International Journal of Advanced Information Science and Technology (IJAIST) *ISSN: 2319:2682*
Vol.6, No.1, January 2017 DOI:10.15693/ijaist/2017.v6i1.11-17

Biometric traits for Unremitting User Verification system

K.R.Vinothini
Research Scholar
Annamalai University

Dr.B.Shanthi
Professor/ C.I.S.L Department
Annamalai University

***Abstract*— An unremtting user verification system uses both soft and hard biometric traits for authentication. This system is used to authenticate the user by continuously monitoring the user even in different postures. Human facial features and iris are used as hard biometric traits. Skin colour and hair colour are employed as soft biometric traits . The system continuously verifies the user without interrupting on his/her work. It is able to recognise who is in front of the system and it denies the access to invader. In this system face recognition system is implemented using Eigen face method and Intelligent Artificial Bee Colony algorithm. The facial features are used as the main component for face regognition assisted by the skin color. In this paper blur and illumination changes of the face is supported by the Robust Blurr and llumination Algorithm. This algorithm is used to recover original candidate image from blurred image. Due to usage of above algorithm, the accuracy can be increased. The relighting module is used to avoid the illumination changes.**

Index terms - Blur and Illumination algorithm, InABC algorithm, biometric, Unremtting authentication (UA), face recognition, relighting module.

I. INTRODUCTION

For the past few decades the face recognition has been an intensely researched field of computer vision. Humans have used body characteristics such as face, voice, and iris 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 overcome the limitations of the conventional authentication system,an unremitted authentication system is used .In the conventional 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 be overcome from the continuous authentication system.

In this paper, an unremitting authentication system by combining the methods of 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.

In the proposed system, an intelligent artificial bee colony (InABC) 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. RELATED WORK

In [14], a (blur) subspace is associated with each image and face recognition is performed in this feature space. It has been shown that the (blur) subspace of an image contains all the blurred version of the image. However, this analysis does not take into account the convexity constraint that the blur kernels satisfy, and hence the (blur) subspace will include many other images apart from the blurred images. In [12], the local phase quantization (LPQ) [13] method is used to extract blur invariant features. Though this approach works very well for small blurs, it is not very effective for large blurs. The third approach is the direct recognition approach. This is the approach taken in [13] and by us. In [13], artificially blurred versions of the gallery images are created and the blurred probe image is matched to them. Again, it is not possible to capture the whole space of blur kernels using this method. We avoid this problem by optimizing over the space of blur kernels. Finally, the fourth approach is to jointly deblur and recognition the face image [12]. However, this involves solving for the original sharp image, blur kernel andidentity of the face image, and hence it is a computationally intensive approach. Set theoretic approaches for signal and image restoration have been considered. In these approaches the desired signal space is defined as an intersection of closed convex sets in a Hilbert space, with each

set representing a signal constraint. Image de-blurring has also been considered in this context [13], where the non-negativity constraint of the images has been used to restrict the solution space. We differ from these approaches as our primary interest lies in recognizing blurred and poorly illuminated faces rather than restoring them. 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 InABC algorithm

InABC, which is a branch of IABC 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 InABC to calculate the interactive affection between different numbers of employed bees.

Step 1) **Initialization**: randomly spread n 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 InABC, 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.

The main factors that make the face recognition challenging are image degradation due to blur, and appearance variations due to illumination and pose, so Robust blur and illumination algorithm is used.

Face recognition from blurred images can be classified into four major approaches. In the first approach, the blurred image is first deblurred and then used for recognition. The drawback of this approach is that they first need to solve the challenging problem of blind image deconvolution. In the second approach, blur invariant features are extracted from the blurred image and then used for recognition[10] and [11]; It has been shown that the (blur) subspace of an image contains all the blurred version of the image. However, this analysis does not take into account the convexity constraint that the blur kernels satisfy, and hence the (blur) subspace will include many other images apart from the blurred images. In recent years, person re-identification has attracted growing attention in computer vision community. Studies on person re-identification can be roughly divided into two categories, i.e. feature and learning. For feature, color histograms and local texture descriptors are commonly utilized. Besides, Ad Hoc features are also proposed, including local motion features [14], shape and appearance context features [2] and the symmetry-driven accumulated local features. Attributes information has been utilized in computer vision in recent years. Liu et al. [15] use an information theoretic approach to discover the attributes of human actions automaticaly. The inffered attributes are embedded into a latent SVM classifier for action recognition.

III. OBJECTIVES & OVERVIEW OF THE PROPOSED MECHANISM

A. Objectives

- To recognize who is in front of the terminal. and to decide whether to obey the command from the user.
- To overcome the potential security leaks, such as the user being temporarily absent from the terminal.
- The unremitting authentication keeps the user away from being interrupted by providing the username and password for authentication.
- If the user's account and password is stolen by the invader, the invader cannot get access to the machine because of the authentication

system requires the facial feature and skin colour of the authorized user.

B. Overview of the Proposed Mechanism

The proposed Unremittng Authenticaton system architecture aims to provide verification using face recognition and skin color. Hence, the whole system is based on software. In this design, the system contains two major modules: the face detection module (Hard biometrics) and the skin color detection module (Soft biometrics).

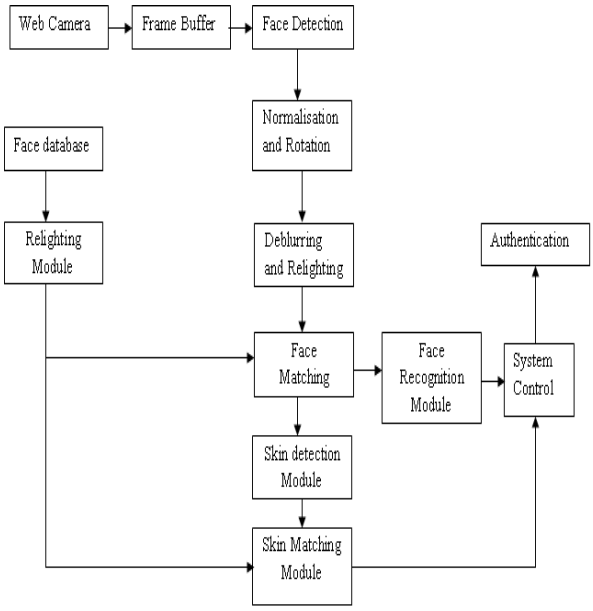

Figure 1. Face Recognition and Skin Detection Module

The webcamera is used to capture the video image. Then the captured image is stored in the video frame buffer(Figure.1). If the input face can be recognized as a registered user in the face database, the output will be send directly. On the other hand the input frame will be sent to the soft biometric skin 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 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. The System Control (SC) 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. . If hard biometric and soft biometric features are matched, then system produces Authentication.

In rotation and normalisation module, when a face image is sent into this module, 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.

IV. EXPERIMENTAL RESULTS

Face recognition from blurred images can be classified into four major approaches. In the first approach, the blurred image is first deblurred and then used for recognition. The drawback of this approach is that we first need to solve the challenging problem of blind image deconvolution. Though there have been many attempts at solving the blind deconvolution problem it is an avoidable step for the face recognition problem. In statistical models are learned for each blur kernel type and amount; this step might become infeasible when we
try to capture the complete space of blur kernels. In the second approach, blur invariant features are extracted from the blurred image and then used for recognition. 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 Unremitted system can be summarized in four ways.

The algorithm for recognizing blurred image is given below.

Algorithm: Direct Recognition of Blurred Faces
Input: (Blurred) probe image and a set of gallery images
Output: Identity of the probe image
1. For each gallery image, find the optimal blur kernel by solving either or its robust version
2. Blur each gallery image with its corresponding and extract LBP features.
3. Compare the LBP features of the probe image with those of the gallery images and find the closest match

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 unremtting authentication system. Initially, the candidate image will be 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 InABC algorithm with Eigen face method is used in order to increase accuracy rate.

An obvious approach to recognizing blurred faces would be to deblur the image first and then recognize it using face recognition technique.

Figure 2. Input video screen

The Input Video image is shown in the Figure 1.

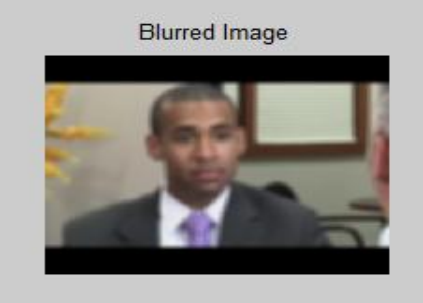

Figure 3(a). Blurred Image

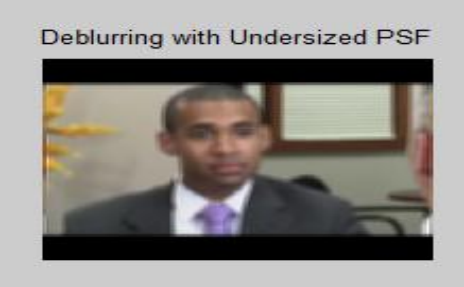

Figure 3(b). Deblurred Image with Undersized Point Spread Function

Figure 3(c). Deblurred Image with Overesized Point Spread Function

Figure 3(d) .Deblurred Image with intial Point Spread Function

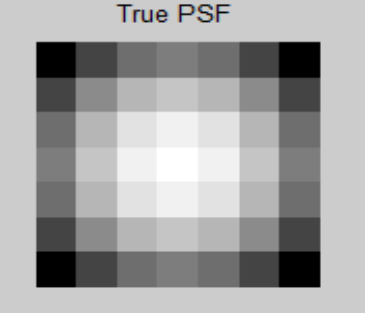

Figure 3(e). True Point Spread Function

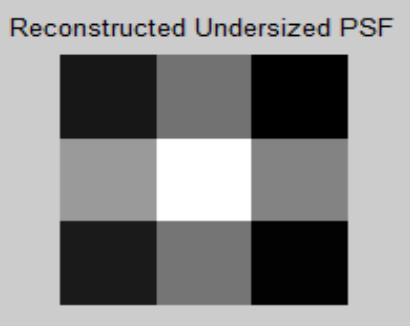

Figure 3(f). Reconstructed Undersized Point Spread Function

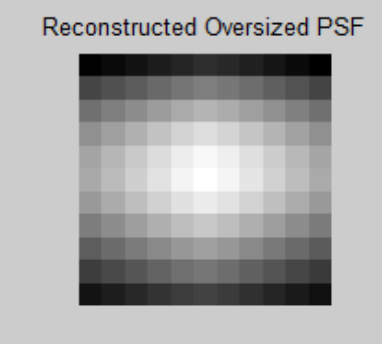

Figure 3(g). Reconstructed Oversized Point Spread Function

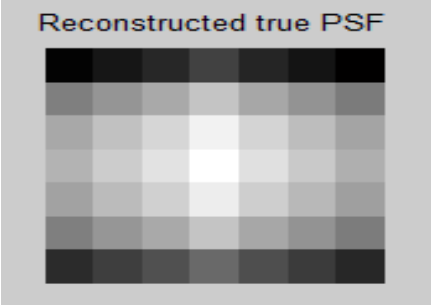

Figure 3(h). Reconstructed True Point Spread Function

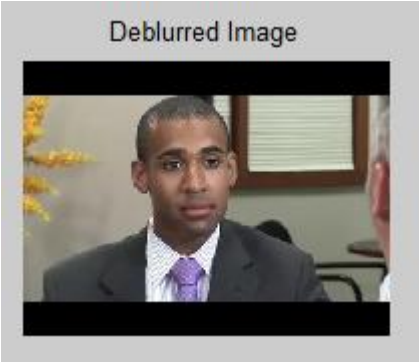

Figure 3(i) Deblurred Image

As shown in Figure 3(a)-(i), the blur and illumination algorithm is used to recover original database image from the video sample image. In the algorithm proposed above, the weight-matrix Ws used to make them robust to outliers due to non-rigid variability (like facial expressions) and misalignment. They also help reduce the importance of pixels in the low-frequency regions of the face in the kernel-estimation step. This is desirable as the effects of blur are not really perceivable in these regions. In this algorithm prior knowledge on the type of blur as constraints can be easily incorporated. Using the low-dimensional linear subspace model for illumination, the set of all images obtained from a given image by blurring and changing its illumination conditions is a bi-convex set is been showed.

As shown in Figure 4, the input image is captured using the webcam. This input image face is detected and checked for matching in the face database module . Hence, further steps will proceed to match the corresponding biometric features.

As shown in Figure 5, the face is detected by using the InABC algorithm by comparing with the face database module and it is checked for authorisation . The face detection module is used in addition with relighting module. If there is chance for illumination changes then blur and illumination is used.

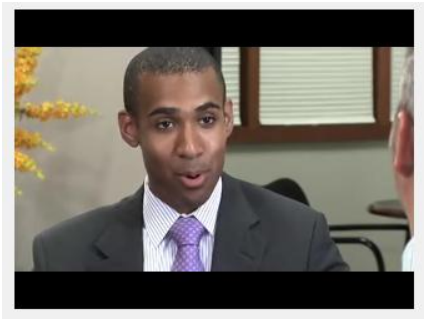

Figure 4.Input image captured by the Webcam

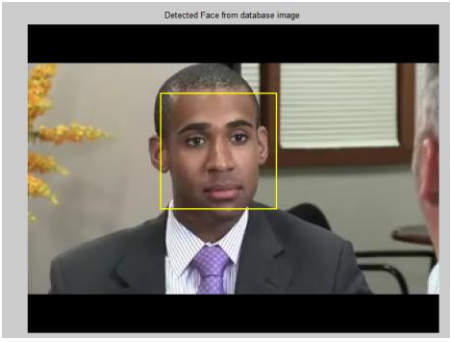

Figure 5. Detected face with the Database image

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 unremitting 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.

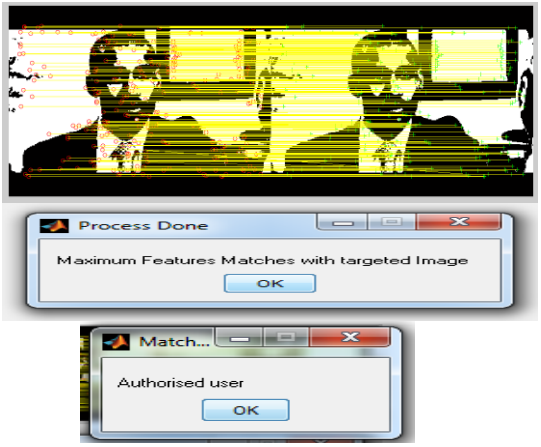

Figure 6. Maximum features matches and authentication is provides

The first experiment utilizes face database module to test the accuracy of the proposed InABC 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 InABC is an optimization algorithm under the branch of evolutionary computing, the results obtained with different random seeds may be different with various input image.

Initially, the image taken by webcam compared with the face database module . As shown in Fig. 5 If database image is same as video sample image, then it indicates authorised user result. If database image is different from image taken by webcam, then it refers unauthorised candidate (Figure 6).As shown in Figure 7(a) and (b), the InABC algorithm is used feature matching between database image and video sample image.

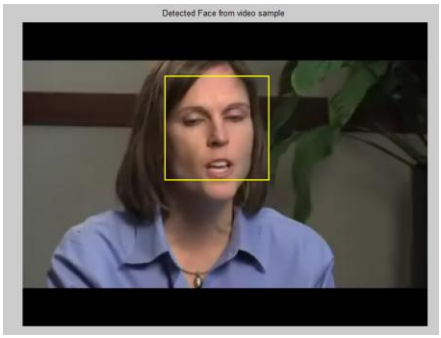

Figure 7(a). Database image different from video sample image

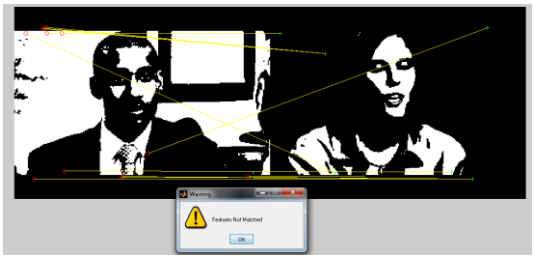

Figure 7(b). Feature not Matched indicates the unauthorised user.

The features not matched with unauthorised candidate which is shown in Figure.7(b).If the unauthorised user comes and sits in front of the terminal then the detected face of the unauthorised person will not match with the database face module and so the features are not matching and the unauthorised user is not provides any authentication and that user cannot use the terminal.Figure. 8 determines the detected face of the unauthorised user.

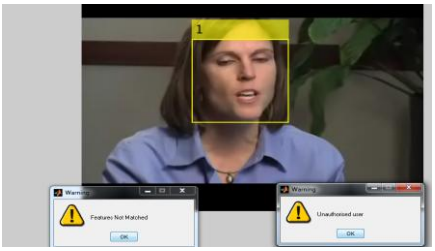

Figure 8.Detected face of the unauthorised user.

For the detection of the skin region the skin extraction algorithm is used . First the input image is provded with the lighting compensation and then the skin regions [Figure 9(a) & 9(b)]are extracted and then the noise are removed from the skin regions.Then the bounding regions are generated and the skin regions(Figure 10) of the input image is detected. The authorized user with detected face is checked for the skin matching in the skin matching module and the authentication is provided. Thus both the hard biometrics(face)and soft biometrics(skin color)are used for unremitting authentication of the user.

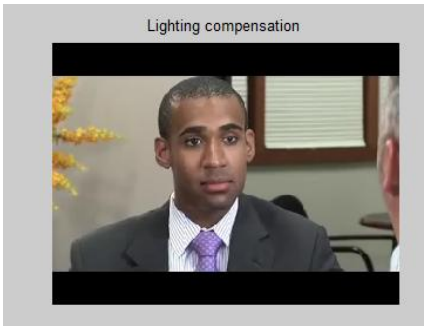

Figure 9(a). Lighting Compensation

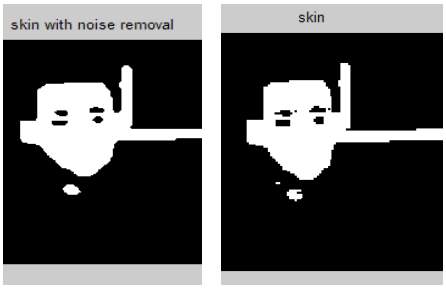

Figure 9(b).Skin region with removal of Noise

Figure 10: Skin detected from the detected face

V. CONCLUSION

In this paper, an unremitting authentication system for real-time usage was built based on both the hard and the soft biometric features. In addition, InABC 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 unremitting system, but improved the recognition accuracy of the face recognition. The algorithms used can tackle the challenging problem of face recognition in uncontrolled settings. 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 access the system.

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.

[10] *T. Ahonen, E. Rahtu, V. Ojansivu, and J. Heikkila, "Recognition of blurred faces using local phase quantization," in International Conference on Pattern Recognition, 2008.*

[11] R. Gopalan, S. Taheri, P. Turaga, and R. Chellappa, "A blur-robust descriptor with applications to face recognition," IEEE Trans Pattern Anal. Mach. Intell., 2012.

[12] T. Ahonen, E. Rahtu, V. Ojansivu, and J. Heikkila, "Recognition of blurred faces using local phase quantization," in International Conference on Pattern Recognition, 2008.

[13] V. Ojansivu and J. Heikkil, "Blur insensitive texture classification using local phase quantization," in Image and Signal Processing. Springer Berlin / Heidelberg, 2008.

[14] R. Gopalan, S. Taheri, P. Turaga, and R. Chellappa, "A blur-robust descriptor with applications to face recognition," IEEE Trans Pattern Anal. Mach. Intell., 2012.

[15] J. Liu, B. Kuipers, and S. Savarese, "Recognizing Human Actions by Attributes," in IEEE Conference on Computer Vision and Pattern Recognition, 2011, pp. 3337–3344

Authors Profile

K.R.Vinothini received the **B.E.** degree in Electronics and Communication Engineering from the A.V.C College of Engineering, Mayiladuthurai, in the year 2002.Completed M.E**.** in Power Electronics and Drives in Jerusalem college of Engineering, Pallikaranai, Chennai,in the year 2006. Currently doing research in the field of Digital Image processing ,in Annamalai University. She has been working as Assistant Professor/ECE in AVC College of Engineering, Mayiladuthurai for the past 10 years.

Dr.B.Shanthi was born in 1970 in Chidambaram. She has obtained B.E (Electronics and Instrumentation) and M.Tech (Instrument Technology) from Annamalai University and Indian Institute of Science, Bangalore in 1991 and 1998 respectively. She obtained her Ph.D. in Power Electronics from Annamalai University in 2009. She is presently a Professor in Central Instrumentation Service Laboratory of Annamalai University where she has put in a total service of 24 years since 1992. Her research papers (65) have been presented in various international /national seminars/conferences. She has 47 publications in national journals and 61 in international journals. Her areas of interest are: modeling, simulation and intelligent control for MLI and Z-source inverters.