence of user is identified. The absence of user check moves into loop that of mode 2 that traces user using histogram based tracker, this tracker may have a false detected region if the background color matches with the face color. To avoid false accept the system again calculate S_{final} , which is observed to fall below threshold even though was traced as probable face region by histogram based tracker., and thus declaring the user's absence and incrementing the count value.

If user's face was occluded and the S_{final} falls below threshold for managing such situation another count value named tcount is calculated along with count value this tcount value can re-authenticate user if the user has not left his place and still not traced due to occluded facial region. The maximum tcount value is less than time required to capture 5 frames. If user's face is available within that time limit the count value is restored to 1. And the system resumes to mode 2. Else if the count value reaches the threshold value the system locks itself and is brought back to mode 1.

V. EXPECTED RESULTS

- ***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 one of identification is mitigated.

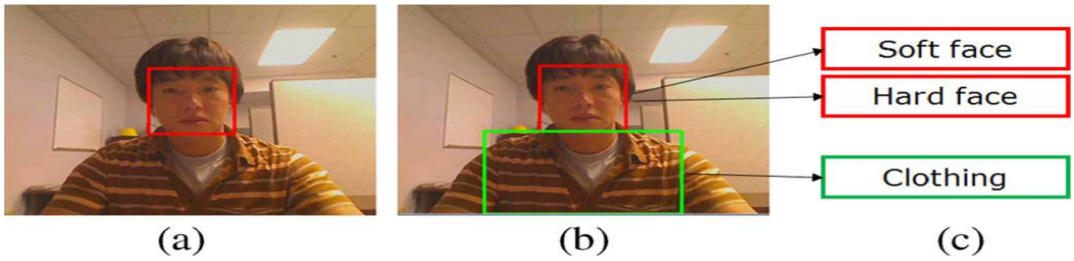

Figure 1. Initial enrollment mode. (a) Face detection, (b) body localization, and (c) registration.

- ***MODE 2:***

Authenticate the user continuously based on user's skin and clothing color irrespective to user position

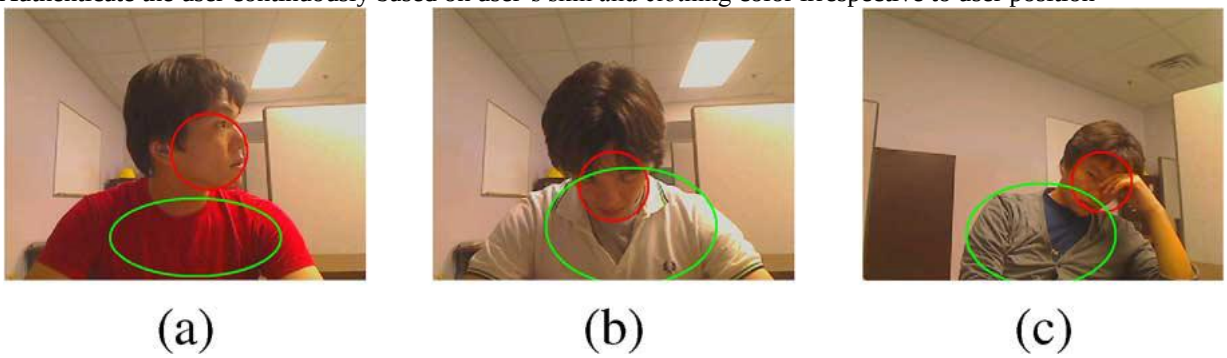

Figure 2. Examples of user's posture. The two ellipses in each image denote thefacial and clothing regions used to compute the color histograms.

- ***MODE 3:***

Check for illumination changes or changes in clothing.

Figure 3. 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 showchange in illumination between (a) and (b).

- ***MODE 4:***

Logoff if user is not in front of console for predefined count value.

Figure 4. No detection in case user is absent.

VI. CONCLUSION

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.

VII. FUTURE WORK

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 can also be added.

ACKNOWLEDGMENTS

Hearty thanks to my guide Mr. Kiran bhandari for his support and guidance.

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,"

AUTHORS

Nida Jawre, received bachelors degree in computer science from university of pune in 2008,now pursuing ME in computer science from university of Mumbai since 2011.

Kiran Bhandari ,received bachelor in ETRX, he received second degree in ME in ECT and is currently pursuing Phd.His area of interest is image processing and computer vision.