Stride Towards Proposing Multi-Modal Biometric Authentication for Online Exam

A. Prakash[1,2], R. Dhanalakshmi[3]
(Corresponding author: A. Prakash)
Department of Computer Science and Engineering, Hindustan University[1]
Rajiv Gandhi Salai (OMR), Padur, Kelambakam, Chennai 603103, India
Information Technology, Jerusalem College of Engineering[2]
Velacherry Tambaram Main Road, Pallikkaranai, Chennai 600100, India
(Email: prakash1712@yahoo.com)
Department of Computer Science and Engineering, KCG College of Technology[3]
KCG Nagar, Rajiv Gandhi Salai, Karapakkam, Chennai 600097, India
(Received June. 7, 2015; revised and accepted Aug. 11 & Sep 5, 2015)

Abstract

Biometric authentication has been getting widespread attention over the past decade with growing demands in automated secured personal identification and has been employed in diverse fields. It ensures actual presence of biometric entity of a person in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem. Also in the previous work they use face and dress color as hard and soft biometric traits. The major drawback of the existing continuous authentication system is, it is able to successfully authenticate the user continuously with high tolerance to the user posture. So, to overcome this drawback and improve the systems robustness against illumination changes and cluttered background, in this paper we use additional biometric traits which are mole, ornament details and face dimensions in addition to the dress color and face color. Also, we extend it to the online exam application. That is, continuously monitoring of a person in an online exam is proposed employing hard biometric like facial recognition and soft biometrics. Modified PCA (Principal Component Analysis) is employed here for the facial recognition part. Both the hard biometric (face) and soft biometrics is fused with the help of optimization algorithm based similarity technique. Finally the authentication is performed and evaluated using standard evaluation metrics. The technique is implemented in MATLAB and will be compared to prominent existing techniques.

Keywords: Biometric traits, continuous biometric authentication, face recognition, MPCA, multimodal biometric systems

1 Introduction

The excellence of a biometric technique is assessed by means of its inherent competence in recognition, which is estimated using the bogus refutation and fake acceptance paces. The birth of the multimodal biometrics is brought about by the synthesis of the diverse biometric mode data at the trait mining, match score, or decision level [17]. One of the generally used biological features is the face recognition [18]. Face recognition has the aim of identifying individuals in photographs or videos from their facial appearance. When comparing is done with other biometrics, face recognition is found passive and does not necessitate supportive persons who are close to sensor or in contact with it. Human faces, automatic recognition are an aggressively investigated part, which discovers many applications such as surveillance, authentication or human-computer interaction. In universal and non-intrusive biometric, face is an effortlessly obtainable [17], which makes it perfect for applications where other biometrics such as fingerprints or iris scanning are not possible [13]. In pattern recognition system, the most focused area is face recognition. The face recognition rate will get affected due to variation of human face like different pose, illumination and different expression. Real-world automatic face recognition tackled these variations [14]. Under different illumination environment it is not simple to attain for robust face recognition. The variation of illumination causes changes in face appearance considerably, it discriminate that the difference between the changes in same face image due to illumination is higher than the variation due to change in face identity [10]. It is accepted by numerous that feature based face recognition systems hold guarantee in specific applications where movement can be utilized as a sign for face segmentation and tracking, and the vicinity of more information can

expand recognition execution. On the other hand, these systems have their own difficulties. They oblige tracking the video sequence, and recognition algorithms that have the capacity to incorporate data over the whole video. The capacity of diverse approaches to adapt to face posture and misalignment can be generally controlled by the measure of express geometric data they use in the face representations [10].

The fundamental objective of face recognition system is to divide the qualities of a face that are controlled by the intrinsic shape and color of the facial surface from the arbitrary states of image generation. Different methods were utilized for the face recognition methodology like Diffusion-Based Face Selective Smoothing in DCT Domain where impact of illumination changes on distinctive frequency subbands and propose a dissemination based image selective smoothing algorithm to eliminate the undesired impacts of illumination varieties [9]. Soft biometrics additionally has increased considerable significance. Soft biometric attributes are characterized as "those qualities that give some information about the individual, however fail to possess the peculiarity and perpetual quality to sufficiently separate any two individuals [11]. These characteristics incorporate sexual orientation, ethnicity, colour of eye/skin/hair, tallness, weight, and SMT (scars, marks, and tattoos). While soft biometric attributes do not have sufficient oppressive information to completely verify the client, it has been demonstrated that they can enhance system login security when consolidated with hard biometric characteristics [4].

2 Literature Review

Recently, a number of researches are being carried out in multi-biometric authentication area. A brief review of some of these researches is given in this section, especially related to facial recognition based authentication.

Galbally et al. [5] proposed security of biometric recognition frameworks by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The technique consisted of two phases namely, feature extraction phase and classification phase. In feature extraction phase, the features amounting to 25 of them were extracted. It included full reference based features and no reference based features. Subsequently, classification based on these features was carried out by the trained QDA classifier. The proposed technique was applied to Iris, Fingerprint and Face Recognition.

Chen et al. [3] had proposed a method for face recognition or authentication against pose, illumination, and expression (PIE) variation using modular face features. A sub-image in low-frequency sub-band was extracted by a wavelet transform (WT) to reduce the image dimensionality. It was partitioned into four sections for indicating to the local features and diminishing the PIE impacts, and the small image in a coarse scale was produced by means of the WT without losing the worldwide face features. Five measured feature spaces were developed. The most discriminative common vectors in each one feature space were found, and a nearest feature space-based (NFS-based) distance was ascertained for characterization. The weighted summation was performed to combine the five distances. Examinations were directed to demonstrate that the proposed method was better than traditional techniques.

Shermina and Vasudevan [1] had proposed a face recognition method that was robust to pose and illumination variations. For processing the pose invariant image, the Locally Linear Regression (LLR) method was used to create the virtual frontal view face image from the non frontal view face image. The low frequency components of Discrete Cosine Transform (DCT) were utilized to regularize the illuminated image during processing the illumination invariant image. The Fisher Linear Discriminant Analysis (FLDA) method and Principal Component Analysis (PCA) methods were implemented to identify the facial images with both pose variant and illumination variant. To be a last element the scores regarding FLDA and also PCA were being combined utilizing a hybrid approach based on the Feed Forward Neural Network (FFN). Scores obtained from the initial recognition method, the weight was allocated to the image. The authentication process of image was form on the weight assigned and the mixture of the scores. The experimental results determined that their proposed method based on hybridization technique recognizes the face image was efficiently than traditional method.

Ajay et al. [19] had compared the performance of various combinations of edge operators and linear subspace methods to determine the best combination for pose classification. To estimate the behavior, they had accomplished analysis on CMU-PIE database which had images with wide variation in illumination and pose. They established that the behavior of pose classification mainly dependent on the selection of edge operator and linear subspace method. From Prewitt edge operator and Eigen feature regularization approach the most excellent classification precision was attained. Adaptive histogram equalization was utilized as a preprocessing step to adapt illumination variation, which resulting into considerable improvement in performance.

Muruganantham [6] had proposed a method that offers an up-to-date evaluation of major human face recognition research. They presented a summary of face recognition and its applications. The face databases, explanation and restrictions which were used to evaluate the performance of these face recognition algorithms were given. The face recognition system was mostly affected by four significant factors; they were pose illumination, uniqueness, occlusion and facial expression. Here they anticipated a vital evaluation of the current researches related with the face recognition process. They proposed a wide review of most important researches on face recognition process accomplished on various scenarios. Additionally, abbreviation

portrayal of face recognition process in conjunction with the methods linked with the different factors that affected the face recognition process

Arindam et al. [12] had proposed a method for automatic face recognition by means of integrated peaks of the Hough transformed significant blocks of the binary gradient image. In this technique initially the gradient of an image was computed and a threshold was get on with it to obtain a binary gradient image, which was less responsive to noise and illumination changes. Secondly, major blocks were taken out from the absolute gradient image, to obtained pertinent information with the idea of dimension reduction. Lastly the most excellent fitted Hough peaks were taken out from the Hough transformed significant blocks for competent face recognition. These Hough peaks were joined together, which were utilized as feature in classification process.

Choudhary et al. [7] had proposed a method to label a Self-Organizing Map (SOM) to measure image similarity. In their work, into the neural network the facial images along with the regions of interest were introduced. After completion of training process, each neural block was tuned to a particular facial image prototype. Then, the probabilistic decision rule performed facial recognition. Their method provided very accurate results for face identification along with illumination variation and facial poses and facial expressions. From a single database onwards the SOM method was trained. A facial recognition system automatically recognized a person, which obtained from a digital image or video frame from a video source. It was applied in security systems and the analysis could be compared with other biometric recognition system like fingerprint or eye iris recognition systems.

Khourya et al. [16] were presented bi-modal biometric authentication on mobile phones in challenging conditions. They looked at the issue of face, speaker and bi-modal verification in mobile situations when there was critical condition disparity. They presented this disparity by selecting customer models on high quality biometric samples acquired on a laptop computer validating them on lower quality biometric examples gained with a mobile phone. To perform these tests they build up three novel authentication protocols for the expansive publicly available MOBIO database. They assessed state-of-the-art face, speaker and bi-modal validation methods and demonstrated that between session variability modelling utilizing Gaussian mixture models gave a reliably powerful system to face, speaker and bi-modal verification. It was likewise demonstrated that multi- algorithm combination gave a steady execution change to face, speaker and bi-modal authentication. Utilized the bi-modal multi- algorithm system they infer a state-of-the-art authentication framework that acquired a half total error rate of 6.3 % and 1.9 % for Female and Male trials, separately.

3 Problem Identification

There are several issues that threaten the security in biometric authentication systems. User authentication merely at the very first login session is one among these severe issues, which is normally found in majority of the currently available computer and network systems. This issue is a massively serious security issue, particularly in systems with high security requirement, since an imposter is permitted to access the resources in the system in the period between user log in and user log out.

Together with this, only using the face and dress color as biometric traits in continuous authentication system reduces the accuracy of the system under pose variations. Also, the previous continuous biometric system uses PCA for face recognition. But the PCA has various drawbacks such as, recognition rate is not high in case of images having different poses, facial expressions and change in illumination and also the accuracy rate is not high.

4 Proposed Continuous Biometric Authentication System

There are several issues that threaten the security in biometric authentication systems. User authentication merely at the very first login session is one among these severe issues, which is normally found in majority of the currently available computer and network systems. This issue is a massively serious security issue, particularly in systems with high security requirement, since an imposter is permitted to access the resources in the system in the period between user log in and user log out. Therefore, this paper introduces a continuous biometric authentication system, wherein, the system is observed incessantly from the time the user logs in. This system makes use of diverse user authentication modalities like face, ornaments, dress colour, beard, scars and mustache for monitoring the logged in user in a continuous manner. Moreover, the login security of this system is augmented through the union of hard as well as soft biometric traits. Figure 1 portrays the entire block representation of the proposed continuous multimodal biometric authentication system.

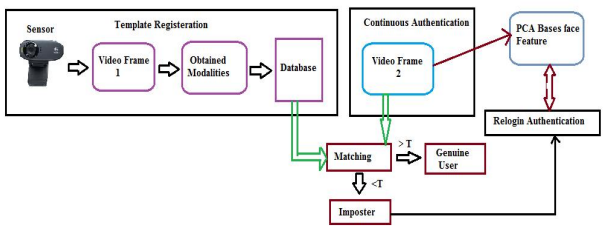

Figure 1: Block diagram of the proposed method

From the above figure, it is clear that the user's image is captured via a sensor in the beginning. Next, the de-

sired user authentication modalities are chosen from the sensor image and registered in the database. Face, ornaments, dress colour, beard, scars and mustache serve as the necessary modalities for authentication. This is then followed by the continuous authentication process, which is performed through the matching of the registered template and the subsequent video frame. Normalized cross correlation process is being utilized for carrying out the matching procedure. At the end of matching, the similarity score is produced from each and every modality. Later on, the Group Search Algorithm (GSO) with optimized weights aids in fusing these scores. Then, a threshold is preset to allow the authentication of the user as the genuine user or the imposter. A genuine user will be the authentication result, if the fused score exceeds the predetermined threshold. Otherwise, the presence of imposter is evident. In the proposed system, a remedy is provided for the situation with an imposter. Re-login authentication mode is that remedy, wherein, matching is accomplished with the application of the Modified principle component analysis (MPCA) on the face image. The following sections give a concise explanation of the proposed continuous biometric authentication system. There are totally three authentication subsystems available in the proposed system, namely, Initial login authentication, Continuous authentication and Re-login authentication.

All the subsystems in the continuous biometric authentication system have three modules each and they are the acquisition module, the feature extraction module and the matching module. An interface exists between the matching module and the database enclosing the templates. In this approach, whenever a user logs in, an enrollment template is freshly registered. So, temporal details such as color in the user's wear can also be used as the enrollment template. Two main processes are carried out here, namely, the training and the testing. The modalities of the user are gained by means of the sensor and the database stores them during the training phase. On the other hand, the stored template is utilized to perform the matching procedure at the time of testing. The vital processes involved during the period of initial login authentication and continuous login authentication are depicted in Figure 2.

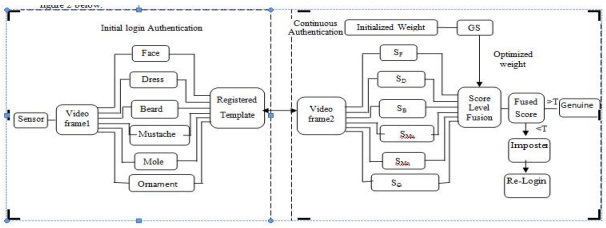

Figure 2: Initial and continuous authentication

4.1 Initial Login Authentication

The user employs the conventional authentication system for entering the system. Then, the sensor focuses the user's body for making the registration of the modalities like face, ornaments, color of clothing, mole, beard and mustache. During the period of training, the various poses of the user like turn head down, turn head to right, turn head to left, stretching the arms, quitting and leaning back in chair are caught due to the fact that the user may make movements or leave the spot. Training with these poses of the user can largely enhance the authentication system's accuracy.

4.2 Continuous Authentication

Mostly, the user templates are registered in a system only for particular time duration. In continuous authentication process, the template that is registered in the beginning and the second frame of the video are subjected to the matching process. Normalized cross correlation is utilized for deciding the likeness between the image and each one of the modalities.

4.3 Feature Matching Using Normalized Cross Correlation

The inspiration for employing cross correlation to handle template matching comes from the square Euclidean distance, which is given by,

$$D^2_{f,t}(u,v) = \sum_{x,y}[f(x,y) - t(x-u, y-v)]^2.$$

Where represents the image and the sum is over , subject to the window consisting of the feature located at. The expansion of is:

$$D^2_{f,t}(u,v) = \sum_{x,y}[f^2(x,y) - 2f(x,y)t(x-u,y-v) + t^2(x-u,y-v)]^2.$$

The expression $t^2(x-u, y-v)$ specifies a constant. If $f^2(x,y)$ is more or less constant, the rest of the cross-correlation terms will be:

$$c(u,v) = \sum_{x,y}[f(x,y)t(x-u,y-v)].$$

The above-mentioned equation offers the measure of how closely the image as well as the feature resemble. Few shortcomings are produced, when the above equation is employed for handling template matching. The first shortcoming is that the template matching with the above equation will not succeed, if the image energy $\sum f^2(x,y)$ alters with position. An example for this case is that the correlation existing among the feature and a precisely matching image area may be found to be smaller, when compared to the correlation between the feature and a bright region. In addition, the range of $c(u,v)$ relies on

the feature size. Further, the equation undergoes modifications with the variations in image amplitude, which are created due to the changes in illumination all throughout the image sequence. The aforementioned drawbacks can be tackled with the normalization of the image and feature vectors to unit length through the correlation coefficient, which in turn generates a correlation coefficient in the form of cosine.

$$\gamma(u,v) = \frac{\sum_{x,y}[f(x,y) - \bar{f}(u,v)t(x-u,y-v) - \bar{t}]}{\{\sum_{x,y}[f(x,y) - \bar{f}(u,v)]^2 \sum_{x,y}[t(x-u,y-v) - t]^2\}^{0.5}}.$$

Where, $\bar{t}$ indicates the mean of the feature and $\bar{f}(u,v)$ points to the mean of $f(x,y)$ that lie in the region below the feature. The equation stated above is termed as the normalized cross-correlation. At last, a similarity score for the image and every single modality is computed depending on the normalized cross correlation procedure. Assume that the continuous biometric authentication system makes use of NN modalities, $M_1, M_2, \cdots, M_N$ for authenticating a person. Further, let the similarity score yielded for each one of the modality be $S = S_1, S_2, \cdots, S_N$. Now, the weighted sum rule of the fused matching score F_S can be given as:

$$F_S = \sum_{i=1}^{n} W_i S_i.$$

Where W_i specify the weight allotted to M_i in the interval $[0, 1]$.

A weighting strategy that relies on Group Search Algorithm is being proposed here for accomplishing an enhancement in the performance of the score level fusion. The score weights of each and every feature are chosen in a random fashion and then, the GSO algorithm is exploited for optimizing the score weights with n number of iterations.

4.4 Group Search Optimization Algorithm

GSO is normally a population-dependent optimization algorithm with three constituent members, namely, the producer, the scrounger and the ranger. In this algorithm, a population containing arbitrary weights that lie in the interval between 0 and 1 is created at first. Each one of the individual residing in this population is known as the group. All these random weights will not be the best one. Hence, a fitness function that is applied on all the random weights is used to spot the best weight from the population. The member of the population holding the best fitness value will be the producer. The other members holding the best fitness values, but excluding the producer will be the scroungers. Finally, the rest of the members that are neither the producer nor the scrounger will be the rangers. The current position of every single member in the group of best weights is given by, $X_i^K \in R^n$ .The computation of the head angle, $\phi_i^K = (\phi_{i1}^K .....\phi_{in}^K) \in R^{n-1}$, and the head direction, $D_i^k \phi_i^K = (d_{i1}^K .....d_{in}^K) \in R^{n-1}$, is done with the help of polar to Cartesian coordinates transformation.

$$d_{i1}^k = \prod_{p-1}^{n-1} cos(\phi_{ip}^k) d_{ij}^k - sin(\phi_{i(j-1)}^k) \prod_{p-i}^{n-1} cos(\phi_{ip}^k) d_{in}^k - sin(\phi_{i(n-1)}^k).$$

As the subsequent action, the producer scans the field and this can be described in terms of the distance and the maximum pursuit angle. Here, θ_{max} stands for the maximum pursuit angle and l_{max} specify the maximum pursuit distance. During the k^{th} iteration, the producer does the scanning process in three directions and those directions are zero degree, left hand side hypercube and right hand side hypercube. In the direction of zero degree,

$$X_Z = X_p^k + r_1 l_{max} D_p^k(\phi_k).$$

During the right hand side hypercube direction,

$$X_r = X_p^k + r_1 l_{max} D_p^k(\phi^k + \frac{r_2 \theta_{max}}{2}).$$

At the time of left hand side hypercube direction,

$$X_1 = X_p^k + r_1 l_{max} D_p^k(\phi^k - \frac{r_2 \theta_{max}}{2}).$$

Where, r_1 denotes the normally distributed number and r_2 refers to the distributed random sequence lying in the interval between 0 and 1. Moreover, the producer makes the choice of the best point through the fitness value computation. The current position is deemed as the best position in situations, where the producer could not discover a best position than the present one. Else, the present point will be modified and the new angle will be formed with the expression stated below.

$$\phi^{k+1} = \phi^k + r_2 \alpha_{max}.$$

Where α_{max} indicates the maximum turning angle The angle will become as $\phi^{K+a} = \phi^k$ in cases where the producer fails to uncover a better resource than the current position, even when a^{th} iteration is completed. Then, the scrounging function takes place and the resultant will be the arbitrary selection of 80 % of the members from the remaining members. Random walk is employed for making a search of the distributed resources from the disperse operator. It forms a random head angle ϕ_i at K^{th} and selects a random distance as specified underneath. $l_i = a.r_1 lmax$ The last strategy in the GS algorithm is ranging, in which a movement to the new point is accomplished as given by the expression,

$$X_i^{K+1} = X_i^k + l_i D_i^K(\phi^{k+1}).$$

At the end, the best updated weights are achieved later to the completion of n number of iterations in the GSO algorithm, which has enabled the score level fusion as explained in Section 5.3.2.

4.5 Matching

Matching is conducted with a threshold, preset as T. An optimized weighting strategy was used in an earlier phase for yielding a fused score of all the features. The fundamental structure of the matching process, which works in accordance to the preset threshold, is shown in Figure 3.

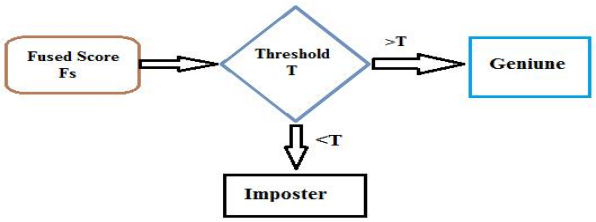

Figure 3: Matching process

The above figure states that a comparison is made between the fused modality score and the preset threshold. If the result of comparison is in such a way that the fused score exceeds the threshold level, the user is deemed as genuine. Else if the threshold is smaller than the fused score, the user is proved to be an imposter or a fake one. If a fake user is identified, our proposed methodology allows another process, known as Re-login authentication, to be carried out.

4.6 Authentication Using Modified PCA (MPCA)

In this phase, the face image in the initial template as well as the failed frame is applied with the modified PCA. Once MPCA is applied over the face image, the cross correlation is replaced by the Euclidean distance. Hence, MPCA only does the face authentication in continuous biometric system. If unsuccessful authentication occurs in any place of the authentication process, Re-login authentication is immediately conducted as the subsequent step in the proposed scheme.

4.7 MPCA Based Face Feature Extraction

The steps involved in MPCA are: (i) divide the face images into N number of sub-block images at an initial period and (ii) apply PCA to every single sub-block image using the local information pertaining to the face. When the process is started, the first sub-image of the image under consideration is compared against the entire number of images residing in the database. The images that satisfy a match with the first sub-image are alone chosen. Then, the second sub-image is compared against the set of images chosen in the previous step and the matched images are discovered. This procedure is repeated for all the sub-images and the recognized image will be the final outcome. If any of the sub-images is found to have got rid at an earlier stage, then the image is unrecognized. MPCA outweighs PCA by taking the changes in illumination, pose and facial expressions into account, in addition to offering improved results with larger accuracy. This recognition phase computes the weights W_k for both the training as well as the test frame. The computation of the difference in weights allows finding the Euclidean distance. To achieve recognition, a threshold has to be predetermined. The expressions in the images would be identical, if the threshold and the Euclidean distance have the same value. The weight W_k is computed in accordance to the following equation.

$$W_k = U_k(A_i - \varphi_i).$$

Where $U_k = \sum_{k=1}^{M} V_k \Phi_k$. Further, U_k denotes the Eigen faces, V_k points to the Eigen vectors and Φ_k represents the mean adjusted value. Re-login step will be performed at the condition, when the authentication ends up in failure in the proposed continuous biometric system.

5 Experimental Results

In this part we have presented the results of our proposed methodology and have scrutinized their appearance. The suggested multi-modal biometric authentication is executed in the MAT LAB program and the multi-modal biometric authentication is tested with the hard biometric (face) and soft biometrics (Ornaments, beard, mustache, dress color, mole) the result is contrasted with FAR and FRR values. The proposed authentication is implemented in a windows machine having configurations Intel (R) Core i5 processor, 1.6 GHz, 4 GB RAM, and the operation system platform is Microsoft Wnidow7 Professional. In Figure 1 the continuous authentication system setup is specified.

Figure 4: Continuous authentication system setup: Laptop with a webcam

5.1 Database Description

In our work, to evaluate the proposed continuous authentication scheme we collected videos of 10 subjects using the system shown in Figure 4. Every one user was asked to carry out the subsequent set of action while seated in front of the webcam. A few example screen shots are illustrated in Table 1.

- Scenario A: turning head to the left;
- Scenario B: turning head to the right;
- Scenario C: turning head down;
- Scenario D: straight to the chair;
- Scenario E: stretch arms;
- Scenario F: walk away.

Table 1: Example video frames used in experimentation

5.2 Evaluation Metrics

The effectiveness of proposed technique is analyzed by invoking some performance measures such as false rejection ratio (FRR), false accept ratio (FAR). The performance measures are explained below;

False rejection ratio: The system identifies imperfectly that a user is not in the cameras field of view although the user is yet in front of the camera. False discards lower the usability of the system.

False accept ratio: The system incorrectly identifies an imposter as the legitimate user. False admits lower the security of the system.

5.3 Performance Evaluation

The basic idea of our research is to continuously authenticate the subject in the online examination by means of soft and hard biometrics. To develop the authentication competence in our work we employ the MPCA (Modified Principal Component Analysis) with GSO. Niinuma et al. [13] have made cleared the incessantly validate the online examination by means of PCA and resemblance measures. We employ the MPCA with GSO algorithm to develop the competence. In Niinuma et al. [13] the facial recognition was performed by means of the PCA and soft biometric used were face colour and dress colour. However in our work the facial recognition is performed by means of MPCA and soft biometrics we are use (Ornaments, beard, mustache, dress color, mole). Both the hard biometric (face) and soft biometrics are fused with the assist of GSO algorithm based resemblance technique. The subsequent graph elucidated the presentation of the suggested approaches.

5.3.1 Performance of Continuous Authentication

In this section, we explain the performance of continuous systems using the Niinuma et al. [13] and proposed MPCA with GSO. The following graph demonstrates how our approach MPCA with GSO is effectively better then the Niinuma et al. [13].

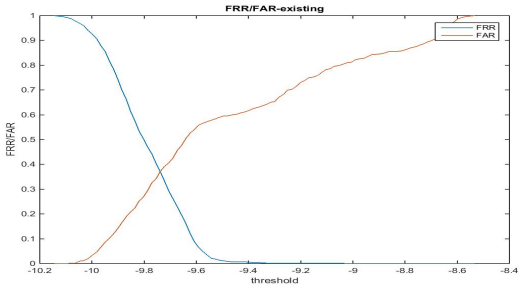

Figure 5: Performance of FAR and FRR for the continuous authentication using Niinuma et al. [13]

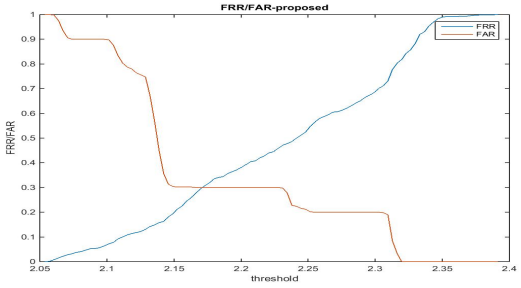

Figure 6: Performance of FAR and FRR for the continuous authentication using MPCA with GSO

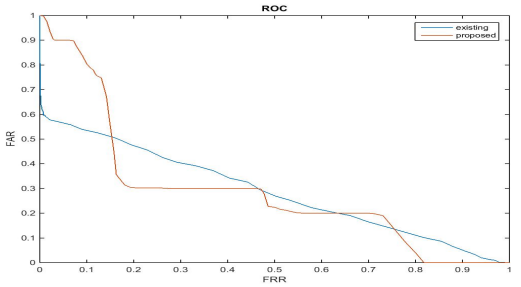

Figure 7: Performance of continuous authentication using ROC curve

Figures 5 and 6 illustrate the performance of the continuous authentication of Niinuma et al. [13] and proposed approach MPCA with GSO. When analyzing Figure 6, the approach achieves the minimum FRR and FAR of 0.3 but in Niinuma et al. [13] obtain the 0.37 which value is very much high compare to the proposed approach which

shows in Figure 5. When the system achieves the minimum FRR and FAR values the system achieve the maximum accuracy. In Figure 7 illustrate the performance of the continuous authentication using ROC curve. The approach Niinuma et al. [13] shows the resulted in an equal error rate (EER) of 0.49% and the proposed method of MPCA with GSO system using resulted in an EER of 0.28%, which is significantly better than the existing system Niinuma et al. [13].

5.3.2 Re-login Authentication

The user approaches to the re-login authentication, every time the system identifies that the user is no longer in front of the console. In this time, the system is bolted and it attempts to identify the user and re-authenticate him routinely. Now, the user is validated by means of both soft (colour histograms) and hard biometrics (face). The suggested re-login authentication method is assessed by means of video clips where an authorized user logs in, the user leaves the work environment (without logging out) and next, another user (an impostor) emerges in the field of view of the webcam. Figure 8 demonstrates this scenario. The system effectively identifies an impostor in Figure 8(c) and allows re-login to the first logged in user in Figure 8(e).

The colored ellipses in Figure 88(a) and (e) point out that the system properly identified the valid user in front of the console. At the same time, black-and-white images in Figure 8(b), (c), and (d) point out that the system properly recognized the absence of the legitimate user in front of the console.

Figure 8: Example results of re-login authentication experiments

Figures 9 and 10 show the re-login authentication of the online examination by means of Niinuma et al. [13] and suggested approach MPCA with GSO. When examining Figure 9, we attain the FAR and FRR rate is 0.65 which value is high. If the FAR and FRR values are high means the system can never get the higher competence. On the other hand, in Figure 10 we get the FRR and FAR value of 0.35 which value is very much low compare to the Niinuma et al. [13]. In our suggested work we employ the modified PCA and GSO algorithm for the system. The modified PCA employed to develop the efficiency of the

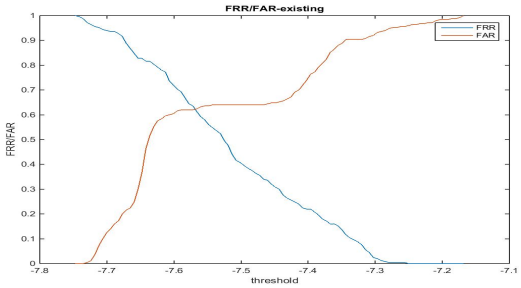

Figure 9: Performance of FAR and FRR for the re-login authentication using Niinuma et al. [13]

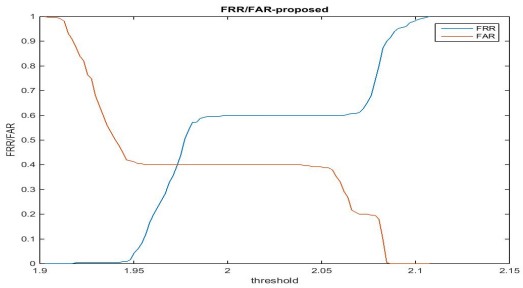

Figure 10: Performance of FAR and FRR for the Re-login authentication using MPCA with GSO

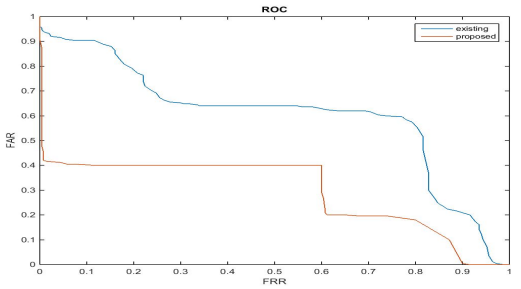

Figure 11: Performance of re-login authentication using ROC curve

hard biometric feature such as face. The presentation of the re-login authentication system is specified by the detection error rate (DET) curve exposed in Figure 11. The approach Niinuma et al. [13] demonstrates the resulted in an equal error rate (EER) of 0.62% and the suggested method of MPCA with GSO system by means of resulted in an EER of 0.40%, which is considerably better than the presented system Niinuma et al. [13].

6 Conclusion

We have proposed a new framework that uses both soft biometric traits and hard biometric traits for continuous user authentication. This framework registers a new en-

rollment template every time the user logs in, which enables the system to effectively use soft biometric traits for continuous authentication. The proposed system uses, face, dress colour, beard, mustache, and mole as biometric traits for continuous authentication. At a specified time interval, the initially registered template was matched with the next frame obtained through a sensor. Finally, for each biometric traits a matching score was generated based on the cross correlation. The generation matching scores were fused with the help of GSO based similarity technique. At any stage of mismatching, it requests to a re-login authentication stage. The experimental results of our proposed continuous biometric authentication system show better and improved authentication accuracy compared with the existing technique.

References

[1] Y. N. Chen, C. C. Han, C. T. Wang, K. C. Fan, "A novel scheme for face recognition and authentication against pose, illumination and expression changes," *Journal of Information Science and Engineering*, vol. 27, pp. 369–380, 2011.

[2] W. Fu Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016

[3] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," *IEEE Transactions On Image Processing*, vol. 23, no. 2, pp. 710–724, 2014.

[4] A. K. Jain, S. C. Dass, and K. Nandakumar, "Can soft biometric traits assist user recognition?," in *Proceedings of SPIE*, LNCS 5404, pp. 561–572, Springer, 2004.

[5] A. K. Jain, S. C. Dass, and K. Nandakumar, "Soft biometric traits for personal recognition systems," in *Proceedings of the First International Conference on Biometric Authentication (ICBA'04)*, LNCS 3072, pp. 731–738, Springer, 2004.

[6] A. Jaiswal, N. Kumar, R. K. Agrawal, "Illumination invariant facial pose classification," *International Journal of Computer Applications*, vol. 37, no. 1, pp. 0975-8887, 2012.

[7] A. Kar, D. Bhattacharjee, D. K. Basu, M. Nasipuri, M. Kundu, "Face recognition using Hough peaks extracted from the significant blocks of the gradient image," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 1, Jan. 2012.

[8] E. Khourya, L. El Shafeya, C. McCoolb, M. Gnthera, S. Marcela, "Bi-modal biometric authentication on mobile phones in challenging conditions," *Journal of Image and Vision Computing*, vol. 32, no. 12, pp. 1147–1160, Dec. 2014.

[9] M. Leszczynski, "Image preprocessing for illumination invariant face verification," *Journal of Telecommunication and Information Technology*, vol. 4, pp. 19–25, 2010.

[10] C. C. Liu, D. Q. Dai and H. Yan, "Local discriminant wavelet packet coordinates for face recognition," *Journal of Machine Learning Research*, vol. 8, pp. 1165–1195, 2007.

[11] M. C. Mohan, V. V. Kumar and K. V. Subbaiah, "A new method of face recognition based on texture feature extraction on individual components of face," *International Journal of Signal and Image Processing*, vol. 1, no. 2, pp. 69–74, 2010.

[12] S. Muruganantham, "A comprehensive review of significant researches on face recognition based on various conditions," *International Journal of Computer Theory and Engineering*, vol. 4, no. 1, Feb. 2012.

[13] 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.

[14] P. Paysan, R. Knothe, B. Amberg, S. Romdhani and T. Vetter, "Face recognition using 3-D models: Pose and illumination," *Proceedings of IEEE*, vol. 94, no. 11, pp. 1977–1999, 2009.

[15] A. Prakash, "A biometric approach for continuous user authentication by fusing hard and soft traits," *International Journal of Network Security*, vol. 16, no. 1, pp. 65–70, 2014.

[16] R. Rathi, M. Choudhary, B. Chandra, "An application of face recognition system using image processing and neural networks," *International Journal of Computer, Technology and Applications*, vol. 3, no. 1, pp. 45–49, 2012.

[17] A. Ross and A. K. Jain, "Multimodal Biometrics: An Overview," in *Proceedings of 12th European Signal Processing Conference (EUSIPCO'04)*, pp. 1221–1224, Sept. 2004.

[18] A. Ross and A. K. Jain, "Information fusion in biometrics," in *Proceedings of AVBPA*, pp. 354–359, Halmstad, Sweden, June 2001.

[19] J. Shermina and V. Vasudevan, "An efficient face recognition system based on the hybridization of invariant pose and illumination process," *European Journal of Scientific Research*, vol. 64, no. 2, pp. 225–243, 2011.

[20] J. R. Sun, M. L. Shih, M. S. Hwang, "A survey of digital evidences forensic and cybercrime investigation procedure," *International Journal of Network Security*, vol. 17, no. 5, pp. 497–509, 2015

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.

R. Dhanalakshmi a Ph.D holder from College of Engg.,

Guindy Anna University Chennai for the research activities in Information Security and Networking. She holds a B.E in Computer Science from Bharathidasan University and M.Tech in Advanced Computing from SASTRA University. She has vital research experience serving as a research Associate in the NTRO Sponsored Project Collaborated directed basic research on Smart and Secure Environment at Anna University under the consortium of IIT Madras. To her credit, she has nearly 25 research papers in International Conferencess and International Journals including Elsevier, Springer, IFIP and IGI Global. Her fields of interest include Information Security, Data Mining, Knowledge and Semantic Networks, Intelligent Networks and Mobile Computing.