International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 21 Issue 1 – APRIL 2016.

A CONTINUOUS USER VERIFICATION SYSTEM BASED ON BLUR-ILLUMINATION ALGORITHM AND LATENT SVM APPROACH IN ONLINE EXAMINATION

E.Divya[#1], Mrs.K.R.Vinothini[*2]

[#1]*M.E., Dept. Of ECE,* A.V.C College Of Engineering, Mayiladuthurai, India

[*2]*M.E., Assistant Professor, Dept. Of ECE,* A.V.C College Of Engineering, Mayiladuthurai, India

Abstract **--- In this paper, during online examination a continuous authentication system based on hard biometric and soft biometric is presented. It is used for monitoring the candidate during online examination. Human facial features are used as hard biometrics. Skin colour is employed as soft biometric. This system continuously verifying the user or candidate without interrupting on his work. It is able to recognise who is in front of the system. It denies the access to Invader during online examination. In this system face recognition system is implemented using Eigen face method and interactive ABC algorithm. Hence the accuracy can be increased. The relighting module is used to avoid the illumination changes.**

Index Terms **--- Interactive Artificial bee colony (IABC), biometric, continuous authentication (CA), face recognition, passive authentication, relighting module.**

I. INTRODUCTION

Humans have used body characteristics such as face, voice, and gait to recognize each other. The conventional authentication system only requests the user to provide the authorized account and password to log into the system once they start to use a computer or a terminal. However, under this authentication work, the machine can only recognize the user from the login information. It lacks the information to know who is using it and unnoticeable. The common disadvantage of the one-time authentication system, which people used in the daily life, is that when the user leaves the seat for a short break.

To avoid this disadvantage under the conventional authentication system, the user can only log off the system or lock the screen manually before leaving, and log in afterwards. Again when coming back to continue the work. This produces an inconvenience to the user, especially when the user is busily coming and doing other things. Sometimes, the user may skip the log-off process just to keep away from the exasperation caused by repeating the log-off and re-login processes. Hence, the leak of the information appears. But, these drawbacks will not happen in case of passive continuous authentication system. happen in case of passive continuous authentication system.

The system presented in this paper is able to authenticate and memorize both the user's hard and soft biometric information, e.g., face, skin colour are continuously authenticating whether the person using the terminal is as the same valid user as the one login at the beginning. The principal advantage of the initiative CA system can be summarized in four ways.

1) The machine or system is able to recognize who is in front of the terminal.

2) The potential security leaks, such as the user being interim absent from the terminal, are overcome.

3) The passive continuous authentication system keeps the user away from being interrupted by providing the username and password for authentication during online examination..

4) If the user's account and password is stolen by the attacker, the attacker cannot get access to the machine because of the CA system requiring the facial feature and skin color of the authorized user in online exam.

In this paper, an initiative passive CA system by combining the methods in swarm intelligence, face recognition and image or video processing is presented. It aims at automatically overcoming the disadvantage of one time authentication which mentioned above by the biometric features without interrupting the user from his work.
Algorithms in swarm intelligence utilize puny intelligence from the creatures in Mother Nature to solve engineering problems. In the proposed CA system, interactive artificial bee colony (IABC) algorithm is employed to assist the face recognition module for raising the hard biometric recognition rate. The processes of IABC are executed offline to train a weighting mask for adjusting the value of the input image feature. The goal for IABC algorithm to achieve is finding the proper mask to modify the input features. The trained weighting mask is capable of extending the difference between different registered users and narrowing the difference between the registered images from the same user. The relighting module is used to avoid illumination changes.

II.LITERATURE SURVEY

The interest in this continuous authentication field is growing with time due to the immediate need of the security issue existing in the conventional one-time authentication system. The current authentication system widely utilized in our daily life can be classified as the one-time authentication system. It requests the user to enter the account and the corresponding password to login the system. After the login procedure, the account will be kept in the login status until the user logoffs the system. However, during the period of the user using the system, the machine is blind as a mole to identify who is currently using it. To overcome this defect, many CA strategies, models, and Systems have been presented.

A. *Related Works in a continuous authentication System*

A brief review of CA systems using inherence factor to be the authentication core is given as follows. Bae proposed real-time face detection based on hybrid-information extracted from the face space and facial features. Zuo proposed an embedded real-time face recognition system in a networked house environment for triggering personalized services by automatically identifying the user. Janakiraman presented a continuous face verification system to improve the personal system security. Kumar] proposed a Continuous biometric verification scheme to protect interactive login sessions by fusing different biometrics and presented three criteria for CA

.

B. *Swarm Intelligence for Authentication*

Algorithms in swarm intelligence can be utilized to solve problems in many fields. In the authentication or security related field, swarm intelligence algorithms can be used as the key process or an auxiliary module.

C. *Review of IABC algorithm*

IABC, which is a branch of ABC algorithm, is employed to train a weighting mask for adjusting the input features in the hard biometric authentication module. The formula, which takes the location of the employed bees in the consideration for moving the onlooker bees, is modified, and the concept of universal gravitation is introduced into the process in IABC to calculate the interactive affection between different numbers of employed bees.

Step 1) *Initialization: randomly spread ne percent of the* population into the solution space, where *ne indicates* the ratio of employed bees to the total population.

Step 2) *Move the onlookers: move the onlookers by (1) with* roulette wheel strategy.

Step 3) *Move the scouts: when the iteration matches the multiples* of the predefined *Limit iteration, the employed* bees, whose fitness values are not improved, become the scouts. In IABC, two employed bees fitting the condition are remained, and the remaining employed bees satisfying the condition listed above are moved.

Step 4) *Update the near best solution: memorize the near* best fitness value and the corresponding coordinate found so far by the bees.

Step 5) *Termination checking: if the termination condition* is satisfied, exit the program; otherwise, go back to step 2.

We address the problem of unconstrained face recognition ,The main factors that make this problem challenging are image degradation due to blur, and appearance variations due to illumination and pose, so blur/illumination robust algorithm is used.

III. PROPOSED ARCHITECTURE

The proposed passive CA system architecture aims to provide the protection of the candidate presence during online examination. Hence, the whole system is based on software. In this design, the system contains five major modules: the skin color detection module, the face detection module, rotation and normalization module, the face recognition module, and the soft biometric recognition module.

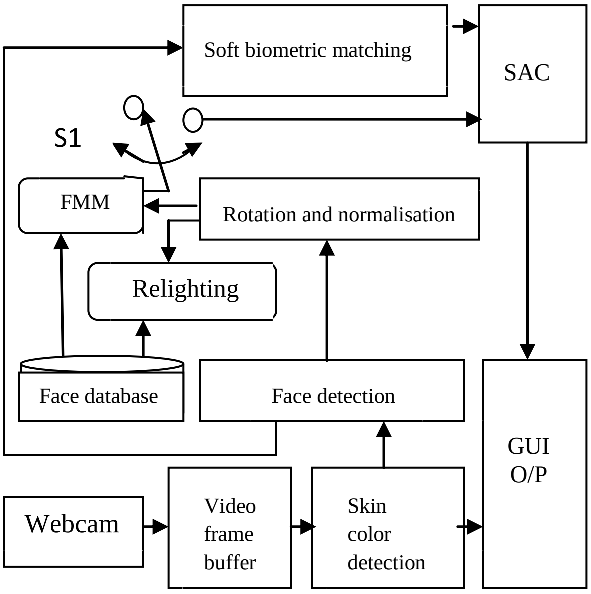

Fig 1: CA system for online examination

The switch *S*1 is controlled by the output of the face matching result. If the input face can be recognized as a registered user in the database, the output will be send directly. On the other hand the input frame will be sent to the soft biometric matching module for the second time recognition in case the input face is not recognizable. The soft biometric matching module requires a stored database from the output of the face matching module with the recognized user face. The soft biometric feature is extracted from that database as a template. If registered user image is not a input to the system, then the system will automatically log out. Hence, the invader access during online exam can be avoided. In the proposed system, the hard biometric is the important feature used in the authentication system, and the soft biometric is employed as a supporting system. Multimodal biometric improve the accuracy rate.Relighting module is employed to avoid illumination changes. An Eigen face with blur-robust face recognition algorithm is used to find identity of the closest gallery image. Improved face recognition accuracy obtained by ORL database by about 3.23% more than Eigen face method. The System Access Control (SAC) unit is used to compare the hard biometric and soft biometric. If hard biometric and soft biometric feature will not match, then system gets log out.

The eye detection module is also built by the boosted classifiers, except that the Haar-like features are replaced by the left eye and right eye features. In rotation and normalisation module, when a face image is sent into this module, the left eye and right eye coordinates are detected within the region of this image. They are also attached to the reference information for rotating the face image to be horizontal. In soft biometric matching module, the pose, the face direction, and the rotation angle of the face affect the detection result directly. For instance, if the candidate turns his head over with a wide angle, the face detection might fail to detect the face even if the skin color detection still indicates that there is a mass of skin color pixels. For the reason mentioned above, this system provides the soft biometric matching in case the user's face is not detected.

A latent SVM approach based person re-identification process is proposed to describe the relations among the low-level part features, middle level clothing attributes, and high-level re-identification labels of person pairs. Continuous attributes based LSVM is more flexible in modelling the uncertainties in attribute value assignments and re-identification label. Verification can be formulated as a binary classification problem, i.e. whether two testing samples belong to the same person or not.

IV. EXPERIMENTS AND RESULTS

To test the performance of the prototype system, two experiments with different data base are performed. The first experiment aims at testing the accuracy of recognition and the second experiment is taken for testing both the accuracy and the usability of the proposed passive continuous authentication system. Initially, the candidate image will taken by using webcam. Then, the video frame buffer is employed to transfer the corresponding information. If, hard and soft biometric feature will not match, then system will log out. In case of lighting changes, the relighting module is employed to avoid such illumination changes. Here IABC algorithm with Eigen face method is used in order to increase accuracy rate.

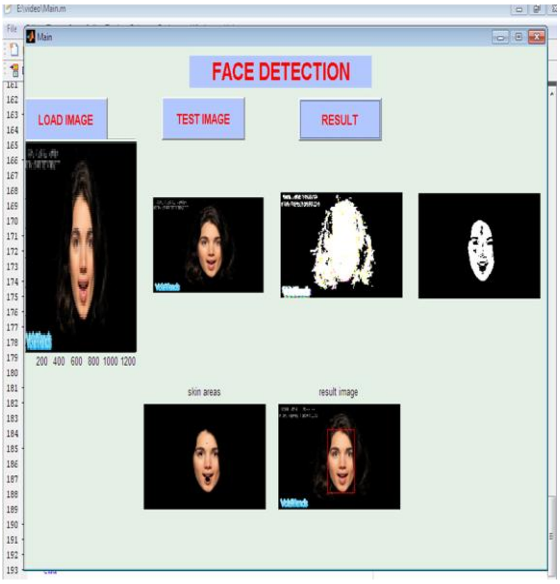

Fig 2: Detection result for authorised candidate

As shown in Fig. 2, the image which taken by webcam is authorised candidate. Hence, further steps will proceed to match the corresponding biometric features. The test image given is same as image in ORL database. The face detection module is used in addition with relighting module. If there is chance for illumination changes then blur and illumination is used. The first three images on the top are the input frame, the face detection result, and the result from the eye detection module. If, and only if, the eye pair is detected, can it trigger the face image rotation process; hence, the eye detection result is not displayed in below figure. The first experiment utilizes ORL database to test the accuracy of the proposed IABC with Eigen face method. In this experiment, six images per user are used to be the training image, and the rest four images are used to be the test images. Since IABC is an optimization algorithm under the branch of evolutionary computing, the results obtained with different random seeds may be different with various input image. The reason is that different random seeds generate different random number sequences. The different random number sequences lead the artificial agents searching in different locations in the solution space. Every user is asked to sit in front of the computer to enter some answers, turn over their face or body as the usual way to read a questions, Hence, the database presents a wide range of skin tones and facial features. Although our continuous authentication system is a hybrid system with both hard and soft biometrics, the hard biometric provides stronger and more reliable information for the authentication. The longer the hard biometric authentication module controls the system output, the more reliable access control is implemented.

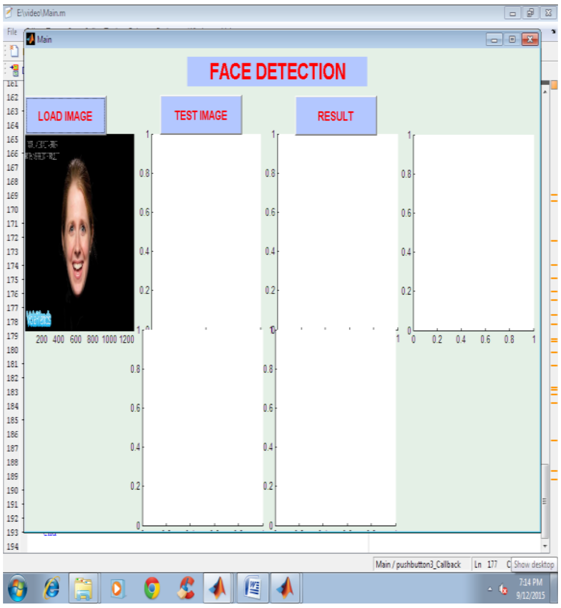

Fig 3: Detection result for unauthorised candidate

V. CONCLUSION

In this paper, an initiative passive continuous authentication system for real-time usage i.e., during online examination was built based on both the hard and the soft biometric features. In addition, IABC optimization algorithm was used to train a weighting mask for assisting the face identification process. Because the training process can be finished offline, the proposed method did not slow down the real-time initiative passive CA system, but improved the recognition accuracy of the face recognition.

The face recognition was designed to be the major part for controlling the authentication result, and the soft biometric matching was employed as the supporting system. The experimental results indicated that the proposed method improved the face recognition accuracy in six over seven test samples.

The proposed system was less weight and was able to operate with low system resources. Hence, this system will suit for wide range of application for authentication of user. With the assistance of the proposed system, the information security on the terminal access right was secured and invader cannot the system during online examination.

REFERENCES

[1] H. Bae and S. Kim, “Real-time face detection and recognition using hybrid-information extracted from face space and facial features,” *Image Vision Comput.*, vol. 23, pp. 1181–1191, Jul. 2005.

[2] M. K. Khurram, P.-W. Tsai, J.-S. Pan, and B.-Y. Liao, “Biometric driven initiative system for passive continuous authentication,” in *Proc. 7th Int. Conf. Inform. Assurance Security*, Dec. 2011, pp. 139–144.

[3] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, “Continuous verification using multimodal biometrics,” *IEEE Trans. Pattern Anal. Mach.Intell.*, vol. 29, no. 4, pp. 687–700, Apr. 2007.

[4] Q. Xiao and X.-D. Yang, “Facial recognition in uncontrolled conditions for information security,” *EURASIP J. Advances Signal Process.*, vol. 2010, pp. 1–9, Feb. 2010.

[5] D. Karaboga, “An idea based on honey bee swarm for numerical optimization,” Comput. Eng. Dept., Eng. Faculty, Erciyes Univ., Kayseri, Turkey, Tech. Rep. TR06, Oct. 2005.

[6] M. S. Packianather, M. Landy, and D. T. Pham, “Enhancing the speed of the bees algorithm using pheromone-based recruitment,” in *Proc. 7th IEEE Int. Conf. Ind. Informatics*, Jun. 2009, pp. 789–794.

[7] P.-W. Tsai, J.-S. Pan, B.-Y. Liao, and S.-C. Chu, “Enhanced artificial bee colony optimization,” *Int. J. Innovative Comput. Inform. Control*,vol. 5, no. 12, pp. 5081–5092, Dec. 2009.

[8] M. C. Ang, d. T. Pham, and K. W. Ng, “Minimum-time motion planning for a robot arm using the bees algorithm,” in *Proc. 7th IEEE Int. Conf.Ind. Informatics*, Jun. 2009, pp. 487–492.

[9] R. Janakiraman, S. Kumar, S. Zhang, and T. Sim, “Using continuous face verification to improve desktop security,” in *Proc. IEEE Workshop Applicat. Comput. Vision*, Jan. 2005, pp. 501–507.