Temporal Information a Permanent Solution for Continuous Monitoring System

Nida Jawre
Thakur College of Engg. & Technology

Kiran Bhandari
ThakurCollegeofEngg.&Technology

ABSTRACT

Today there is no way that can ensure that person who logged in as authenticated user is the same user accessing the system. To resolve this problem continuous monitoring system can serve the purpose on the basis of extracted biometric features. But providing biometric features continuously cannot be feasible for the user. In the proposed method a continuous user monitoring system is developed which observe user's presence in front of console using a webcam and face detection technique on captured frame. This is implemented using both hard biometric and soft biometric features extraction. A final comparative analysis is drawn from the extracted results to prove the upper hand of soft biometric features over hard biometric features when it comes to continuous monitoring system.

General Terms

Image processing

Keywords

Biometrics, continuous authentication, secure log-in, face detection, color histogram

I INTRODUCTION

Humans have used body characteristics such as face, voice, and gait for thousands of years to recognize each other. But these features are helpful only when their respective biometric features are extracted, Conventional 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 [15] . The term *biometric* comes from the Greek words *bios* (life) and *metrikos* (measure). It is well known that humans intuitively use some body characteristics such as face, gait or voice to recognize each other. Since, today, a wide variety of applications require reliable verification schemes to confirm the identity of an individual, recognizing humans based on their body characteristics became more and more interesting in emerging technology applications. Traditionally, passwords and ID cards have been used to restrict access to secure systems but these methods can easily be breached and are unreliable. Biometric cannot be borrowed, stolen, or forgotten, and forging one is practically impossible [14]. The system using biometric features must be user friendly; it should be capable of monitoring user's presence even in absence of biometric features. For a system that works totally on biometric features giving results in absence of these features will be a problem. 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 [1, 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, a new method is proposed for continuous user authentication and is implemented using hard and soft biometric features. Our method uses PCA based face recognition techniques for hard biometric user authentication where as uses color information of users' clothing and face as soft biometric features. The system using soft biometric features cannot pre-register the clothing color information because this information is not permanent. To deal with the problem, system automatically registers both clothing color and faces information every time the user logs in and then fuses it with a conventional identification system.

2. RELATED WORK

Biometrics refers to the identification of a person based on his or her physiological or behavioral characteristics. Today there are many biometric devices based on characteristics that are unique for everyone. Some of these characteristics include, but are not limited to, fingerprints, hand geometry, and voice. These characteristics can be used to positively identify someone. Many biometric devices are based on the capture and matching of biometric characteristics in order to produce a positive identification. 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" [2]. 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.). 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. This property of soft biometric feature is very helpful when the system is supposed to continuously monitor the user's presence.

3. GENERAL FRAMEWORK

The proposed framework is implemented in two modes: Mode 1 uses soft biometric features for user authentication and Mode 2 uses hard biometric features for user authentication. A conventional identification method (such as password authentication or fingerprint authentication), which authenticates users at the initial log-in session. In general, there is need to pre-register our information as an enrollment template before using proposed framework if system is operating in mode 1. There is no need of pre-registration if soft biometric features are used for authentication i.e. the system is operating in mode 2.

- 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.
- Monitor: Continuous authentication of user based on operating mode
- False reject: Avoid probable false reject.

  Mode 1: use image normalization

  Mode 2: using image subtraction
- Terminate: Log off

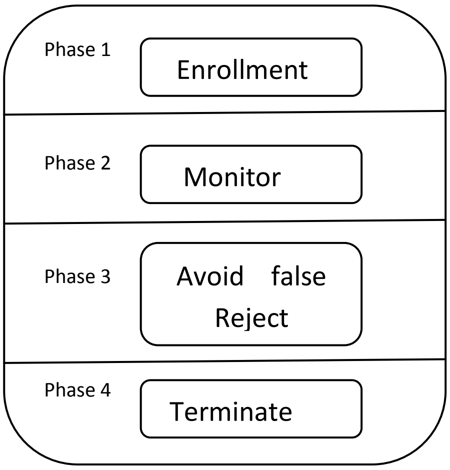

Fig.1 Outline of the framework

4. IMPLEMENTATION

The framework is operated in two modes. Mode 1: Using hard biometric features, Mode 2: Using soft biometric. Mode 1 uses PCA based face recognition technique for authentication. Mode 2 uses color information of users' clothes as an enrollment.

Conditions

The proposed framework satisfies the following conditions. It is assumed that this framework is used for PC user identification, including laptop PCs, so these conditions are important for that specific purpose.

The framework is subjected to following scenarios

1. Executed in real time on a PC.
2. Executed for the change of users' posture.
3. Framework operating in Mode 1 requires pre-registration of user's face.
4. Framework executing in mode does not requires pre-registration.
5. Executed without a specific background scene.

The framework is divided into 4 phases.

1. Enrollment

1.Face detection: The system uses Haar classifier[11] as the face detection method, The system assumes that users usually face front during phase 1 because of conventional identification, like password identification, and the system can detect a full view of the user's face during this phase.

2. Body localization: This phase is used only when the system is operating in Mode 2 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: This phase is used only when system is operating in Mode 2.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: this phase is used only when the system is operating in Mode 1. The system registers face biometric data. System uses PCA based face recognition, but any face recognition algorithm can be used instead.

- **Identification**

Identification Phase when operating in Mode 1:

1. Face using haar classifier: If the user is sitting in frontal pose the face is detected from every captured frame using haar classifier. The detected face is compared with the pre-registered face and similarity score is calculated using PCA face recognition. Since haar classifier is not capable of detecting face in any other posture other than frontal the system fails to detect the presence of user in front of console, making system feasible only for frontal posture.

Identification Phase when operating in 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 [11], 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 frames 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 where x=[0,1]

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

- **Avoid False reject**

Mode 1: If the similarity score falls below threshold value then the system checks if there has been an illumination change the cropped face is normalized to nullify the effect due to illumination change.

Mode 2: To check if there has been an illumination change the system performs image subtraction between frame captured before the S_{final} value was below threshold and current frame.

- **Terminate**

This phase 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.

Mode 1: This mode is not robust for change user's posture, this act as an advantage for intruder. Hence the false reject ratio is high.

Mode 2: The absence of user check moves into loop that of phase 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 Sfinal , 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 Sfinal falls below threshold for managing such situation another count value named tcount is calculated along with count value this tcount value can reauthenticate 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.

5: RESULTS AND COMPARISON

- ***Registration of face biometric data :***

The system registers face biometric data. Here PCA based face recognition is used, 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.

Mode 1 results:

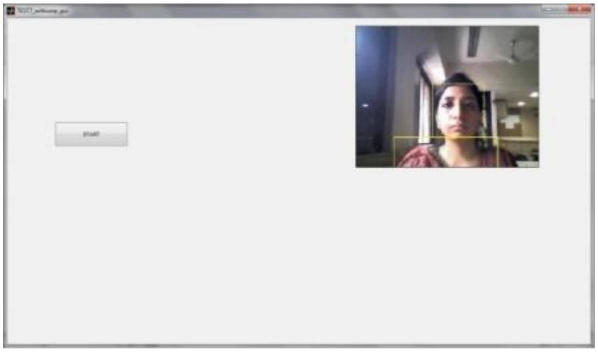

Figure 2. Phase 1.

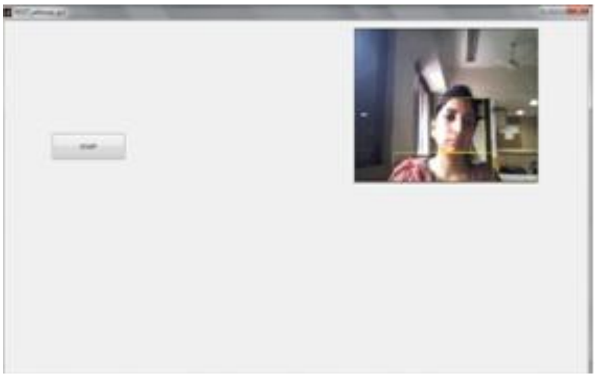

Figure 3. Phase 2 & Phase 3

Phase 4 results are unpredictable due to lack of robustness to user's posture.

Mode 2 results:

- ***Phase 2 & Phase 3***

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

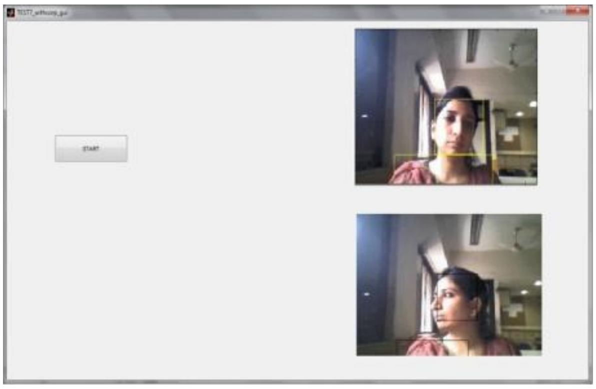

Figure 4. User being monitored even in varying posture.

- ***Phase 4:***

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

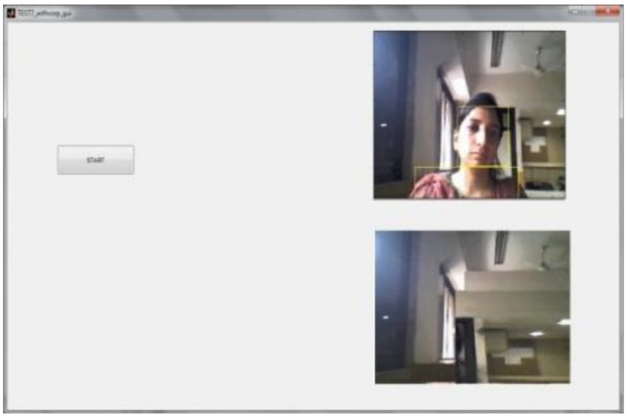

Figure 5 .No detection in case user is absent

Observed similarity score in Mode 1 and Mode 2 for following posture of user

A. Turn left
B. Straight
C. Turn right
D. Walk away
E. Come back before count=10

Mode 1:

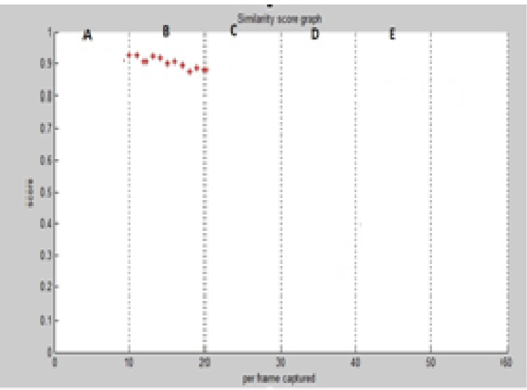

Figure 6: No similarity score in absence of biometric features

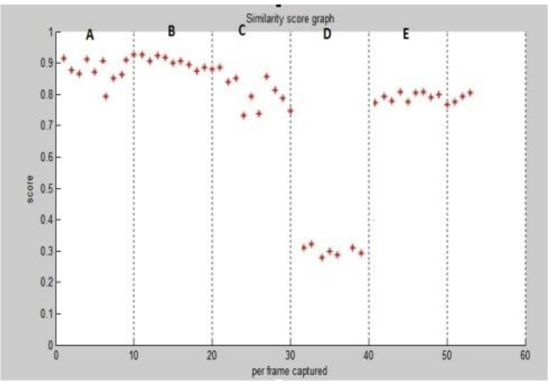

Figure 7 Graph for similarity score per frame captured

Observed similarity score for following posture of user

A. Turn left
B. Straight
C. Turn right
D. Walk away
E. Log off

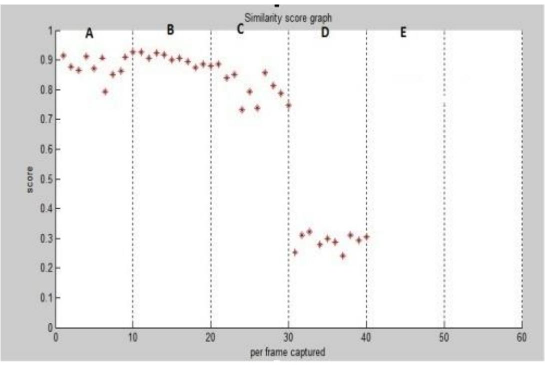

Figure 8. Graph for similarity score per frame captured.

Final analysis:

Mode 1:

Scenario	FRR	FAR
A. Turn head to the left.	No biometric features	
B Sit straight	=0% (0/25)	=0% (0/25)
C Turn head to the right.	No biometric features	
D Lean back in the chair.	=70%	=70%
E Walk away	Unpredictable	

Mode 2:

Scenario	FRR	FAR
B. Turn head to the left.	=0% (0/25)	=0% (0/25)
B Sit straight	=0% (0/25)	=0% (0/20)
C Turn head to the right.	=0% (0/25)	=0% (0/25)
D Lean back in the chair.	=0% (0/25)	=0% (0/25)
E Walk away	=0% (0/25)	=0% (0/25)

6. CONCLUSION

For a continuous monitoring system, observing user's presence in front of console is the great task which is achieved using soft biometric features achieving almost 100% results compared to conventional biometric systems. Along with this system usability, robustness, security is also maintained. Hence it can be concluded that the use of soft biometric traits for continuous authentication satisfies these criteria and also authenticates users regardless of their posture in front of the workstation (laptop or PC). Many studies on continuous authentication use multimodal biometrics[7], but none of these studies can identify the user in the absence of biometric observation. Overall, the use of soft biometric traits for continuous authentication shows promise. Preliminary tests demonstrate that the system is able to continuously authenticate a user despite posture changes

7. 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.

8. ACKNOWLEDGMENTS

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

9. 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] Nida Jawre, Kiran Bhandari ,"Use authentication using temporal information", IJAET.

[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, Visvanathan Ramesh and Peter Meer, "Kernel-Based Object Tracking,"

[14] Kresimir Delac **,** Mislav Grgic, "A Survey of biometric recognition methods".

[15] Koichiro Niinuma, Anil K. Jain, "Continuous User Authentication Using Temporal Information".