International Journal of Infinite Innovations in Technology|ISSN:2278-9057
IJIIT|Volume-IV|Issue-II|2015-2016 October|Paper-04
Reg. No.:20150904|DOI:V4I2P04

Continous User Authentication

Dr.Manjusha Deshmukh, Ms.Jayshree K,, Ms.Preeti Lodaya, EXTC Department

Abstract- **Security has always been a very important aspect, whether it may be personal or commercial usage. Normally systems have passwords for login to deter unwanted users from logging into the system. Experience tells us now that authenticating a user only at initial login session is not sufficient to keep off malicious intentions. A user may access the data from the system till the authenticated user logs out. Such problems are encountered probably when user takes a short break or when the user may not have logged out due to some reason. This is a critical issue as far as security is concerned especially for systems holding confidential information. In order to overcome this problem this paper proposes a continuous authentication scheme with continuous monitoring of the user. The proposed system uses soft biometric traits like face recognition, skin colour and the user's clothing. This system automatically enrolls soft biometrics every time user logs in and fuses matching of soft biometric with conventional authentication namely the password and face biometrics. The proposed system will have a good tolerance if the user's posture is mostly static when he or she is using the system.**

*Keywords**: Authentication, soft biometrics, passwords, face recognition, skin colour.***

I. INTRODUCTION

Computer security is a wide concept that encompasses almost any software or hardware that is designed to prevent the loss or theft of electronic data. It is important for a number of reasons, but perhaps, principally, as a means of keeping information safe. Most of the time, the term "computer security" refers to the security of a computer's insides. The data and compendious information, that most users store on their hard drives, is often far more valuable than the machines themselves. Broadly speaking, the importance of computer security lies in how harmful it can be if that data is lost.

Mostly people perceive computer security in a corporate or business context. Companies often store a lot of very sensitive information electronically, including trade secrets, customer lists and extensive corporate documents, both finished and those in progress. The importance of computer security is obvious in these contexts. It is perhaps less obvious for home computer users, but it is no less essential.

Computers are not inherently open to risks such as hacking or data breach. In order for outsiders to get into a computer, that computer must somehow open itself up to intrusion. Internet activity is the primary highway for these transactions. Many computer users do not realize that simply accessing the web could make their computers more vulnerable.

User authentication is a process that allows a device to verify the identity of someone who is using the system. For the security of the Computer and network system, user authentication is mandatory. Current methods like password or token based security are very popular but have a number of flaws like passwords can be forgotten, stolen or hacked. It is very common in several instances we notice people using very simple passwords like first name, birthdates, 1234567etc.or use same passwords across different applications as a solution to forgetting passwords. Also complex passwords are difficult to remember, though they are more secure. Similarly in token based method the token can be stolen or made duplicate for misuse. And the above methods authenticate the user only at initial stage once the system is logged into, there is no security till the user logs out. Biometric based authentication system offers several advantages over traditional password and token based authentication methods. Also the biometric systems raise several privacy concerns. A biometric authentication system is permanently associated with a user and cannot be changed or modified.

Authentication only at initial login is not sufficient, since anybody can access the system if the user leaves the system without logging off, to a take break or forgets to logout due to some reason. Thus to overcome this problem continuous user authentication is very important. A new method for continuous user authentication that continuously collects soft biometric traits is introduced.

Biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes.

Biometric is a physiological or behavioral characteristics of human being that can distinguish one person from another and that theoretically can be used for identification or verification.

Soft biometrics traits are physical, behavioral or adhered human characteristics, which have been derived from the way human beings normally distinguish their peers (e.g. height, gender, hair color). Those attributes have a low discriminating power, thus not capable of identification performance; additionally they are fully available to everyone which makes them privacy-safe. The method used automatically registers the user every time the user logs in by combining conventional password with soft biometric traits or face recognition method.

3 LITERATURE REVIEW

Yan Zhao described that Image hashing is the technique used for authentication. Hashing is extracting some features from image & authenticating by comparing that features, author has described different methods of authentication. Both global and local features are used and have tried to provide good efficiency with short image hash [1]. Che-Wei Lee described that a new blind image authentication method with a data repair capability for binary-like grayscale document images based on secret sharing has been proposed. Both the generated authentication signal and the content of a block have been transformed into partial shares [2]. A practical method for a noncontacting and real-time feature extraction for personal authentication is proposed using finger and palm feature extraction method. This is the traditional method for authentication [4]

Judith Liu-Jimenez has shown the case of high security environments, where low error rates are extremely important, the microprocessor solution is recommended, especially when the number of users in the system is relatively high; however, if the number of users is lower size and execution times are significant constraints, the dedicated hardware solution should be chosen [6]. Konstantinos Moustakas presents a novel framework for gait recognition augmented with soft biometric information. Geometric gait analysis is based on Radon transforms and on gait energy images. User height and stride length information is extracted and utilized in a probabilistic framework for the detection of soft biometric features of substantial discrimination power[7].

Different methods of continuous user authentication have been shown in [7]-[14] hard biometric and soft biometric are the different methods used for authentication hard biometric has the advantage of less memory required while the possibility of error increases in hard biometric and efficiency is less, on the other hand soft biometric has good efficiency.

Research on biometric methods has gained renewed attention in recent years brought on by an increase in security concerns. Many biometric techniques have been developed and are being improved with the most successful being applied in everyday law enforcement and security applications. Biometric methods include several state-of-the-art techniques. Among them, fingerprint recognition is considered to be the most powerful technique for utmost security authentication.

The term “Biometrics” is derived from the Greek words “bio” (life) and “metrics” (to measure) (Rood and Hornak, 2008). Automated biometric systems have only become available over the last few decades, due to the significant advances in the field of computer and image processing.

2.PROBLEM DEFINITION

In computer security generally password are used or token which can be easily stolen or forgotten. So system is less secure along with that, only initial authentication for a system is not sufficient, data can be access by unauthorized user in absence of valid user. authenticating a user only at initial login session is not sufficient. A user may access the data from the system until the initial user logs out. This problem normally occurs when user takes a short break or user may have not logged out due to some reason. This could be a critical problem for security especially for systems holding confidential information So continuous authentication is required especially for system carrying very confidential information. Few continuous authentication systems are being introduced, where preregistration of soft or hard biometric is required. Similarly there may be problem in finger print biometric that it is showing false result for actual user or detecting true result for invalid user.

4. METHODOLOGY

The Figure 4.1 shows the process flow, Mode I to Mode II arrow represents process flow and all other arrows represent possible transitions when appropriate conditions are met. Security is very important aspect nowadays; it may be for personal or commercial use. Normally in a system whenever we login there is password which is our security to prevent unwanted user to login in our system.

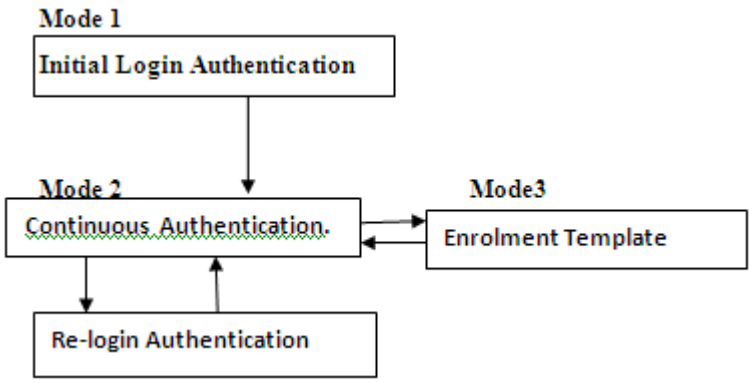

Fig 4.1: Continuous authentication

But authenticating a user only at initial login session is not sufficient. A user may access the data from the system until the initial user logs out. This problem normally occurs when user takes a short break or user may have not logged out due to some reason. This could be a critical problem for security especially for systems holding confidential information. In order to overcome this problem a continuous authentication scheme is proposed further where continuous monitoring and authentication of login user occurs. The proposed system uses a soft biometric trait like facial skin and users clothing. This system automatically enrols soft biometrics every time user login and fuses matching of soft biometric with conventional authentication namely password and face biometric.

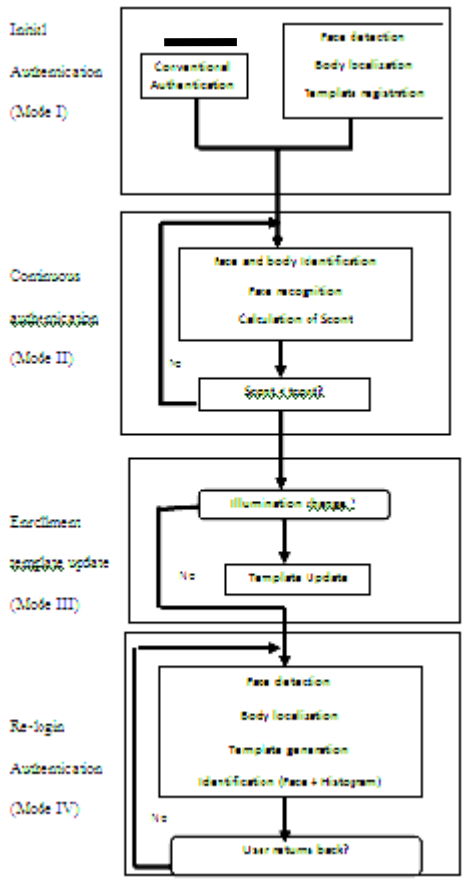

Fig 4.2: Flow chart of Continuous Authentication

5.1 Initial login Authentication

Initially when user will login he will be using normal login method like password or token based method but generally password based method is used and during that time the soft biometrics traits of those users will be saved like facial skin, clothing colour. It is being assumed that user is looking in front direction during login, this is reasonable assumption since the person is normally expected to look in front while login. Haar classifier is used for face detection.

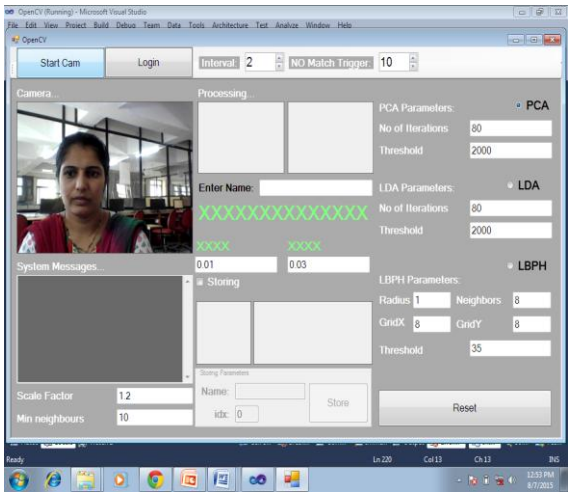

Fig 4.3: Camera On

Haar-like features are digital image features used in object recognition. They owe eir name to their intuitive similarity with Haar wavelets and were used in the first real-time face detector. Location and size of user face is estimated with respect to the face.

Face localization

Face Detection using Haar Cascades.

We will see the basics of face detection using Haar Feature-based Cascade Classifiers.

We will extend the same for eye detection etc.

Object Detection using Haar feature-based cascade classifiers is an effective object detection method proposed by Paul Viola and Michael Jones in their paper, "Rapid Object Detection using a Boosted Cascade of Simple Features" in 2001. It is a machine learning based approach where a cascade function is trained from a lot of positive and negative images. It is then used to detect objects in other images.

Here we will work with face detection. Initially, the algorithm needs a lot of positive images (images of faces) and negative images (images without faces) to train the classifier. Then we need to extract features from it. For this, haar features shown in below image are used. Each feature is a single value obtained by subtracting sum of pixels under white rectangle from sum of pixels under black rectangle.

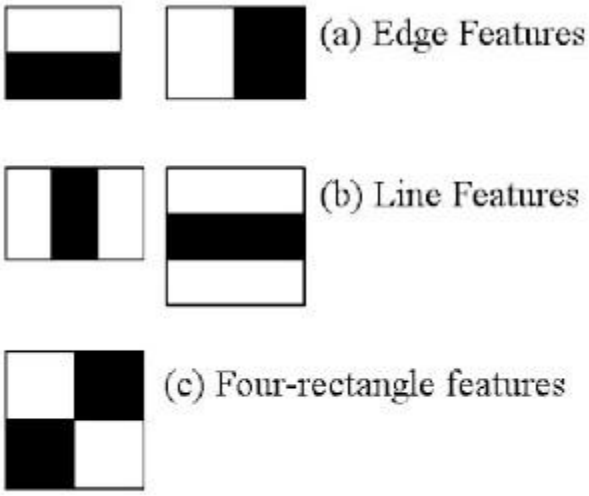

Fig 4.4: Haar features

Now all possible sizes and locations of each kernel is used to calculate plenty of features. For each feature calculation, we need to find sum of pixels under white and black rectangles. To solve this, the integral images are introduced. It simplifies calculation of sum of pixels, how large may be the number of pixels, to an operation involving just four pixels. It makes things super-fast.

But among all these features we calculated, most of them are irrelevant. For example, consider the image below. Top row shows two good features. The first feature selected seems to focus on the property that the region of the eyes is often darker than the region of the nose and cheeks. The second feature selected relies on the property that the eyes are darker than the bridge of the nose. But the same windows applying on cheeks or any other place is irrelevant. So selection of relevant face is achieved.

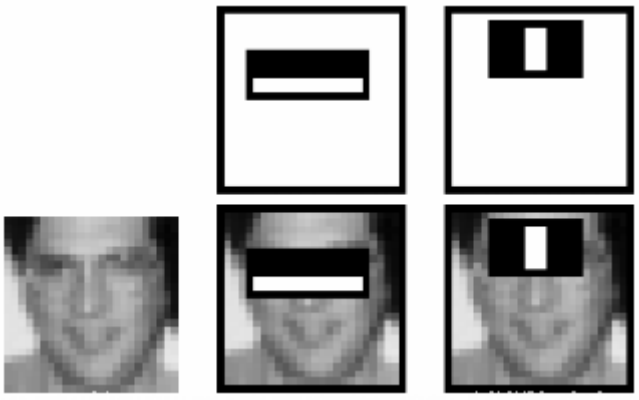

Fig 5.5: Training images

For this, we apply each and every feature on all the training images. For each feature, it finds the best threshold which will classify the faces to positive and negative. But obviously, there will be errors or misclassifications. We select the features with minimum error rate, which means they are the features that best classifies the face and non-face images. The process is not as simple as this. Each image is given an equal weight in the beginning. After each classification, weights of misclassified images are increased. Then again same process is done. New error rates are calculated also new weights. The process is continued until required accuracy or error rate is achieved or required number of features are found.

Final classifier is a weighted sum of these weak classifiers. It is called weak because it alone can't classify the image, but together with others forms a strong classifier. Even 200 features provide detection with 95% accuracy. Their final setup had around 6000 features. (Imagine a reduction from 160000+ features to 6000 features. That is a big gain).So now you take an image. Take each 24x24 window. Apply 6000 features to it. It is less time consuming.In an image, most of the image region is non-face region. So it is a better idea to have a simple method to check if a window is not a face region. If it is not, discard it in a single shot. Don't process it again. Instead focus on region where there can be a face. This way, we can find more time to check a possible face region.

For this they introduced the concept of Cascade of Classifiers. Instead of applying all the 6000 features on a window, group the features into different stages of classifiers and apply one-by-one. (Normally first few stages will contain very less number of features). If a window fails the first stage, discard it. We don't consider remaining features on it. If it passes, apply the second stage of features and continue the process. The window which passes all stages is a face region.

Authors' detector had 6000+ features with 38 stages with 1, 10, 25, 25 and 50 features in first five stages. (Two features in the above image is actually obtained as the best two features from Adaboost). According to authors, on an average, 10 features out of 6000+ are evaluated per sub-window.OpenCV comes with a trainer as well as detector. If you want to train your own

classifier for any object like car, planes etc. you can use OpenCV to create one. Its full details are given here: Cascade Classifier Training.

Here we will deal with detection. OpenCV already contains many pre-trained classifiers for face, eyes, smile etc. Those XML files are stored in opencv/data/haarcascades/ folder. Let's create face and eye detector with OpenCV.First we need to load the required XML classifiers. Then load our input image (or video) in grayscale mode. Now we find the faces in the image. If faces are found, it returns the positions of detected faces as Rect(x,y,w,h). Once we get these locations, we can create a ROI for the face and apply eye detection on this ROI

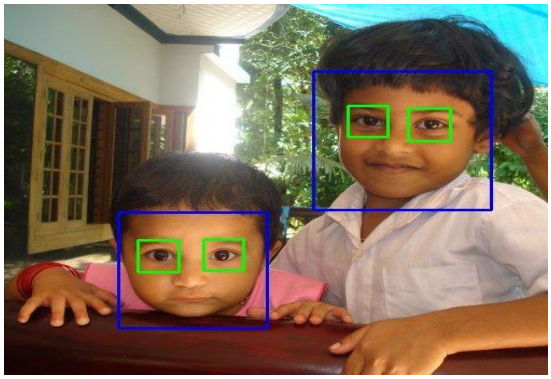

Fig 4.6 Face and eye detection

5.2 Mode II: Continuous authentication

The system keeps on Authenticating the user by soft face and clothing enrolment template stored during initial login authentication. System status changes to mode III that is enrolment template update when ever it recognize that user is no longer in front of Console. This mode consist of Face Recognition using color histogram & PCA method.

- Face & body Identification using color histogram

  Mean shift algorithm is being used to track the face and body separately based on histogram registered in first mode and calculating similarities between the current histogram and registered histogram.

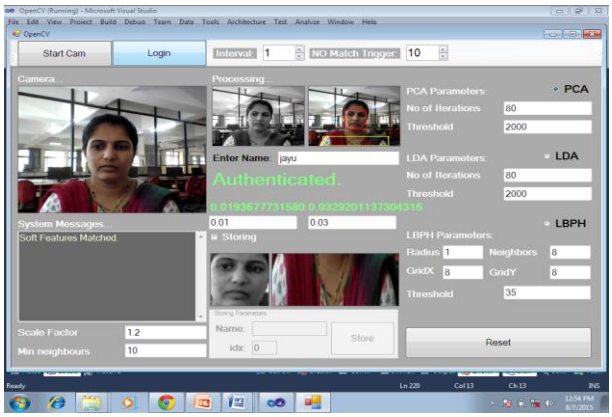

Fig. 4.7: Verified and authenticated

- Face Recognition

  PCA based face recognition technique is used to extract the facial features. Face recognition is executed at regular interval. Principal Components Analysis (PCA) is a mathematical formulation used in the reduction of data dimensions. Thus, the PCA technique allows the identification of standards in data and their expression in such a way that their similarities and differences are emphasized.

- Computing the final similarity

  The system calculates the final similarities, if it is below the threshold then the system enters the mode III to check whether it is due to change in ambient illumination or users absence in front of console.

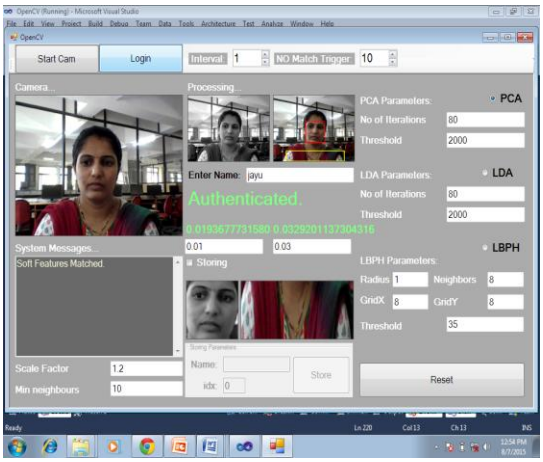

Fig 4.8 Soft features matched

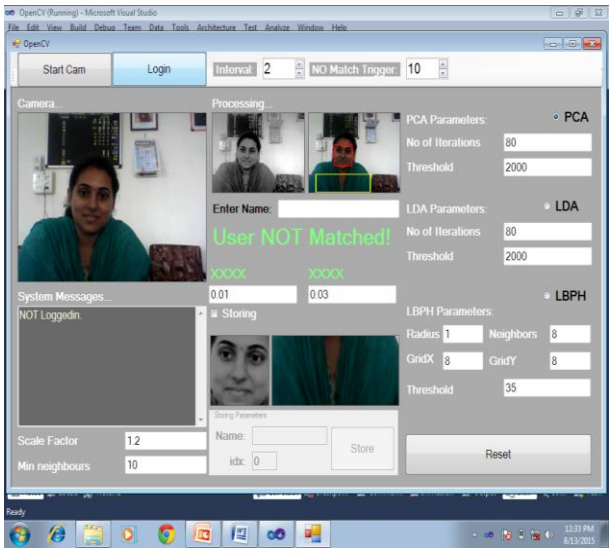

Fig 4.9 Soft features not matched & not loggin

5.3 Mode III Enrollment Template update

The system enters in this mode whenever Scount falls below threshold value. This mode is introduce to reduce the false rejection caused due to illumination change or any change in background. This process consist of

- Illumination change detection.

When Scount is lower than Threshold in mode II, system checks whether:

User is no longer in front of console.

Or

Their has been change in illumination.

Illumination change is detected by a well known and very easy method of image subtraction. A pair of image one just before and one immediately after the time are compared. If the difference image shows intensity difference all over the image than it is decided that their has been an illumination change.

- Enrolment template update

When an illumination change is detected, we update users biometric template.

5.4 Mode IV Relogin authentication

The status moves to this mode every time the system detects that user is no longer in front of console. In this mode system is locked and it tries to detect user and reauthenticate him automatically. If the system detects a user and reauthenticate user as genuine status moves to mode II.

6 CONCLUSION

User authentication is very important for security of computer and network system. In the traditional methods after the initial login the system is not secured until it is logout. A new frame work is proposed where continuous user authentication is done. New enrolment templates are updated every time the user logs in, both color of the cloth and face are being used for authentication. It is the process that allows the device to verify the identity of someone who is using the system. The proposed method can be used to prevent the confidential data of the system to be access by the unauthenticated user.

7 REFERENCES

[1] Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao, "Robust Hashing for Image Authentication Using Zernike Moments and Local FeaturesInformation," *in Proc.* Vol. 8, no. 1, January 2013.

[2] Che-Wei Lee, Student Member, IEEE, and Wen-Hsiang Tsai, Senior Member, IEEE" A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image With a Data Repair Capability" *IEEE transactions on image processing*, vol. 21, no. 1, january 2012.

[3] Weimin Wei, Shuozhong Wang, Xinpeng Zhang, and Zhenjun Tang," Estimation of Image Rotation Angle Using Interpolation-Related Spectral Signatures With Application to Blind Detection of Image Forgery" *IEEE transactions on information forensics and security*, vol. 5, no. 3, september 2010

[4] Junta Doi, Member, IEEE, and Masaaki Yamanaka," Discrte Finger and Palmar Feature Extraction for Personal Authentication." *IEEE transactions on instrumentation and measurement*, vol. 54, no. 6, december 2005.

[5] Ana M. Guzman, Mohammed Goryawala, Jin Wang, Armando Barreto, Jean Andrian, Naphtali Rishe,and Malek

Adjouadi." Thermal Imaging as a Biometrics Approach to Facial Signature Authentication" *IEEE journal of biomedical and health informatics,* vol. 17, no. 1, january 2013.

[6] Judith Liu-Jimenez, Student Member, IEEE, Raul Sanchez-Reillo, Member, IEEE, and Belen Fernandez-Saavedra, Student Member, IEEE," Iris Biometrics for Embedded Systems" *IEEE transactions on very large scale integration (vlsi) systems,* vol. 19, no. 2, february 2011.

[7] Konstantinos Moustakas, Member, IEEE, Dimitrios Tzovaras, Member, IEEE, and Georgios Stavropoulos," Gait Recognition Using Geometric Features and Soft Biometrics*" IEEE signal processing letters,* vol. 17, no. 4, april 2010.[8] A. Altinok and M. Turk, "Temporal integration for contnuous 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] Yao-Chung Lin, David Varodayan, Member, IEEE, and Bernd Girod, Fellow, IEEE" Image Authentication Using Distributed Source Coding" *IEEE Transactions On Image Processing*, vol. 21, no. 1, 2012.

[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., 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.