Soft Biometrics Traits for Continuous Authentication in Online Exam Using ICA Based Facial Recognition

Prakash Annamalai[1], Krishnaveni Raju[1], and Dhanalakshmi Ranganayakulu[2]
(Corresponding author: A. Prakash)

Department of Computer Science and Engineering, Hindustan Institute of Technology and Science[1]
Old Mahabalipuram Road, Padur 603103, India
(Email: prakash1712@yahoo.com)
Department of Computer Science and Engineering, KCG College of Technology, Chennai, India[2]

(Received Nov. 8, 2016; revised and submitted Feb. 1, 2017)

Abstract

Biometric authentication has been getting widespread attention over the past decade with growing demands in automated secured personal identification. Continuous Authentication (CA) system verifies the user continuously once a person is logged in. Continuous Authentication system prevents the intruders from invoking the system. A new framework for continuous user authentication that primarily uses hard and soft biometric traits using Independent Components Analysis (ICA) dimension reducing method for video frames. The proposed framework automatically registers (enrolls) soft biometric traits every time the user logs in and fuses soft biometric matching with the conventional authentication schemes. Different soft biometrics are considered to obtain the matching score value, here optimize the soft biometrics weights using Grey Wolf Optimization (GWO) technique is used. Finally the authentication is performed and evaluated using standard evaluation metrics then produce the maximum accuracy compared to existing methods.

Keywords: Biometric Traits; Continuous Biometric Authentication; Face Recognition; Online Exam Authentication

1 Introduction

In a modern life personal authentication is a common concern to both industries and academia due to its numerous applications such as physical access control, computer security, banking, airport, computer system login, and mobile phones law enforcement, etc [16, 17, 21]. Biometric measurement is a key component of several personal authentication systems that only render services to legitimately enrolled users [8, 10, 12]. The most known and often used modalities are fingerprints, face, hand geometry, knuckle print, palm and iris. These are widely deployed in large-scale systems such as border control and biometric passports [2, 6, 20]. Biometric information stored in a database may leak biometric features which can be used to reconstruct a biometric image [1]. Biometric traits are difficult to counterfeit and hence results in higher accuracy when compared to other methods such as using passwords and ID cards [7]. Biometrics identifies the person by what the person is rather than what the person carries, unlike the conventional authorization systems like smart cards [9, 13]. Hand-based person identification provides a reliable, low-cost and user-friendly viable solution for a range of access control applications. Palm print is one of the relatively new hand-based biometrics due to its stable and unique characteristics [15]. Authentication with respect to fingerprints implies that recognition is based on matching the features of a live fingerprint against those of fingerprints that are already stored in a server database. In addition, a digital signature of a fingerprint can be used for reliability [18].

2 Literature Review

In 2014, Gao *et al.* [3] Had proposed the Competitive Coding (Comp Code) scheme, which extracts and codes the local dominant orientation as features, had been widely used in Finger Knuckle Print (FKP) verification. However, Comp Code may lose some valuable information such as multiple orientation and texture of the FKP image. To remedy the above drawback, a novel multiple orientation and texture information integration scheme is proposed in the process. As compared with Comp Code, the proposed scheme not only considers more orientations, but also introduces a multilevel image thresholding scheme to perform orientation coding on each Gabor filtering response. For texture features extraction, LBP maps are first obtained by performing Local Binary Pattern (LBP) operator on each Gabor filtering response, and then a similar coding scheme is applied on these LBP maps.

In 2014, Gupta *et al.* [4] had proposed an efficient algorithm to segment all finger tips from a slap-image and to identify them into their corresponding indices i.e. index, middle, ring or little finger of left/right hand. Geometrical and spatial properties have been used to identify these fingertips. The proposed algorithm can handle various challenges like the presence of dull prints, large rotational angles of the hand, small variation in the orientation of the fingertips and non-elliptical shape of components. It has been tested on a database of 6732 images of 1122 subjects. Experimental results reveal the segmentation of all fingertips from slap-images with an accuracy of 99.02%.

Tan *et al.* [19] had presented that discrimination of Used Frying Oil (UFO) from Edible Vegetable Oil (EVO), the estimation of the using time of UFO, and the determination of the adulteration of EVO with UFO. Both the heating time of laboratory prepared UFO and the adulteration of EVO with UFO could be determined by Partial Least Squares Regression (PLSR). To simulate the EVO adulteration with UFO, for each kind of oil, fifty adulterated samples at the adulterant amounts range of 1-50% were prepared. PLSR was then adopted to build the model and both full (leave-one-out) cross-validation and external validation were performed to evaluate the predictive ability.

Lai *et al.* [11] 2016 had proposed a new lip feature representation for lip biometrics which can portray the static and dynamic characteristics of a lip sequence. The new representation catches both the physiological and behavioral parts of the lip and is strong against varieties brought about by various speaker position and posture. In our approach, a lip sequence is initially partitioned into a few subsequences along the fleeting measurement. For every subsequence, sparse coding (SC in short) is received to portray the details of the lip locale and its development in little spatiotemporal cells. At long last, notwithstanding when there is one and only preparing test per speaker, the proposed feature still accomplishes high discriminative power (an exactness of 98.39% and HTER of 2.62%).

Gupta *et al.* [5] 2016 had exhibited that hand dorsal images procured under infrared light are utilized to outline a precise individual authentication framework. Another quality estimation algorithm is proposed to assess the nature of palm dorsal which appoints ease back qualities to the pixels containing hair or skin surface. Matching scores are acquired by matching palm dorsal veins and infrared hand geometry features. These are in the long run combined for authentication. For execution assessment, a database of 1500 hand images gained from 300 unique hands is made. Exploratory results exhibit the predominance of the proposed framework over existing frameworks.

3 Biometrics

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Biometrics is used to refer to the field of technology devoted to identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, or face recognition. Biometrics provides a convenient and low-cost additional tier of security. It eliminates problems caused by shared passwords by using physiological attributes. This work Authentication process considers the some natural and soft bio metrics are considered to the online exam process.

4 Proposed Methodology

In the current investigation, an earnest effort is made to design an effective technique for the multimodal biometric recognition employing the soft bio metrics in online exam process. Initially prepare the video frame database for the authentication process. 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 proposed method for continuous user authentication is proposed that continuously collects soft biometric information. In particular, in this method the colors of user's clothing and face as the soft biometric traits are used. This proposed approach having four models such as Initial login authentication, continuous authentication, re login authentication and enrollment template are considered to bio metric authentication process. Proposed block diagram shown in Figure 1. Then the dimension reduction process Independent Component Analysis (ICA) is used and also obtain the matching score value Grey Wolf Optimization (GWO) techniques are used.

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.

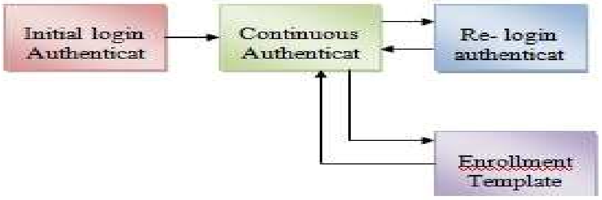


Figure 1: Block Diagram of the proposed method

Figure 2 shows the diagram of template registration and continuous authentication process consider the

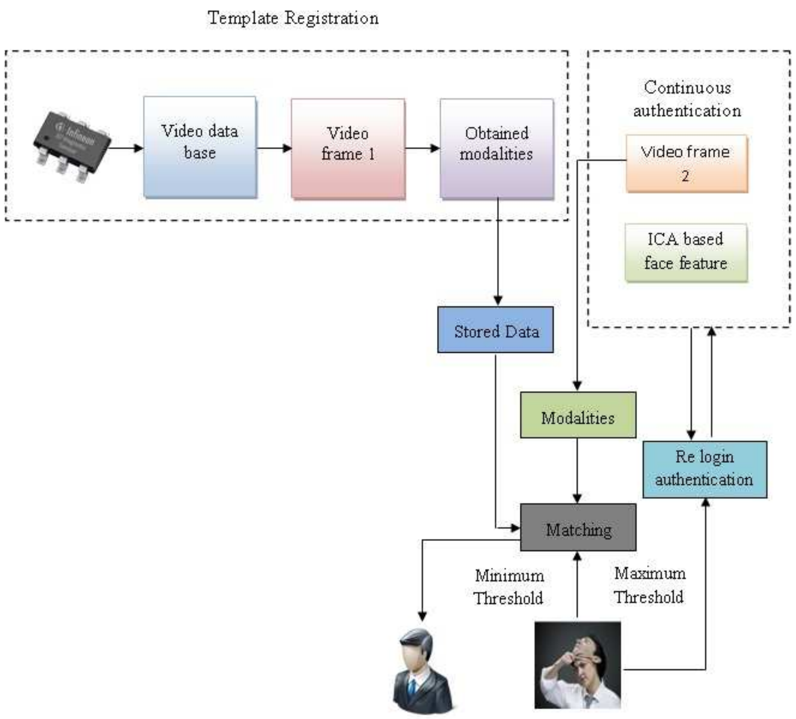


Figure 2: Schematic for continuous authentication system

modalities such as 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. Initially template registration process considers the database to obtain the above mention modalities are considered to store the data. Then continuous authentication process chooses the different video frame find the modalities with the dimension reducing ICA technique is used after this process finding maximum score value using optimization technique. This score value based to obtain the fusing score value to identify the user if minimum fusing score value means that is a original user and maximum fusing score means the user is imposter to re login the authentication process.

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 imposter.

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 different above mention modalities. 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.

Initial Authentication: Biometric face recognition authentication method can be used.

Face Detection: A user is typically looking in the frontal direction during the login session. This is a reasonable assumption because the user typically looks at the monitor at the login time as the user wants to be authenticated.

Body Localization: Location and size of the user's body with respect to his face are estimated.

4.2 Continuous Authentication

Continuous authentication starts after Initial login process. The system continuously authenticates the user by using the "soft face" and "clothing" enrollment templates registered in initial login authentication. The system tracks the face and the body separately based on the histograms registered in initial login process. Hard face recognition is not directly used in continuous authentication but it is stored for use in relogin authentication. 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. The matching score value calculated in video frame 1 and video frame 2 in continuous authentication process help of optimization technique, this initial login and continuous authentication with modalities shown in Figure 3.

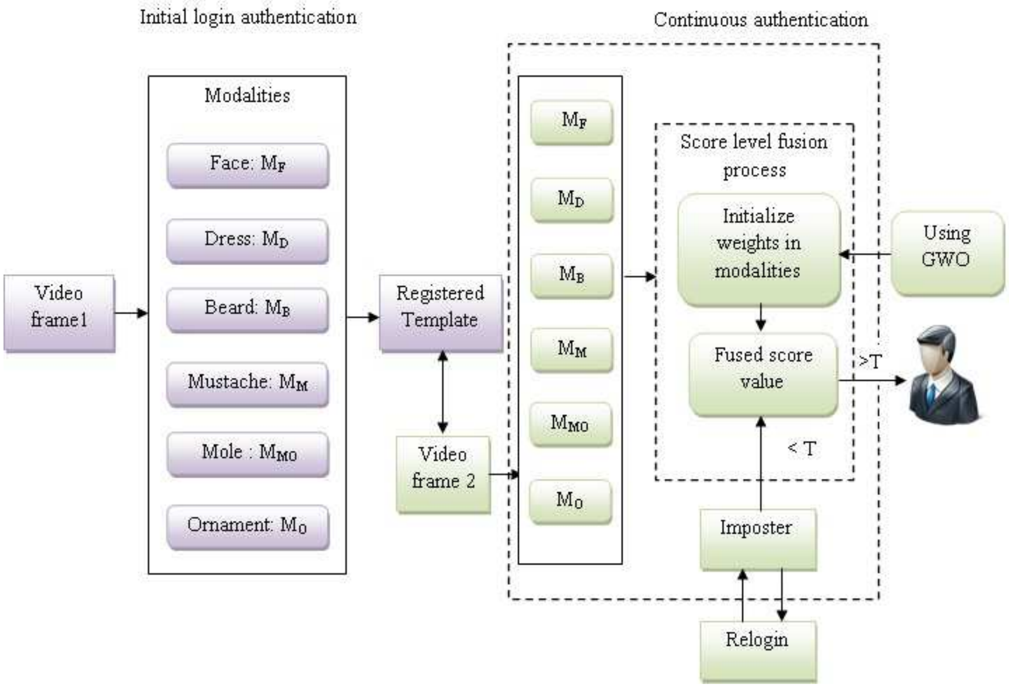


Figure 3: Diagram for Initial and continuous authentication

4.3 Enrollment Template

The system status enters enrollment template whenever the similarity falls below threshold. This step is introduced to reduce the false rejects caused by illumination changes. A pair of images, one just before and one immediately after the time when Similarity ≤ threshold is used for image subtraction; the number of pixels that show a large difference in brightness between the two images is counted.

4.4 Score Level Fusion Process

The score level fusion effectively matches scores output of the multiple biometric matchers by integrating them to produce a new match score. The score value calculation different modalities weights are considered to the score value evaluation process. Now the feature weights are optimally chosen with the help of GWO optimization technique the score value is attained. The gradual process of the score level fusion for the authentication process in different modalities considered to find the values. Score value calculation process optimal modalities weights are considered this optimization process is discuss below.

4.4.1 Grey Wolf Optimization Process

The grey wolves adequately frame a Canidae's piece family and are esteemed as the apex predators showing their position at the sustenance's food chain. They routinely show an inclination to make due as a group. The choices made by the alpha are passed on to the group. The Beta speaks to the second rank in the pecking order of the grey wolves. They are, basically, auxiliary wolves which adequately offer some assistance to the alpha in the choice making or comparable group functions. In the GWO technique the hunting (optimization) is guided by the α, β, δ and ω.

Initialization Process: In the district developing procedure, pick the weights of the different modalities such as face, ornaments, dress colour, beard, scars and mustache $W_i = W_1, W_2, ...W_n$ and algorithm parameters, for example, a, A,and C as coefficient vectors.

Fitness Evaluation: In video frame different modalities are considered to the score value calculation process the weights and random values are selected. This GWO Algorithm is being proposed here for accomplishing an enhancement in the performance of the score level fusion. In above equation W_i specifies weight and r_i are random values from [0 to 1].

Based on the fitness separate the solution: Now, we find the fitness separate solution (weight) based on the fitness value.Let the first best fitness solutions be α the second best fitness solutions β and the third best fitness solutions δ.

Update the position: We assume that the alpha (best candidate solution) beta and delta have the improved knowledge about the potential location of the prey in order to mathematically reproduce the hunting behavior of the grey wolves. As a result, we hoard the first three best solutions attained so far and require the other search agents (including the omegas) to revise their positions according to the position of the best search agent. For revision, the novel solution $W(t+1)$ below mentioned formulas are employed.

$$\begin{aligned} D^{\alpha} &= [C_1.W^{\alpha} - W], \\ D^{\beta} &= [C_1.W^{\beta} - W], \\ D^{\delta} &= [C_1.W^{\delta} - W]. \end{aligned} \tag{1}$$

$$\begin{aligned} W_1 &= W_{\alpha} - A_1(D_{\alpha}, \\ W_2 &= W_{\beta} - A_2(D_{\beta}, \\ W_3 &= W_{\delta} - A_3(D_{\delta}. \end{aligned} \tag{2}$$

Algorithm 1 Pseudo code for GWO

```
Begin
Initialize the solution
$W_i = W_1, W_2, ....W_n$
Initialize a,A and C
Find the fitness for the initial solution
$$F_i = \sum_{i=1}^{n} W_i.r_i$$
Based on the fitness separate the solution
$W_\alpha$ = the best search solution
$W_\beta$ = the second best search solution
$W_\delta$ = the third best search solution
Update the position of the current search solution
$W(t+1) = \frac{\bar{W_1}+\bar{W_2}+\bar{W_3}}{3}$
Calculate the fitness for new search solution
$$F_i = Max \sum_{i=1}^{n} W_i.s_i$$
Store the best solution so far attained
Iteration=Iteration+1
Stop until optimal solution attained
End
```

To have hyper-spheres with different random radii the arbitrary parameters A and C help candidate solutions. Investigation and utilization are guaranteed by the adaptive values of A and α. The values of parameters A and α permit the GWO to smoothly transition them among the investigation and the utilization. With decreasing A, half of the iterations are dedicated to the investigation ($|A| < 1$) and the other half are devoted to the utilization. Encircling the behavior, the subsequent equations are employed in order to mathematically model.

$$D = |CW_{p(t)} - W(t)| \tag{3}$$

For find the coefficient vectors use Equation (3):

$$A = 2ar_1 = a, \quad C = 2r_2 \tag{4}$$

Where t indicates the current iteration, A and C are coefficient vectors, $W_p$is the position vector of the prey T and indicates the position vector of a grey wolf. The components of α are linearly decreased from 2 to 0 over the course of iterations and r_1, r_2 are random vectors in [0, 1]. The GWO has only two main parameters to be adjusted (α and C). However, we have kept the GWO algorithm as simple as possible with the fewest operators to be adjusted. The maximum score value obtained in the process will be continued.

4.4.2 Matching Process

Matching is conducted with a weight preset as W. 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 as follows:

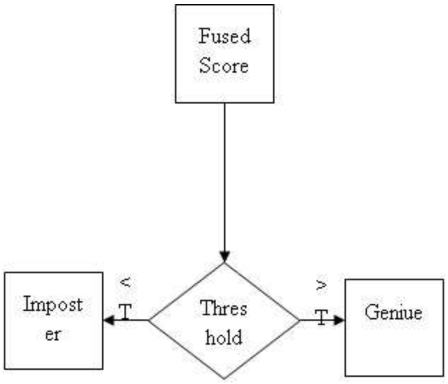


Figure 4: Matching process

The below Figure 4 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.

4.5 Independent Component Analysis (ICA)

ICA is a data analysis tool derived from the "source separation" signal processing techniques. The aim of source separation is to recover original signals S_i , from known observations O_j , where each observation is an (unknown) mixture of the original signals. 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. It is expected that, ICA source vectors being independent (instead of PCA eigenvectors being uncorrelated only), they will be closer to natural features of images, and thus more able to represent differences between faces.

4.5.1 Use of ICA in face feature authentication

ICA is an unsupervised technique which separates the independent sources from a mixture. The general model of ICA is

$$O = BS. \tag{5}$$

Where B represents unknown mixing matrix, S represents unknown source signal and O represents observed mixtures. In this case, it is assumed that the source signals are statistically independent and non-Gaussian and observed mixtures is the only information to have. In ideal condition, mixing matrix B can be inversed. If the estimation of separation matrix is accurate, then a good approximation of source signal will be obtained.

$$I = WO = WBS \quad and \quad W = B^{-1}. \tag{6}$$

Where I represents unknown mixing matrix.

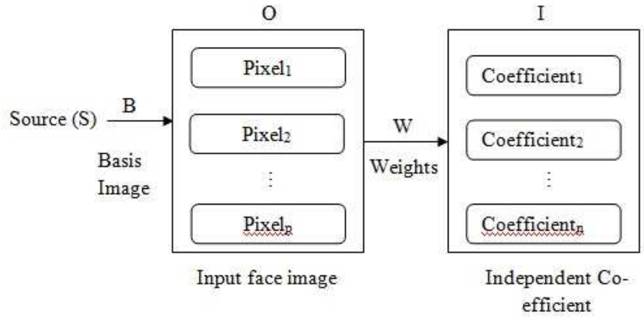


Figure 5: Image synthesis model

In Figure 5 shows the pixels are treated as variables and images are observations. This results the column of $B = W^{-1}$ as a set of basis image. Column of I contains a set of independent coefficient of basis images in A for reconstructing image in O. Therefore, I is a factorial code representation. In order to assess the sensitivity of ICA in terms of the dimension of the compressed and whitened space where it is implemented, we carried out a comparative assessment for different dimension whitened subspace.

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.

$$W_k = I_k(B_i - \phi_k) \tag{7}$$

Where

$$I_k = \sum_{k=1}^{n} E_k.\phi_i$$

Further, I_k denotes the Eigen faces,E_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.

4.6 Relogin Authentication

In this process the system is locked and it tries to detect the user and re authenticates him automatically. If the system detects a user and re authenticates the user as genuine, the status moves to continuous authentication process. Here, the user is authenticated using both soft (colour histograms) and hard biometrics (face). The similarity score is used for relogin authentication. There will be a small discontinuity in the values of soft biometrics when the unauthenticated person tries to replace the student. When there is a discontinuity in the similarity scores based on the soft biometric, the system enters relogin authentication mode. In the relogin authentication mode, the user must provide valid soft and hard biometrics.

5 Result and Discussion

This section discusses about the results of the proposed method biometric authentication using ICA with GWO technique and has scrutinized their appearance in the working platform of MATLAB 2014 with the system configurations as i5 processor with 4GB RAM. This model consider the hard biometric is face and soft biometrics Ornaments, beard, mustache, dress color and mole different performance evaluation parameters are obtained.

5.1 Database Description

This work generates the synthetic database to the continuous authentication scheme. Each user was asked to perform the following set of actions while seated in front of the webcam. We collected videos of 20 subjects using the system shown in Figure 8. Every one user was asked to carry out the subsequent set of action while seated in front of the webcam. A few examples are illustrated in Figure 6.

5.2 Performance Evaluation Metrics

The effectiveness of proposed technique is analyzed by invoking some performance measures such as False Rejection Ratio (FRR), False Accept Ratio (FAR), Sensitivity, specificity and accuracy. The performance measures are explained below:

False Rejection Ratio: The system identifies imperfectly that a user is not in the camera's field of view although the user is yet in front of the camera. False discards lower the usability of the system.

$$FRR = \frac{Genuine\ \ scores\ \ falling\ \ below\ \ Threshold}{All\ \ Genuine\ \ Score} \tag{8}$$

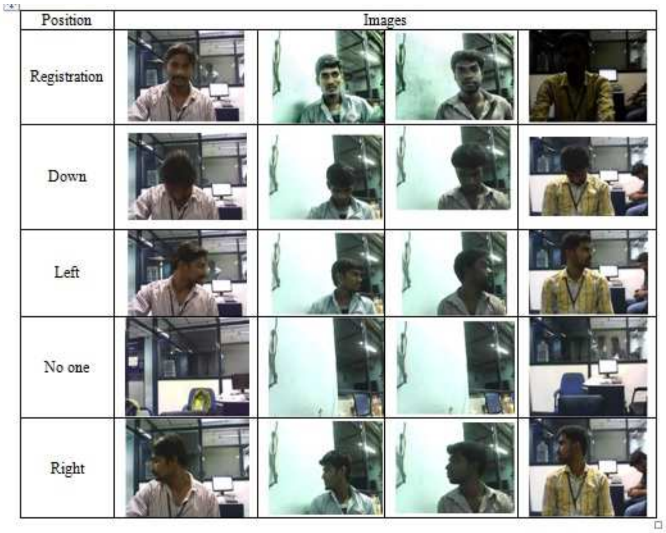


Figure 6: Sample Video frames for authentication process

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

$$FRR = \frac{Imposter\ \ scores\ \ exceeding\ \ Threshold}{All\ \ Imposter\ \ Score} \tag{9}$$

Sensitivity: Sensitivity is a measure which determines the probability of the results that are true positive as 'that person has the authenticated person.

$$Sensitivity = \frac{NTP}{NTP + NFN} \tag{10}$$

where NTP denotes number of true positives; NFN denotes number of false negatives.

Specificity: Specificity is a measure which determines the probability of the results that are true negative as 'that person does not have the authenticated person.

$$Specificity = \frac{NTN}{NTN + NFN} \tag{11}$$

where NTN denotes number of true negatives; NFN denotes number of false negatives.

Accuracy: Accuracy is a measure which determines the probabilities that how may results are accurately authenticated.

$$Accuracy = \frac{(TP + TN)}{TP + TN + FP + FN}. \tag{12}$$

5.3 Registration of Biometric Data

The system registers face biometric data. This work using ICA with GWO optimization approach based face recognition. Because the system registers face biometric data every time a user logs in, the problem of the illumination difference between the time of enrolment and the time of identification is mitigated. 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 6 shows the different position identification of the data.

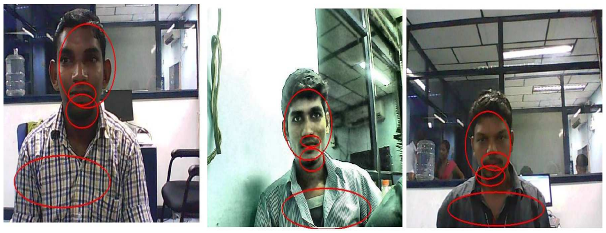


Figure 7: Face, clothing and mustache sample

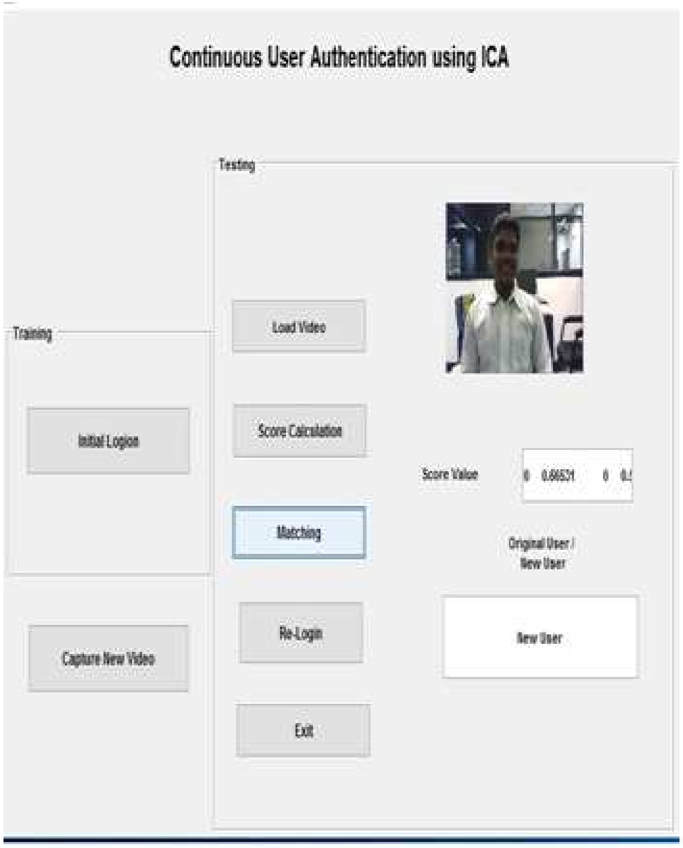
Face recognition is executed at regular intervals (e.g., once every 10 seconds). If it succeeds, Tlast, which represents the last time the face recognition was successful, is updated. Face recognition is used only for assisting the identification using colour histograms because the system cannot obtain the face information during different cases. The system enters the initial login authentication mode. On the other hand, if the user is absent for only a short time, it is more likely that he will be accepted given valid soft and hard biometric traits.

Figures 8 and 9 shows that the Graphical User Interface (GUI) for new user authentication and original; user authentication process. Initially load the video then obtain the score value and compare the matching score in original and new user authenticated the person, if the score value based obtain similarity in original user and imposter.

Figure 10 shows that the FRR and FAR in GWO and GSO techniques, the FRR rate is maximum value compared FAR. Performances of face and soft biometrics are evaluated using False Acceptance Rate FAR and the False Rejection Rate FRR. Test was conducted using different number of training files. FAR is the percentage of illegal users that are accepted as genuine. FRR is the percentage of legal user rejected as imposter. From the result, FAR and FRR is high for small number of trained samples. The proposed technique FRR is 0.82 its maximum value compared to GSO similar difference in FAR in authentication process.

5.4 Comparative Analysis in Performance Parameters

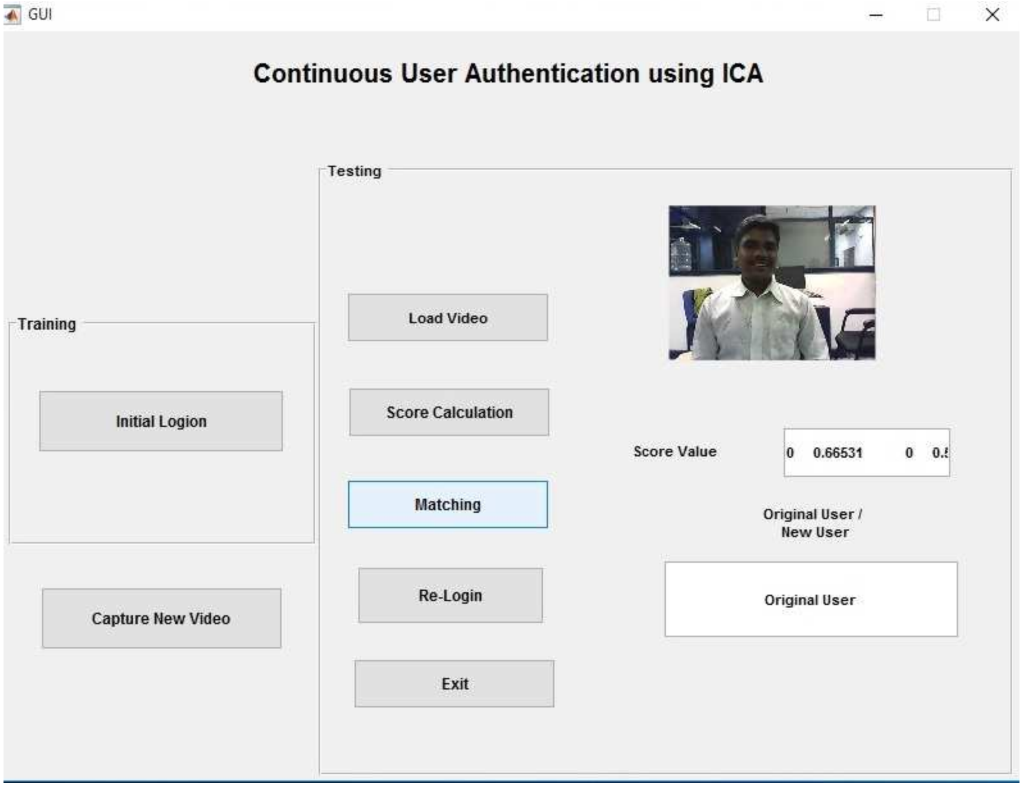
Here a comparison of authentication process in existing approach PCA with GSO and propose technique ICA with GWO techniques is compared. The parameters such as accuracy, sensitivity, specificity, FRR and FAR are compared.



Score Value 0 0.66531 0 0.5

Original User / New User: New User

Figure 8: New user login authentication



Score Value 0 0.66531 0 0.5

Original User / New User: Original User

Figure 9: Original user login authentication

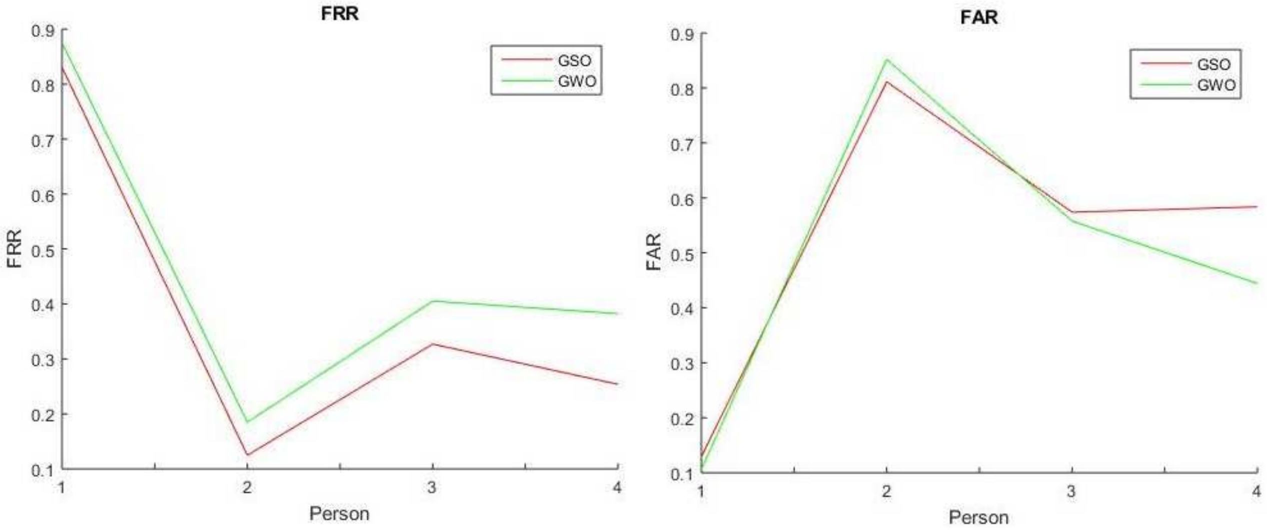


Figure 10: Comparison graph for FRR and FAR

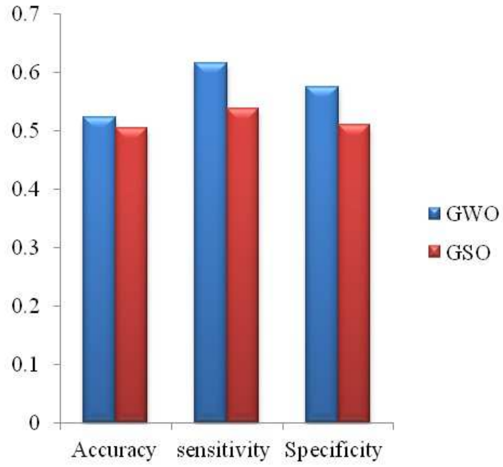


Figure 11: Comparative analysis graph

Figure 11 shows that the accuracy, sensitivity and specificity comparison GWO and GSO technique, here different four persons are considered to evaluate this performance. The maximum performance attained in ICA with GWO techniques, maximum accuracy is 0.5246 it's compared to GSO the difference is 0.256%. Likewise, the accuracy of the ICA with GWO being 6.05% , it is seen reduced by 0.16% and 1.15% respectively in the case of GSO. As a whole, the proposed method shows a significant hallmark of 0.75% when compared with the other methods in terms of the parameters specified in the bar graph. Similarly other parameters are smaller difference in authentication process.

6 Conclusion

This framework registers a new enrolment 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 color information as well as clothing color (soft biometric) to continuously authenticate the user. This authentication process ICA with GWO produced the maximum accuracy value. The main purpose of this paper is to present a new e-learning model used for identification, authentication and tracking the student. The system is robust with respect to user's posture in front of the workstation. Experimental results demonstrate that the system is able to successfully authenticate the user continuously with high tolerance to the user's posture. In our ongoing work, we are considering introducing additional soft biometric traits. By applying these methods we enhance Continuous Authentication system and try to obtain better result other than state-of-art method.

References

[1] T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinate-based cancelable fingerprint templates", *Journal of Pattern Recognition*, vol. 44, pp. 2555-2564, 2011.

[2] M. Choras, and R. Kozi, "Contactless palmprint and knuckle biometrics for mobile devices", *Journal of Theoretical Advances*, vol. 7, no. 1, pp. 73-85, 2012.

[3] G. Gao, J. Yang, J. Qian, L. Zhang, "Integration of multiple orientation and texture information for finger-knuckle-print verification", *Journal of Neurocomputing*, vol. 135, pp. 180-191, 2014.

[4] P. Gupta, and P. Gupta, "An efficient slap fingerprint segmentation and hand classification algo-

rithm", *Journal of Neurocomputing*, vol. 8, pp. 1-14, 2014.

[5] P. Gupta, S. Srivastava and P. Gupta, "An accurate infrared hand geometry and vein pattern based authentication system", *Journal of Knowledge-Based Systems*, vol. 103, no. 9, pp. 143-155, 2016.

[6] L. Han, Q. Xie, and W. Liu, "An improved biometric based authentication scheme with user anonymity using elliptic curve cryptosystem," *International Journal of Network Security*, vol. 19, no. 3, pp. 469-478, 2017.

[7] C. Hegde, Phanindra, D. Shenoy, and Patnaik, "Human authentication using finger knuckle print", *Journal of Biometric Authentication*, vol. 3, pp. 1-8, 2011.

[8] O. Kaiwartya, M. Prasad, S. Prakash, *et al.*, "An investigation on biometric internet security," *International Journal of Network Security*, vol. 19, no. 2, pp. 167-176, 2017.

[9] Kekre, and Bharadi, "Finger-knuckle-print region of interest segmentation using gradient field orientation and coherence", *Journal of Emerging Trends in Engineering and Technology*, vol. 978, pp. 130-133, 2010.

[10] A. Kumar and D. Zhang, "Improving biometric authentication performance from the user quality", *Journal of Instrumentation and Measurement*, vol. 59, no. 3, pp. 730-735, 2010.

[11] J. Y. Lai, S. L. Wanga, A. W. C. Liew and X. J. Shi, "Visual speaker identification and authentication by joint spatiotemporal sparse coding and hierarchical pooling", *Journal of Information Sciences*, vol. 373, no. 8, pp. 219-232, 2016.

[12] C. T. Li, M. S. Hwang, "An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards," *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 5, pp. 2181-2188, May 2010.

[13] C. T. Li, M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards", *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1-5, 2010.

[14] C. H. Ling, C. C. Lee, C. C. Yang, and M. S. Hwang, "A secure and efficient one-time password authentication scheme for WSN", *International Journal of Network Security*, vol. 19, no. 2, pp. 177-181, 2017.

[15] A. Meraoumia, S. Chitroub, and A. Bouridane, "Palmprint and finger-knuckle-print for efficient person recognition based on Log-Gabor filter response", *Journal of Analog Integration Circuit Signal Processing*, vol. 69, no. 1, pp. 17-27, 2011.

[16] 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, Jan. 2014.

[17] A. Prakash, R. Dhanalakshmi, "Stride towards proposing multi-modal biometric authentication for online exam", *International Journal of Network Security*, vol. 18, no. 4, pp. 678-687, July 2016.

[18] Shankar, Sahoo, and Niranjan, "Using the digital signature of a fingerprint byan elliptic curve cryptosystem for enhanced authentication", *Journal of Information Security*, vol. 21, pp. 243-255, 2012.

[19] J. Tan, R. Li, Z. T. Jiang, *et al.*, "Synchronous front-face fluorescence spectroscopy for authentication of the adulteration of edible vegetable oil with refined used frying oil", *Journal of Food Chemistry*, vol. 217, no. 7, pp. 1-7, 2016.

[20] M. Tarek, O. Ouda, T. Hamza, "Pre-image resistant cancelable biometrics scheme using bidirectional memory model," *International Journal of Network Security*, vol. 19, no. 4, pp. 498-506, 2017.

[21] L. Zhang, L. Zhang, D. Zhang, and H. Zhu, "Online finger-knuckle-print verification for personal authentication", *Journal of Pattern Recognition*, vol. 43, no. 7, pp. 2560-2571, 2010.

Biography

Prakash Annamalai 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.

Krishnaveni Raju is currently working as Professor at Hindustan Institute of Technology and Science, India. She is a PhD holder from Anna University. She completed her B.E degree from Bharadhiyar University and M.E degree from Madras University. She has published around 30 research papers in International Journals and International Conferences including Springer, IFIP, JCTN and many other referred journals. Her areas of research interests include Network Security, Biometrics Security and Web Security.

Dhanalakshmi Ranganayakulu 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 Conferences 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.