A Biometric Approach for Continuous User Authentication by Fusing Hard and Soft Traits

A. Prakash
(Corresponding author: A. Prakash)

Department of Computer Science and Engineering, Hindustan University, Chennai, India
(Email: prakash1712@yahoo.com)
(Received Mar. 21, 2012; revised and accepted Sep. 21, 2012)

Abstract

Most existing computer and network systems authenticate a user only at the initial login session. This could be a critical security weakness, especially for high-security systems because it enables an impostor to access the system resources with the initial access permission. To address this security flaw, Continuous authentication of the user is necessary, to continuously monitors and authenticates the user throughout the session. Existing continuous authentication schemes primarily uses hard biometric traits, which is inconvenient to the user. To mitigate this problem, a new continuous user authentication scheme is designed to authenticate the user irrespective of their posture in front of the system. The system continuously monitors the user by using soft biometrics (color of user's clothing and facial skin) along with hard biometrics. It automatically registers soft biometric traits every time the user logs in and fuses soft biometric matching with the conventional face biometric authentication.

Keywords: Biometrics, continuous authentication, face recognition, hard traits, soft traits

1 Introduction

User authentication is extremely important for computer and network system security. Currently, knowledge-based methods (e.g., passwords) and token-based methods (e.g., smart cards) are the most popular approaches. However, these methods have a number of security flaws. Passwords can be easily shared, stolen, and forgotten. Similarly, smart cards can be shared, stolen, duplicated, or lost. To circumvent these issues, a number of login authentication methods, including textual and graphical passwords, public key infrastructure (PKI), and biometric authentication, have been utilized. All of the above login methods share a common problem, namely, they authenticate a user only at the initial log-in session and do not re-authenticate a user until the user logs out or there is a substantial time interval between user's activities on the workstation. This could pose a critical security weakness not only for high-security systems, but also for personal computers in a general office environment. Anyone can access the system resources if the initial user does not properly log out or the user leaves the workstation unattended to take a short break without logging out.

To resolve this problem, the system must continuously monitor and authenticate the user after the initial login session. The available methods for continuous authentication are limited. For example, systems that request a user to frequently enter his password for continuous authentication are irritating to the user. The method of limiting user's privilege depending on the availability of hard biometric is also not satisfactory; the user will face the inconvenience with limited privilege whenever the system fails to acquire the user's hard biometric trait. A number of studies on continuous user authentication have been published. These schemes typically use one or more primary (hard) biometric traits (e.g., fingerprint or face). They captured the user's face and fingerprint with a camera and a mouse with a built-in fingerprint sensor, respectively. While they showed promising authentication results, their system suffered from low availability of the biometric traits. For example, when a user is typing or entering a document, she often needs to turn her head away from the camera.

Another situation where face image is not properly captured is when the user takes a break from typing to read paper documents and does not look directly at the camera. Similarly, fingerprint can only be authenticated when the user keeps his finger on the reader embedded in the mouse. In some places the user was continuously monitored based on keystroke dynamics, but requires large training to the system and also suffers as the users typing speed varies from time to time. To overcome the problem of availability Soft biometrics like user face color, clothing color and hair color are used to monitor the user. Those systems face difficulty under the situation where all the employees having uniform dress color. In order to address the above problems a new frame work is developed which uses robust face recognition for initial login authentication and registers the soft biometrics of user, monitors the user based on registered traits and verify the user using hard biometric at specific interval to ensure continuous authentication and to provide re-authentication.

2 Related Work

In Face Recognition Zhen Lei et al., [13] proposed a method to detect the face by considering scale and orientation, Koichiro Niinuma et al., [16] et al., introduced the concept of soft traits to continuously monitor the user, Yu-Ting et al., [17] proposed an algorithm to detect the face in Complex background environment, Z.Lei et al., [12] used the local gabor texons to recognize the face, T.Ahonen et al., [1] used the local binary patterns to describe the face, W.CZhang et al., [21] used local gabor binary patterns to recognize the face.

For continuous monitoring, Solami et al. [19] used feature selection technique to reflect the user typing behaviour by using n-graph, but the systems requires high level of training, Moni et al. used face recognition with on-demand fingerprint recognition for remote authentication [15], Sim et al. [9] performed continuous verification with multimodal passive biometric traits of face and fingerprint, these systems provide higher security level but suffered under availability problem. Kurkovsky et al. [10] proposed a location-aware continuous authentication which uses face features along with location information, requires cost and are complex. Brosso et al. [3] used context information to analyse user behaviour by utilizing neuro and fuzzy logic. Shengrong Bu et al. [4] used biometrics for protecting mobile adhoc networks by partially observable markov decision process on biometric features. Shen et al. [18] proposed a modified remote authentication by using smart cards, Lee et al. [11] discussed the security scheme for wireless environments, I-En Liao et al. [14] introduced the password authentication scheme to protect the insecure networks, Zhang et al., [22] applied multi biometric based encryption to ensure authentication, Bromme et al. [2] explored the risk analysis of using biometric authentication, Christos Dimitriadis et al. [6] proposed a biometric authentication protocol for 3G mobile networks. All the above methods provide high level of security by providing continuous monitoring and verification, but all these systems requires some sort of users co-operation to authenticate the user. The objective of the proposed framework is to authenticate the user without their co-operation, i.e., irrespective of user's posture in front of the system. The rest of this paper is organized as follows: Section 3 describes the Soft Biometric approach, Section 4 introduces the proposed framework, Section 5 provides the experimental results. Finally Section 6 includes conclusion.

3 Soft Biometrics

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". These traits include gender, ethnicity, color of eye/skin/hair, height, weight, and SMT (scars, marks, and tattoos).

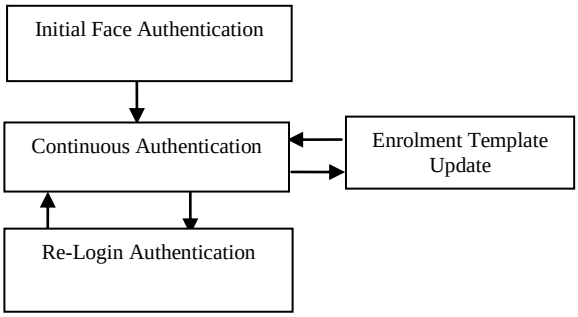

Figure 1: Framework for continuous authentication

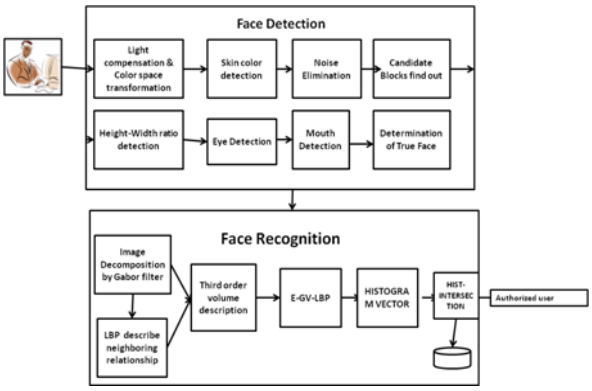

Figure 2: Face recognition

While soft biometric traits do not have sufficient discriminatory information to fully authenticate the user. However, in this frame work, soft biometric has been used to monitor user who logged in, here it acts as like a session key.

4 Proposed System and Its Modules

We propose a versatile framework combining hard and soft biometrics to provide continuous authentication of the user. We initially authenticate the user by conventional face recognition and registers a new template (color histogram of a user's clothing and face), to monitor the user. In case of any variations in soft biometrics, the system checks for hard biometric verification. If both traits differ, system treats user as imposter and moved to logoff state. When the system finds authorized user, by verifying hard biometric allows the user by re-authentication to continue. The proposed framework consists of four modes as described in Figure 1.

4.1 Initial Login – Authentication (Mode I)

In this mode I, the user is authenticated based on their facial feature. The Figure 2 shows the architecture for face recognition mode of the system.

4.1.1 Face Detection

When the user sits before the system the webcam application runs automatically and a snapshot of the running videos is taken. That image is then passed to the lighting compensation and color space transformation block where skinny and non skinny layers are separated and the RGB to YC_bC_r color space transformation is being done. Now the image is in the pipeline for the third block where skin color detection takes place. Then high frequency noises are removed by using a low pass filter (a 5 x 5 mask). After performing the low pass filter skin color blocks are identified. After this face localization step we can get several regions which may be human face. Then, the feature of height to width ratio, mouth, and eyes are detected sequentially for every candidate block. Then mouth and eye detection takes place and at finally a true face is determined.

4.1.2 Face Recognition

The Cropped face image is first decomposed into different scale and orientation responses by convolving multi-scale and multi-orientation Gabor filters. Second, local binary pattern analysis is used to describe the neighbouring relationship not only in image space, but also in different scale and orientation responses, thus forming third order Gabor volume (Figure 3) based LBP. The length of the histogram vector is reduced by the effective formulation of E-GV-LBP. This way, information from different domains is explored to give a good face representation for recognition. Discriminate classification is then performed based upon weighted histogram intersection techniques and results whether the user is authenticated user or not.

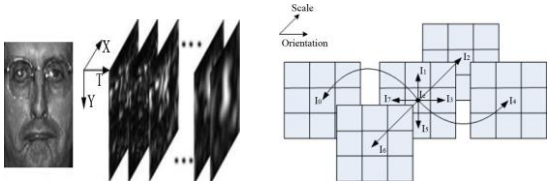

Figure 3: (a) Face image and its Third order volume (b) Formulation of E-GV-LBP

There are mainly three advantages of this representation. First, Gabor feature is applied to the face images to alleviate the variations of facial expression and illumination. Second, the LBP is utilized to model the neighboring relationship jointly in spatial, frequency and orientation domains. In this way, discriminate and robust information, as much as possible, could be explored. The uniform pattern mechanism is then presented to improve the efficacy of the proposed representation. Third, a feature selection and discriminate analysis method is introduced to make the face representation compact and effective for face recognition.

4.1.3 Body Localization & Template Enrollment

Location and size of the user's body with respect to his face are estimated based on the method of Jaffre and Joly [8]. Histogram of the face color (soft face), histogram of the clothing color, and the feature representation of the face (hard face) computed during login session are stored as enrollment templates. We quantize the RGB color space into 16*16*16 bins in order to generate the color histograms of face and clothing.

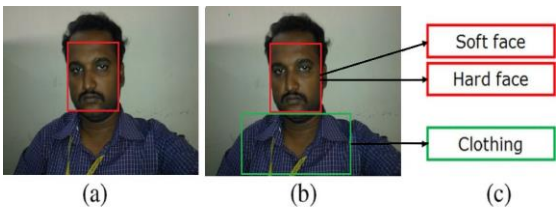

Figure 4: (a) Initial login (b) Body localization (c) registration

4.2 Continuous Authentication (Mode II)

Continuous authentication starts after login session. The system continuously authenticates the user by using the "soft face" and "clothing" enrolment templates registered in Mode I (initial login authentication, see Figure 4). Any time the system recognizes that the user is no longer present in front of the console, the system status changes to Mode III (enrolment template update). The continuous authentication mode consists of the following three steps.

4.2.1 Face and Body Identification Using Color Histograms

The system tracks the face and the body separately based on the histograms registered in Mode I by applying the mean shift algorithm [7], and calculating the similarities $S_{softface}$ and $S_{clothes}$ separately. The Bhattacharyya coefficient is used for calculating the similarity between two histograms. Face recognition is executed at regular intervals (5 secs).

4.2.2 Computing the Final Similarity

The system calculates the final similarity $S_{cont}.(S_{softface} + S_{clothes})$ If is below a threshold T_{cont}, the system enters Mode III to check whether it is due to the change in the ambient illumination or user's absence in front of the console.

4.3 Enrolment Template Update (Mode III)

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

4.3.1 Illumination Change Detection

When the $S_{cont}$is lower than T_{cont} in Mode II, the system checks whether: i) user is no longer in front of the console

or ii) there has been a change in the ambient illumination. We use the well-known and simple method of image subtraction to detect the illumination change. A pair of images, one just before and one immediately after the time when $S_{cont} < T_{cont}$ is used for image subtraction; the number of pixels that show a large difference in brightness between the two images is counted. If the difference image shows intensity differences all over the image, it is decided that there has been an illumination change.

Figure 5: Sample images from CALTECH database

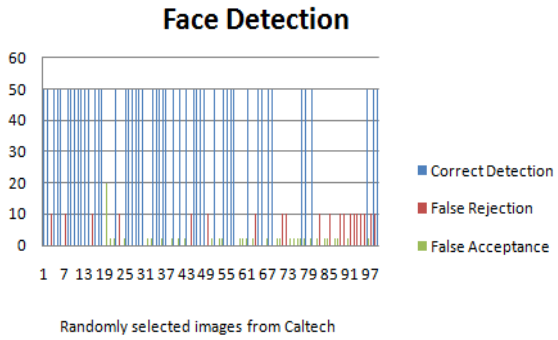

Figure 6: Evaluation parameters obtained from CalTech database

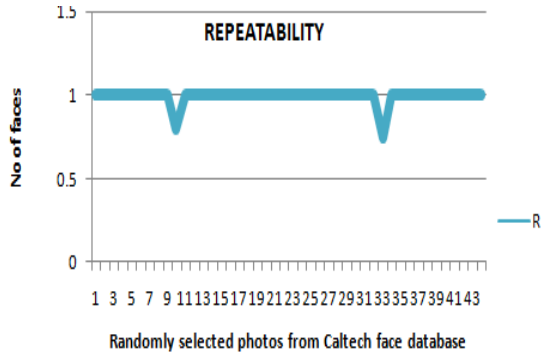

Figure 7 Repeatability obtained from CalTech DataBase

4.3.2 Enrolment Template Update

When an illumination change is detected, we update the user's biometric template to maintain successful continuous authentication in the modified operating environment.

4.4 Relogin Authentication (Mode IV)

The status moves to this mode every time the system detects that the user is no longer in front of the console. In this mode, the system is locked and it tries to detect the user and re-authenticate him automatically. If the system detects a user and re-authenticates the user as genuine, the status moves to Mode II again. The re-login authentication mode consists of four steps. Steps 1), 2), and 3) use the same procedures as used in Steps 2), 3), and 4) in Section III-A. In Step 4), the user is authenticated using both soft (color histograms) and hard biometrics (face). The similarity score is used for re-login authentication. There will be a small discontinuity in the values of soft biometrics when the imposter tries to replace the legitimate user. When there is a discontinuity in the similarity scores based on the soft biometric, the system enters re-login authentication mode. In the re-login authentication mode, the user must provide valid soft and hard biometrics. Imposters may be wearing similar clothes and face color, but it is highly unlikely that he will have similar hard biometric traits. Therefore, the re-login authentication is the method of deterring session hijacking in our system.

Figure 8: Sample images from INDIAN database

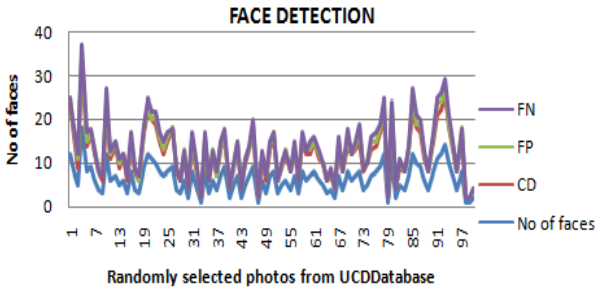

Figure 9: Evaluation parameters obtained from UCD face database

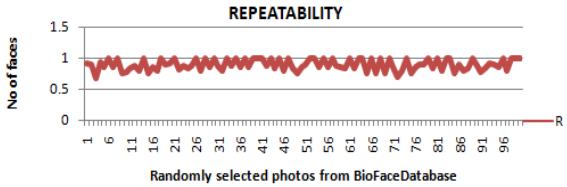

Figure 10: Repeatability obtained from UCD face database

5 Experiments

Experiments are carried out on different database to evaluate the performance of face detection and face recognition.

5.1 Evaluation of Face Detection

Evaluation parameters used for face detection includes, False negative-Number of faces that are not detected by face detection algorithm, False positive-Number of all non-faces that are detected as faces by face detection algorithm

and Correct detection-Number of faces that are correctly detected. Then Repeatability is given by,

$$Repeatabilty = \frac{Correct\ detection}{False\ positive + Correct\ detection}$$

5.1.1 Experiment on Caltech Face Database

The Caltech database created by California University includes 750 facial images. These images are in color and have a resolution of 640 × 480 (See Figures 5, 6, 7, 8, 9, and 10).

5.1.2 Experiment on UCD Face Database

The database consists of 216 color images and has been taken in different locations and at different day time which result in variable illumination conditions and taken at real time environment. In addition to the changes in illumination, the position of the subjects changes as well as their pose. Each image consists of from one face to thirteen faces. The resolution of the image is 556 x 430.

5.1.3 Analysis of Experimental Results

In Face Detection, the images with low illumination (<50 lux) are not able to identified, since it requires histogram of mouth and eye regions, the regions are even darker in dark pictures. Pose variations such as left turn and right turn are allowed, up to 45°, The face rotations above does provide much information about the face features.

Table 1: Evaluation result of face recognition on Indian database

Recognition rate(%)				
Parameters	Exp 1	Exp 2	Exp 3	Exp 4
Frontal pose	93.34	91.6	85.52	89.25
Left turn	87.77	96.67	80.25	78.54
Right turn	86.65	82.34	90.02	76.89
Smile	89.23	84.49	92.56	81.23
Sad	84.47	87.56	85.57	79.95
Neutral	93.35	94.72	86.62	85.26
Average	89.13	89.56	86.75	81.85

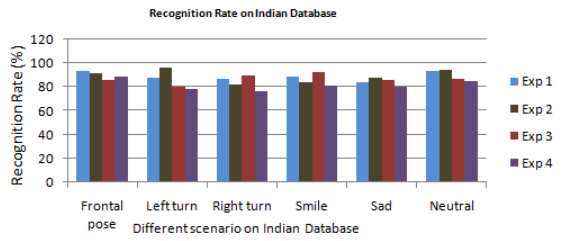

Figure: 11 Recognition rate on Indian database

5.2 Evaluation of Face Recognition System

5.2.1 Experiment conducted on Indian Database

Indian Database includes 660 images of 39 different males and 22 different females. The database considers images with different pose and expressions. The Recognition rate is calculated based on the following different experiments (See Table 1 and Figure 11).

Experiment 1: The Gallery set comprises of single face image of all the persons with neutral frontal pose, and tested with randomly selected images with variations in pose as left turn, right turn and expressions such as smile and sad.

Experiment 2: Two samples of each person with pose of left turn and with neutral are used to form the gallery set, and the remaining samples are used for testing.

Experiment 3: Two samples of each person with pose of right turn and with expression of smile is used as gallery set, and the remaining samples are used for testing. Testing samples comprises of images with different pose and different expressions.

Experiment 4: Gallery set is formed by selecting images randomly comprising single image of all the persons. Testing is performed with the remaining images.

5.2.2 Analysis on Experimental Results

The images with left or right rotations are misidentified as other persons, because the rotated face features of the images have some similarities in their histograms.

6 Conclusion

The new framework fuses hard and soft biometric traits for continuous user authentication. Soft biometrics like face and clothing color are registered every time the user is logged in and continuously authenticate the user based on their hard and soft biometrics. If the final similarity score falls below the threshold level, the system moves to locked state. Initial user authentication by using face biometrics is integrated with continuous monitoring to ensure the genuine user is using the system. The system authenticates the user irrespective of their posture, thus does not requires users active co-operation.

The re-login authentication allows the user to continue the session when the user appears again in front of the system, after a short break. The color variations due to light conditions are handled by enrollment template update. Once the session has been completed, as the user logs out, the soft biometrics of the user is removed to save the memory consumption. The use of the soft biometric also circumvents the situation when the availability of hard biometric trait is limited. The proposed tracking algorithm works well with various users' postures. The continuous user authentication system is tested with various users at different pose and expressions. The test results show that

the system is capable to successfully authenticate the user continuously irrespective of his posture, and the availability of traits reduced the false reject rate. The proposed system is evaluated in the routine operating environment and it results at only 2.67% of False Accept rate, which is at the acceptable level of security, cost and maintenance.

References

[1] T. Ahonen, A. Hadid, and M. Pietikainen, "Face description with local binary patterns: Application to face recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 2037-2041, Dec. 2006.

[2] A. Bromme, "A risk analysis approach for biometric authentication technology," *International Journal of Network Security*, vol. 2, no.1, pp. 52-63, Jan. 2006.

[3] I. Brosso, A. La Neve, G. Bressan, and W. V. Ruggiero, "A continuous authentication system based on user behavior analysis," in *International Conference on Availability, Reliability and Security*, pp. 380-385, Mar. 2010.

[4] S. Bu, F. R. Yu, X. P. Liu, and H. Tang, "Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks," *IEEE Transaction on Wireless Communications*, vol. 10, no. 9, pp. 3064-6073, Sep. 2011.

[5] D. Comaniciu and P. Meer, "Mean shift: A robust approach towardfeature space analysis," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 5, pp. 603-619, May 2002.

[6] C. K. Dimitriadis and S. A. Shaikh, "A biometric authentication protocol for 3g mobile systems: Modelled and validated using csp and rank functions," *International Journal of Network Security*, vol. 5, no. 1, pp. 99-111, July 2007.

[7] S. Gundimada, T. Li, and v. Asari, "Face detection technique based on intensity and skin color distribution," in *2004 International Conference on Image Processing*, vol. 2, pp. 1413-1416, Oct. 2004.

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

[9] S. Kumar, T. Sim, R. Janakiraman and S. Zhang, "Using continuous biometric verification to protect interactive login sessions," in *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005)*, pp. 441-450, 2005.

[10] S. Kurkovsky and E. Syta, "Approaches and issues in location-aware continuous authentication," in *13th IEEE International Conference on Computational Science and Engineering*, pp. 279-283, 2010.

[11] C. C. Lee, M. S. Hwang, and I. E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683-1687, Oct. 2006.

[12] Z. Lei, S. Z. Li, R. Chu, and X. Zhu, "Face recognition with local gabor textons," in *Proceedings of IAPR/IEEE International Conference on Biometic*, pp. 49-57, 2007.

[13] Z. Lei, S. Liao, M. Pietikäinen and S. Z. Li, "Face recognition by exploring information jointly in space, Scale and Orientation," *IEEE Transactions on Image Processing*, vol. 20, no. 1, pp.247-257, Jan. 2011.

[14] I. E. Liao, C. C. Lee, and M. S. Hwang, "A password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, vol. 72, no. 4, pp. 727-740, June 2006.

[15] A. Moini and A. M. Madni, "Leveraging biometrics for user authentication in online learning: A systems perspective," *IEEE Systems Journal*, vol. 3, no. 4, pp. 469-476, Dec.2009.

[16] K. Niinuma, U. Park and A. K. Jain "Soft biometric traits for continuous user authentication," *IEEE Transactions on Information Fo-rensics and Security*, vol. 5, no. 4, pp-771- 780, Dec. 2010.

[17] Y. T. Pai, S. J. Ruan, M. C. Shie, and Y. C. Liu, "A simple and accurate color face detection algorithm in complex background," *IEEE Conference on Image Processing*, pp. 1545-1548, Jan. 2010.

[18] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user autheentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 414-416, May 2003.

[19] E. A. Solami, C. Boyd, A. Clark, and I. Ahmed, "User-representative feature selection for keystroke dynamics," in *5th International Conference on Network and System Security*, pp. 229-233, Oct. 2011.

[20] www.ccs.asia.edu.tw/myjournal/index.htm

[21] W. C. Zhang, S. G. Shan, W. Gao, and H. M. Zhang, "Local gabor binary pattern histogram sequence (lgbphs): A novel non-statistical model for face representation and recognition," in *Proceedings of the IEEE International Conference on Computer Vision*, pp. 786-791, 2005.

[22] M. Zhang, B. Yang, and T. Takagi, "Multibiometric based secure encryption and authentication scheme with fuzzy extractor," *International Journal of Network Security*, vol. 12, no.1, pp. 50-57, Jan. 2011.

A. Prakash is working as Assistant Professor at Jerusalem College of Engineering, Chennai. He has received B.E and M.E degree in Computer Science and Engineering. He is currently pursuing Ph.D at Hindustan Institute of Technology and Science. His areas of research interests include Network Security and Image Processing.