IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 4, April 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104155|

Interactive Artificial Bee Colony Supported Passive Continuous Authentication System

Dipu Jose[1], Saji.M. G[2]

Lecturer in Computer Engineering, Government Polytechnic College Nedumangad, Kerala, India[1]

Lecturer in Computer Engineering, Government Polytechnic College, Nedumangad, Kerala, India[2]

ABSTRACT: This paper presents a Passive Continuous Authentication (CA) system that enhances security by continuously verifying users through facial recognition and clothing color, preventing unauthorized access when the user steps away. By integrating swarm intelligence, face recognition, and image processing, the system ensures only the authorized user can control the system. Using the Interactive Artificial Bee Colony (IABC) algorithm, it improves authentication accuracy and system efficiency. Future enhancements will explore additional biometric modalities and optimization techniques like 2D-PCA or LDA for better computational performance.

I. INTRODUCTION

The traditional authentication method relies solely on usernames and passwords for login. This creates a security vulnerability because it doesn't continuously verify the actual user at the machine. If the authorized user steps away, anyone can potentially gain access and misuse the account. This paper introduces a Passive Continuous Authentication (CA) system to enhance security. Unlike traditional one-time authentication, which relies solely on login credentials, this system continuously verifies the user's identity using biometric information like facial features and clothing color. This eliminates the risk of unauthorized access when the user steps away and prevents interruptions for repeated logins. By integrating swarm intelligence, face recognition, and image/video processing, the system ensures that only the authorized user can access and control the machine, even if their login credentials are compromised.

The principal strong points of the initiative passive CA system can be summarized in four ways.

1) The machine is able to recognize who is in front of the terminal. Furthermore, it is able to decide whether to obey the command from the user.

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

3) The passive CA keeps the user away from being interrupted by providing the username and password for authentication.

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

II. AUTHENTICATION SYSTEMS AND FEATURES

The current authentication machinery widely utilized in our daily life can be classified as the one-time authentication system. In every authentication system, at least one of the factors, namely, knowledge factors, ownership factors, and inherence factors , is used to be the recognition core.

2.1 Limitations of Traditional Authentication:

a. **One-Time Authentication:** Current systems primarily rely on usernames and passwords for initial login.
b. **Lack of Continuous Verification:** After initial login, the system doesn't actively monitor who is using the machine.
c. **Security Vulnerability:** This lack of continuous verification allows unauthorized individuals to access the system if the legitimate user steps away.
d. **Need for Passive Continuous Authentication (CA):**
e. **Enhanced Security:** CA systems aim to address the security shortcomings of traditional authentication.
f. **Continuous User Verification:** They continuously monitor user presence to prevent unauthorized access.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104155|

III. SECURITY THROUGH SWARM INTELLIGENCE

Swarm Intelligence (SI) is a field of AI inspired by the collective behavior of social insects like bees. It leverages concepts like self-organization and division of labor to solve complex problems.

Key Characteristics of SI:
Self-Organization: Individuals act locally but collectively achieve global goals.
Adaptability: Systems can adapt to changes in the environment.
Efficiency: Benefits include scalability, fault tolerance, and speed.

Application in Authentication:
Artificial Bee Colony (ABC) Algorithm: A popular SI algorithm inspired by bee foraging behavior.
Interactive Artificial Bee Colony (IABC): A variant of ABC used in the proposed CA system to enhance face recognition accuracy.

IV. EXISTING SYSTEM

4.1 ABC ALGORITHM

The Artificial Bee Colony (ABC) algorithm is an optimization technique inspired by the foraging behavior of honeybees. It simulates a simplified bee colony with three types of bees:
Employed Bees: Explore and exploit known food sources (potential solutions).
Onlooker Bees: Observe the employed bees' reports and choose promising food sources.
Scout Bees: Randomly search for new food sources when existing ones are depleted.

This process mimics how bees search for and exploit food sources, with employed bees sharing information about their findings with onlooker bees. In the ABC algorithm, food sources represent potential solutions to an optimization problem, and their "nectar amount" corresponds to the quality (fitness) of the solution.

4.2 IABC ALGORITHM

In the proposed CA system, **Interactive Artificial Bee Colony (IABC)** [8] **algorithm**, which is a branch of ABC algorithm, is employed to assist the face recognition module for raising the hard biometric recognition rate.
The Interactive Artificial Bee Colony (IABC) algorithm is employed offline to train a weighting mask within the hard biometric authentication system. This mask dynamically adjusts the importance of input features, aiming to maximize the inter-class distance (between different users) while minimizing the intra-class distance (within the same user's registered images). This optimized weighting scheme enhances the accuracy and robustness of the biometric authentication process.
The process of IABC is given as follows.
Step 1) ***Initialization***: randomly spread n_e percent of the population into the solution space, where n_e indicates the ratio of employed bees to the total population.

Step 2) ***Move the onlookers***: move the onlookers by (1) with roulette wheel strategy based on the probabilities calculated by (2)

$$X_i(t+1)= \Theta_{i+} \sum_{k=1}^{e} \{ \tilde{F}_{ik} \bullet [\Theta_i(t) - \Theta_k(t)] \} \qquad (1)$$

where X_i denotes the coordinate of the ith onlooker bee, t indicates the iteration number, Θ_i and Θ_k are the coordinates of the ith employed bee and the randomly chosen employed bee, respectively, e is the number of the selected employed bees, and $\tilde{F}_{ik}$ is the normalized gravitation

$$Pi = F(\Theta_i) / \sum_{k=1}^{s} F (\Theta_k) \qquad (2)$$

where P_i is the probability of selecting the ith employed bee, and S indicates the total number of the employed bee.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104155|

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 by

$$\Theta_i = \min\{\Theta_i\} + [\max\{\Theta_i\} - \min\{\Theta_i\} \bullet R] \qquad (3)$$

where R is a random variable vector and $R \in [-1, 1]$.

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.

V. PROPOSED DESIGN AND ARCHITECTURE

The proposed passive CA system architecture aims to provide the protection of the computer system. In this design, the system contains six major modules: the skin color detection module, the face detection module, the eye detection module, rotation and normalization module, the face recognition module, and the soft biometric recognition module.

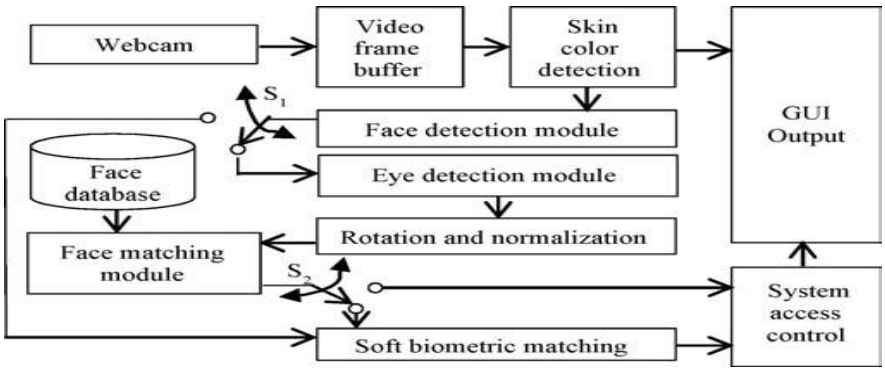

Figure. 4.1. Architecture of the passive CA system.

Switch S1 bypasses face detection when no human face is detected in the input frame. Otherwise, detected faces are sent to the eye detection module and switch S2 Routes the output based on face matching results:

- *Successful Match*: Output is sent directly.
- *Unsuccessful Match*: Input frame is sent to the soft biometric matching module for secondary verification.
- *Soft Biometric Role:* Acts as a supporting mechanism, used only when the primary hard biometric matching fails.

5.1 Webcams and Video Frame Buffers:

Most laptops have built-in webcams, and external webcams are easily connectable via USB.
Video frame buffers are dedicated memory spaces within the computer's memory to store video frames.

5.2 Skin Color Detection:

Skin color detection is the initial step in the system.Color space transformation is necessary to mitigate the impact of varying lighting conditions on skin color detection.The system utilizes RGB to YC_bC_r color model transformation to filter out the nonskin regions because it is easy to implement and has been confirmed that the YC_bC_r color model provides good coverage of different ethnicities. In the experiment, the thresholds for the skin color detection are set by

$$\begin{matrix} Y \\ C_b \\ C_r \end{matrix} \in \begin{bmatrix} 65, & 253 \\ 105, & 125 \\ 138, & 168 \end{bmatrix} \qquad (4)$$

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104155|

5.3Face Detection Module

The face detection module in this system is implemented by an open source computer vision library, namely, OpenCV. The face detection algorithm built in the OpenCV library is constructed based on a cascade of boosted classifiers, which work with Haar-like features. The input frame is converted into gray-scale for face detection. Because the face detection is based on the boosted classifiers with Haar-like features, sometimes a shape similar to a human face will also be detected even if that shape is not composed of human skin color pixels. Therefore, the information obtained from the skin color detection module is utilized to assist in checking whether the detected face region is a potential human face by the criterion listed in

$$f_i \in \begin{cases} \text{face region}, & \text{if } \sum_{j \in skin} x_j / \sum x_j \geq 0.5 \\ \text{nonface region}, & \text{otherwise} \end{cases} \quad (6)$$

where f_i denotes the potential face region located by the classifier and x_j indicates the pixels in the C_r channel corresponding to the same location of f_i.

(a) (b) (c)

Figure. 4.2. Example of face detection result. (a) Frame captured by the webcam.
(b) Detected skin color region. (c) Detected face region.

5.4 Eye Detection Module

The eye detection module is also built by the same boosted classifiers, except that the Haar-like features are replaced by the left eye and right eye features, respectively. It is possible to locate multi faces in the result, and hence the eye detection result may have more than one left or right eye detected.

5.5. Rotation and Normalization

When a face image is sent into this module, the left eye and right eye coordinates, which are detected within the region of this image, are also attached to be the reference information for rotating the face image to be horizontal. Assume that the input eye coordinates of an image are $(x1, y1)$ and $(x2, y2)$. Let $x1 \leq x2$. The predicted rotation angle θ can be found by

$$\theta = \cos^{-1}\left[\frac{(x_2 - x_1)}{\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}}\right] \quad (7)$$

where θ is the rotation angle in radian.

The eye detection module is also built by the same boosted classifiers, except that the Haar-like features are replaced by the left eye and right eye features, respectively. It is possible to locate multi faces in the result, and hence the eye detection result may have more than one left or right eye detected.

5.5. Rotation and Normalization

When a face image is sent into this module, the left eye and right eye coordinates, which are detected within the region of this image, are also attached to be the reference information for rotating the face image to be horizontal. Assume that the input eye coordinates of an image are $(x1, y1)$ and $(x2, y2)$. Let $x1 \leq x2$. The predicted rotation angle θ can be found by

$$\theta = \cos^{-1}\left[\frac{(x_2 - x_1)}{\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}}\right] \quad (7)$$

where θ is the rotation angle in radian.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104155|

5.6. Face Matching Module

The Eigenface method is used for face recognition. For each registered user, six facial images are stored with their corresponding eigenvectors and eigenvalues. The number of eigenvectors used to reconstruct the images is determined by a criterion, which likely optimizes for accuracy while minimizing computational cost.

$$R^2 = \frac{\sum_{i=1}^{n} \lambda_i}{\sum_{j=1}^{r} \lambda_j} \text{ subject to } R^2 \geq 0.85 \text{ and } n \leq r \qquad (8)$$

where R^2 is the variance ratio, r is the total number of eigen vectors, n denotes the number of eigen vectors used to rebuild the image, and λ represents the eigen value.
Without the support from IABC, the Euclidean distance is calculated by

$$dpq = \|(EVp - EVq)\| \qquad q = 1, 2, \ldots, (u \times c) \qquad (9)$$

where EVp and EVq present the 1-by-($n \times l$) eigen vectors of the test image p and the qth image in the database, respectively, L is the length of one eigen vector, d_{pq} denotes the distance between p and q, u is the number of registered users in the database, and c indicates the number of images
per user stored in the database.

In this design, IABC is employed to create a weighting mask for adjusting the importance of the eigen vectors, which are used for decomposing the face image in the Eigenface method, in the training phase of the prototype system. The common measurements used in the field of clustering, e.g., the within distance and the between distance, are utilized to construct the fitness function.

The weighting mask is trained by IABC, and it is a 1-by-n vector. In addition, the weighting mask is defined by

$$M = [m_1, m_2, \ldots, m_n] \qquad (10)$$

where M is the mask and m_i is the ith element presenting the weighting of the ith eigenvector.
Suppose the distances between test image p to all images stored in the database are calculated by (9) and the results are permuted into a 1-D vector, which is formularized by

$$Dpq = [dp1, dp2, \ldots, dp(u \times c)]. \qquad (11)$$

Thus, the within distance and the between distance can be formularized by

$$d_{v_{\text{within}}} = \sum_{v=1}^{u} \sum_{s=2}^{c} [d_{p(v \times c+s)} - d_{p(v \times c+s-1)}] \qquad (12)$$

$$d_{v_{\text{between}}} = \sum_{v=2}^{u} (center_v - center_{v-1}) \qquad (13)$$

where $d_{v\text{within}}$ indicates the within distance, $d_{v\text{between}}$ denotes the between distance, and $center_v$ means the class center, which is defined by

$$center_v = \left[\sum_{s=1}^{c} d_{p(v \times c+s)} \right] / c, \quad v = 1, 2, \ldots, u. \qquad (14)$$

Hence, the fitness function for the IABC process can be formularized by

$$\min \quad F(X) = \alpha \sum_{v=1}^{u} d_{v_{\text{within}}} + \frac{1}{\alpha \sum_{v=1}^{u} d_{v_{\text{between}}}} \qquad (15)$$

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104155|

where α is a constant scalar for adjusting the ratio of the within distance to the between distance, and the goal of the optimization is to minimize the outcome of the fitness function.

Straining the trained weighting mask from a 1-by-n vector to a 1-by-($n \times l$) vector by reproducing every element l times, the weighting mask is formularized by

$$M^{\#} = [m_{11}, m_{12}, \ldots m_{1l}, m_{21}, m_{22}, \ldots, m_{2l}, \ldots, m_{nl}] \qquad (16)$$

where $M^{\#}$ denotes the repermuted weighting mask by reproducing every element from M.
Therefore, the trained weighting mask is involved in the recognition process to calculate the inner product of the weighting mask and the distances between the test images to the images in the database by

$$d_{pq} = M^{\#} \cdot (EVp - EVq),\ q = 1, 2, \ldots, (u \times c). \qquad (17)$$

Consequently, the system uses PCA for face recognition, employs IABC-trained weights to improve matching accuracy, and utilizes a threshold *Trcg* to determine the validity of the match. If the match is invalid, soft biometric matching is triggered as a secondary verification step.

5.7. Soft Biometric Matching

Essentially, soft biometric matching, specifically clothing color analysis, is used as a secondary authentication method when face detection fails, enhancing the system's robustness.

To reduce computational overhead, only clothing color is used as the soft biometric feature. Skin color detection helps locate the upper body region, and a bounding box is defined to focus on this area. The system then compares color histograms of the current frame and a stored frame containing a previously recognized face. The average difference in RGB channels between these histograms determines the soft biometric authentication result.

Figure 4.4. Detected soft biometric information based on the input frame given in Fig. 4.2.

Moreover, an adjustable threshold is used to judge the authentication result by calculating the average luminance of the soft biometric block. The criteria for the soft biometric matching are listed in the following equations:

$$\mathrm{CA}_{\mathrm{res}} = \begin{cases} \text{pass}, & \text{if } C < T_{\mathrm{cf}} \\ \text{fail}, & \text{otherwise} \end{cases} \qquad (18)$$

$$C = \begin{cases} 0, & \text{if } \sum_{\mathrm{R,G,B}} |h_{\mathrm{cur}} - h_{\mathrm{pre}}| < T_{\gamma} \\ C + 1, & \text{otherwise} \end{cases} \qquad (19)$$

$$T_{\gamma} = \begin{cases} 11\,000, & \text{if } 130 < \mu_{\mathrm{cur}} \\ 8000, & \text{if } 110 < \mu_{\mathrm{cur}} \leq 130 \\ 6000, & \text{if } 40 < \mu_{\mathrm{cur}} \leq 110 \\ 4800, & \text{otherwise} \end{cases} \qquad (20)$$

where CA_{res} denotes the authentication result, C is a counter storing the continuous soft biometric authentication failure, T_{cf} is a threshold for the acceptable continuous soft biometric authentication failure, h_{cur} and h_{pre} indicate the histogram

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104155|

acquired from the bounding box in the current frame and the latest stored frame with the recognized face, respectively, T_γ is the threshold to decide whether the authentication is passed in the current frame, and μ_{cur} indicates the mean luminance of the current bounding box. The threshold T_{cf} is designed to increase the toleration of the system for some case that the user has a mass movement in a very short time or his movement is too large to stay in the screen for a short time period in seconds.

VI. EXPERIMENTS AND RESULTS

Two experiments were conducted to evaluate the prototype system. The first experiment focused on recognition accuracy, while the second assessed both accuracy and usability of the passive continuous authentication (CA) system. Both experiments were performed on a Lenovo X201s laptop running Windows 7 with an Intel Core-i7 L640 2.13 GHz CPU. For the second experiment, test videos were captured using a Logitech C510 webcam at a resolution of 640x360 pixels.

6.1.Accuracy Test With ORL Database

The first experiment evaluates the accuracy of the proposed IABC-enhanced Eigenface method using the ORL face database. This database contains variations in facial expressions, lighting, and poses, simulating real-world conditions. Six images per subject are used for training, and the remaining four for testing. The IABC algorithm is executed with 20 different random seeds to assess the robustness of the results. Key parameters for the IABC algorithm, such as population size, number of employed bees, and the limit parameter, are set.

The experiment measures the recognition rate, considering factors like mean, maximum, minimum, standard deviation, and mode to account for the inherent randomness of the IABC algorithm.

The IABC process is executed with 120 iterations and is repeated in 20 runs with different random seeds but the same input data. The population size is set to 16, the number of the selected employed bee is set to 3, the parameter *Limit* is set to 1, and the ratio of employed bees to onlooker bees is 1:1. The IABC process is terminated within an acceptable recognition result. The recognition rate is given in Table I.

Method	Eigenface With regular PCA	IABC Supported Eigenface Method
Recognition rate (mode)	83.75%	86.88%
Max. recognition rate	N/A	86.88%
Min. recognition rate	N/A	84.38%
Recognition rate (mean)	N/A	86.34%
Standard deviation	N/A	0.0099

Table 6.1 Recognition Results From Eigenface With Regular PCA Decomposition and From IABC Supported Eigenface Method

The IABC-enhanced Eigenface method demonstrates improved accuracy and stability compared to the traditional approach, indicating the effectiveness of the IABC optimization in enhancing face recognition performance.

- **IABC Performance:** IABC requires multiple runs with different random seeds due to its evolutionary nature.
- **Accuracy Improvement:** The IABC-enhanced method shows a 3.13% improvement in recognition accuracy compared to regular PCA.
- **Stability:** The IABC method exhibits low standard deviation (0.0099), indicating stable performance.
- **Convergence:** The IABC algorithm converges to a near-optimal solution, as evidenced by the stable decrease in the fitness function.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104155|

VII. CONCLUSION

This research presents an innovative passive continuous authentication (CA) system that integrates both hard and soft biometric features for enhanced security. By incorporating an Interactive Artificial Bee Colony (IABC) algorithm, the system significantly improves face recognition accuracy compared to traditional methods. IABC optimizes feature weights, leading to better discrimination between users and within-user variations. The system demonstrates effective real-time performance with minimal impact on system resources. While the current implementation focuses on facial recognition and clothing color as the primary and secondary authentication factors, future work can explore extending IABC to other biometric modalities and incorporating 2D-PCA or LDA for dimensionality reduction and improved computational efficiency.

REFERENCES

[1] 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.
[2] 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.
[3] S. K. Singh, D. S. Chauhan, M. Vtsa, and R. Singh, "A robust skin color based face detection algorithm," *Tamkang J. Sci. Eng.*, vol. 6, no. 4, pp. 227–234, Sep. 2003.
[4] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 1. Dec. 2011, pp. I511–I518.
[5] E. Bonabeau, M. Dorigo, G. Theraulaz, Swarm Intelligence: From Natural to Artificial Systems, Oxford University Press, Inc., New York, NY, USA, 1999.
[6] I. Kassabalidis, M.A. El-Sharkawi, R.J. II Marks, P. Arabshahi, A.A. Gray, Swarm intelligence for routing in communication networks, Global Telecommunications Conference, GLOBECOM '01, 6, IEEE, 2001, pp. 3613–3617.
[7] D. Karaboga, An Idea Based On Honey Bee Swarm for Numerical Optimization, Technical Report TR06, Erciyes University, Engineering Faculty, Computer Engineering Department, 2005.
[8] T.D. Seeley, The Wisdom of the Hive: The Social Physiology of Honey Bee Colonies, Harvard University Press, 1995.
[9] M. Karnan and M. Akila, "Personal authentication based on keystroke dynamics using soft computing techniques," in *Proc. Int. Conf. Commun. Softw. Netw.*, Feb. 2010, pp. 334–338.
[10] 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.
[11] 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.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details