International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.06, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

HYBRID BACTERIAL FORAGING ALGORITHM FOR CONTINUOUS AUTHENTICATION SYSTEM IN BIOMETRICS

K.R.Vinothini[1] ,Dr.B.Shanthi[2]

Assistant Professor /ECE & Research Scholar[1] , C.I.S.L Department[2]

A.V.C college of Engineering[1] , Annamalai University[2]

ABSTRACT

Security of computer systems is facing a lot of threats and difficulties mainly with the technological aspects and remote access. It has been found that ensuring confidential access to only authorized users and protecting the privacy of their personal and transactional information might limit the influence of the confronted attacks. Authentication systems are supposed to meet three basic requirements, called availability, integrity, and confidentiality, against various attacks. In this work, Local Binary Pattern (LBP) is used for the feature extraction and features given to the Adaboost classifier. Eigen face method also used and it is optimized through the hybrid technique Bacterial Forging Optimization (BFO) with Stochastic Diffusion Search (SDS) algorithm with incorporates the concepts from BFO and SDS and it creates individuals in a new generation. This BFO-SDS method performs local search through the chemotactic movement of BFO and the global search over the entire search domain is accomplished by a SDS algorithm. Experimental results show that the proposed method achieves better performance than other methods.

Keywords: *Biometrics, Continuous Authentication System, Local Binary Pattern (LBP), Adaboost and Eigen Face Method, Bacterial Foraging Optimization (BFO) and Stochastic Diffusion Search (SDS).*

1INTRODUCTION

Today's e-security are in critical need of finding accurate, secure and cost-effective alternatives to passwords and Personal Identification Numbers (PIN) as financial losses increase dramatically year over year from computer-based fraud such as computer hacking and identity theft. Biometric solutions address these fundamental problems, because an individual's biometric data is unique and cannot be transferred. Biometrics which refers to identifying an individual by his or her physiological or behavioral characteristics has capability to distinguish between authorized user and an imposter. An advantage of using biometric authentication is that it cannot be lost or forgotten, as the person has to be physically present during at the point of identification process. Biometrics is inherently more reliable and capable than traditional knowledge based and token based techniques. The commonly used biometric features include speech, fingerprint, face, Iris, voice, hand geometry,

retinal identification, and body odor identification [1].

Information security is concerned with the assurance of confidentiality, integrity and availability of information in all forms. There are many tools and techniques that can support the management of information security. But system based on biometric has evolved to support some aspects of information security. Biometric authentication supports the facet of identification, authentication and non-repudiation in information security. Biometric authentication has grown in popularity as a way to provide personal identification. Individual passwords, pin identification or even token based arrangement all have deficiencies that restrict their applicability in a widely-networked society. Biometric is used to identify the identity of an input sample when compared to a template, used in cases to identify specific people by certain characteristics. So, the advantage claimed by biometric authentication is that they can establish an unbreakable one-to-one correspondence between an individual and a piece of data [2].

Biometric authentication is any process that validates the identity of a user who wishes to sign into a system by measuring some intrinsic characteristic of that user. In biometric-based authentication, a legitimate user does not need to remember or carry anything and it is known to be more reliable than traditional authentication schemes. Biometric authentication offers a convenient, accurate, irreplaceable and high secure alternative for an individual, which makes it has advantages over traditional cryptography-based authentication schemes. There are basically two kinds of biometric systems: Automated identification systems operated by professionals (e.g., police Automated Fingerprint Identification Systems (AFIS)). The purpose of such systems is to identify an individual in question or to find an offender of a crime according to trails left at the crime scene. Biometric authentication systems used for access control. These systems are used by ordinary users to gain a privilege or an access right. Securing such a system is a much more complicated task [3].

Access control to a computer is generally implemented as a one-time proof of identity during the initial log on procedure. The validity of the user is assumed to be the same during the full session. Unfortunately, when a computer is left unattended, any person can have access to the same sources as the genuine user. This type of access control is referred to as static authentication. On the other hand, it have continuous authentication (also called active authentication), where the genuineness of a user is continuously verified based on the activity of the current user operating on the machine. When doubt arises about the genuineness of the user, the system can lock, and the user has to revert to the static authentication access control mechanism to continue working. A continuous authentication system should, with very high probability, never lock out the genuine user. On the other hand, it should detect an impostor user within a short period of time, to limit the potential damage that can be done by this impostor user to information available on the computer and to limit the disclosure of restricted information [4].

Biometric authentication is useful for continuous authentication and several investigations on this topic have

been published. For a continuous user authentication to be user friendly, passive authentication (e.g., face recognition) is desirable because the system should not require users' active cooperation to authenticate users continuously. In addition, a single biometric trait (unimodal technique) is not sufficient to authenticate a user continuously because the system sometimes cannot observe the biometric information. In this application, the use of multimodal biometrics cannot resolve the problem, though it mitigates the problem. For example, the system cannot observe any biometric traits whenever the user takes a break to read a book or consults notes. While these biometric traits contain strong discriminatory information about an individual, sometimes it is hard to observe them. On the other hand, there are soft biometric traits, like gender, skin color, and hair color, which do not have sufficient discriminatory information about the individual, but they are nevertheless useful for identifying individuals in some cases such as continuous authentication [5].

Swarm Intelligence (SI) concerns the collective, emerging behaviour of multiple, interacting agents who follow some simple rules. While each agent may be considered as unintelligent, the whole system of multiple agents may show some self-organization behaviour and thus can behave like some sort of collective intelligence. Many algorithms have been developed by drawing inspiration from SI systems in nature. All SI-based algorithms use multi-agents, inspired by the collective behaviour of social insects, like ants, termites, bees, and wasps, as well as from other animal societies like flocks of birds or fish. The classical Particle Swarm Optimization (PSO), Firefly Algorithm (FA), Cuckoo Search (CS) and Ant Colony Optimization (ACO) [6].

SI-based algorithms are among the most popular and widely used. There are many reasons for such popularity, one of the reasons is that SI-based algorithms usually sharing information among multiple agents, so that self-organization, co-evolution and learning during iterations may help to provide the high efficiency of most SI-based algorithms. Another reason is that multiple agent can be parallelized easily so that large-scale optimization becomes more practical from the implementation point of view. In this work, an effective continuous authentication system by combining the techniques in SI, face recognition, image or video processing, and pattern recognition is presented. It aims at automatically overcoming the disadvantage mentioned by the biometric features without interrupting the user from his work.

In the proposed continuous authentication system, hybrid BFO-SDS algorithm is employed to assist the face recognition module for raising the hard biometric recognition rate. The remainder of this work is organized as follows. The related work in literature are given in section 2. In section 3, the proposed system is described in detail. The experimental results are shown and discussed in section 4. Finally, conclusions are given in section 5.

2.RELATED WORKS

Frank et al., [7] investigated whether a classifier can continuously authenticate users based on the way they interact with the touchscreen of a smart phone. Then proposed a set of 30 behavioral touch features that can be extracted from raw touchscreen logs and demonstrated that different users populate distinct subspaces of this feature space.

Mosenia et al., [8] described the Continuous Authentication based on BioAura (CABA), a novel continuous authentication system that was inspired by and leverages the emergence of sensors for pervasive and continuous health monitoring.

Temper et al., [9] contributed to this research field by introducing an approach for continuous biometric authentication using touchscreen gestures and related posture information as unique features. In first experiments, this new authentication layer for Android-based phones, which was using a fuzzy classifier in combination with a scoring model, demonstrated its feasibility by achieving an Equal Error Rate (EER) of 11.5%.

Shen et al., [10] presented a multimodal biometrics authentication system that can continuously verify the presence of a logged-in user. Three passive biometric modalities are currently used - keystroke (i.e., behavioral biometric), face (i.e., physiological biometric), and skin color (i.e., soft biometric) - but the approach can also be readily extended to include more modalities.

Kumar & Kumar [11] proposed the ACO for the selection of key parameters like decision threshold and fusion rule, to ensure the optimal performance in meeting varying security requirements during the deployment of multimodal biometrics systems.

Tsai et al., [12] presented an initiative passive continuous authentication system based on both hard and soft biometrics. Human facial features are used as hard biometric information for the authentication process, and the clothes' color of a user is employed as the soft biometric information.

Papavasileiou et al., [13] presented a gait-based continuous authentication method using accelerometer and ground contact force data recorded from a pair of smart socks. Multi-modal learning and auto-encoders are used for feature extraction and a multi-task learning approach is used for classification. The effectiveness of the proposed approach has been demonstrated through preliminary experiments on a dataset of eight subjects.

Keerthana et al., [14] suggested the use of soft biometrics for user identification .Only an authorized user can login, user id and password is used in the computer application. As soon as the login process is completed soft biometrics start functioning. In soft biometrics a webcam was used that functions in the background.

3.METHODOLOGY

The face detection module in this system is implemented and work with Local Binary Pattern (LBP) features. The Adaboost and Eigen face method are used. For Eigen face method use hybrid bacterial swarming algorithm (i.e. BFO-SDS).

3.1 Local Binary Pattern (LBP)

LBP is computationally simple yet very efficient local texture operator. These features are invariant to monotonic gray scale changes [15]. LBP value of a sample 3 × 3 image is deliberated by,

$$LBP_{p,r} = \sum_{p=0}^{p-1} s(g_i - g_c)2^i, S(x) = \begin{cases} 1 & if\ x \geq 0 \\ 0 & otherwise \end{cases} \qquad (1)$$

Where g_c is the grey level value of central pixel ,g_p is the grey value of its neighbours around g_c and P is the number of neighbours. A pattern number is computed by comparing the g_c value with those of its neighbourhood. Conventional LBP requires 256 bins

to store all possible patterns. The concept of uniform patterns is introduced to reduce the number of possible bins. It effectively captures the fundamental information of textures.

3.2 AdaBoost Classifier

AdaBoost is the most well-known boosting procedure. It has been used in numerous empirical investigation and have received considerable attention from the machine learning community in the last years. Two interesting properties of AdaBoost. First, the training error exponentially goes down to zero as the number of classifiers grows. Second, AdaBoost still learns after the training error reaches zero. Regarding the last point, the AdaBoost not only classifies samples correctly, but also compute hypothesis with large margins. The margin of an

example is defined as its signed distance to the hyperplane times its label. A positive margin means that the example is well classified. This observation has motivated searching for boosting procedures which maximize the margin. It has been shown that maximizing the margin minimizes the generalization error [16].

3.3 Eigen Face

Face recognition is the technique of identifying a specific fixed face amidst an assortment of faces [17]. The input signals to such model are images. High degree of noise is prevalent in these input signals culminating as a result of variances in poses, lighting, appearance, gender, race, goggles, facial hair, cosmetics, changes due to age and health, face occlusions, etc. In spite of these impediments, there exist patterns which serve the purpose of face recognition. The patterns of interest in the face recognition domain are the nose, eyes, mouth, skin color, etc. These are better known as principal components or Eigen faces. Principal Component Analysis (PCA) is often used to excavate the above mentioned patterns [18]. PCA transforms a given image into a set of Eigen faces (also called Karhunen-Loeve transform).

Eigen faces are the characteristic features of an image. Also, the original image can be reconstructed from these Eigen faces. Each Eigen face represents only a specific characteristic of the face. The feature may or may not be present in the original image. Reconstructing the original image using Eigen faces requires the building of weighted sum of all Eigen faces. The degree to which the specific feature is inherent in the original image is determined by the weight. PCA is generally used to classify faces based on the distance between feature vectors. Euclidean distance, distance criterion and nearest mean classification are the standard classifiers used in this regard. An enhanced version of Eigen face approach was applied by maximizing the inter subject variation and minimizing the intra subject variation [19].

In linear algebra, the eigenvectors of a linear operator are non-zero vectors which, when operated by the operator, result in a scalar multiple of them. Scalar is then called Eigen value (λ) associated with the eigenvector (X). Eigen vector is a vector that is scaled by linear transformation. It is a property of matrix [20]. When a matrix acts on it, only the vector magnitude is changed not the direction.

$AX = \lambda X$, where A is a vector function.

$(A - \lambda I)X = 0$, where I is the identity matrix.

This is a homogeneous system of equations and form fundamental linear algebra. It know a non-trivial solution exists if and only if-

$\text{Det}(A - \lambda I) = 0$, where det denotes determinant.

When evaluated becomes a polynomial of degree n. This is called characteristic polynomial of A. If A is N by N then there are n solutions or n roots of the characteristic polynomial. Thus there are n Eigen values of A satisfying the equation (2).

$AX_{ii} \lambda_i X_i$, *where* i 1, 2,3,..., n (2)

If the Eigen values are all distinct, there are n associated linearly independent eigenvectors, whose directions are unique, which span an n dimensional Euclidean space.

The Eigen vectors of the covariance matrix AA^T are AX^i which is denoted by U^i. U^i resembles facial images which look ghostly and are called Eigen faces. Eigen vectors correspond to each Eigen face in the face space and discard the faces for which Eigen values are zero thus reducing the Eigen face space to an extent. The Eigen faces are ranked according to their usefulness in characterizing the variation among the images.

A face image can be projected into this face space by (3):

$$\Omega_k = U^T(\Gamma_k - \psi);\ k = 1,\ldots,M\ , \qquad (3)$$

Where (Ω_k) is the mean centered image. Hence projection of each image can be obtained as Ω_1 for projection of image1 and Ω_2 for projection of image2 and hence forth.

3.4 Bacteria Foraging Optimization (BFO) Algorithm

The BFO is a novel optimization algorithm based on the social foraging behavior of E. coli bacteria. The motile bacteria such as E. coli and salmonella propel themselves by rotating their flagella. To move forward, the flagella counter clockwise rotate and the organism "swims" (or "runs").While a clockwise rotation of the flagellum causes the bacterium randomly "tumble" itself in a new direction and then swims again [21].

The original BFO system consists of three principal mechanisms, namely, chemo taxis, reproduction, and elimination-dispersal:

Chemo taxis: Suppose $\boldsymbol{\theta}^i$ (j , k , l) represents the bacterium at jth chemo tactic, kth reproductive, and lth elimination-dispersal step. C (i) is the chemo tactic step size during each run or tumble (i.e., run-length unit). Then in each computational chemo tactic step, the movement of the ith bacterium can be represented as (5):

$$\theta^i(j+1,k,l) = \theta^i(j,k,l) + C(i)\frac{\Delta i}{\sqrt{\Delta^T(i)\Delta i}} \qquad (5)$$

Where Δ(i) is the direction vector of the jth chemo tactic step. When the bacterial movement is run, Δ (i) is the same with the last chemo tactic step; otherwise, (i) is a random vector whose elements lie in [−1, 1]. With the activity of run or tumble taken at each step of the chemo taxis process, a step fitness, denoted as J (i, j, k, l), will

be evaluated.

Reproduction: The health status of each bacterium is calculated as the sum of the step fitness during its life in (6), that is,

$$\sum_{j=1}^{Nc} J(i,j,k,l) \qquad (6)$$

Where Nc is the maximum step in a chemo taxis process. All bacteria are sorted in reverse order according to health status. In the reproduction step, only the first half of population survives and a surviving bacterium splits into two identical ones, which are then placed in the same locations. Thus, the population of bacteria keeps constant [22].

Elimination and Dispersal: The chemo taxis provides a basis for local search, and the reproduction process speeds up the convergence which has been simulated by the classical BFO. While to a large extent, only chemo taxis and reproduction are not enough for global optima searching. Since bacteria may get stuck around the initial positions or local optima, it is possible for the diversity of BFO to change position to eliminate the accidents of being trapped into the local optima. Then some bacteria are chosen, according to a preset probability Ped, to be killed and moved to another position within the environment.

3.5 Stochastic Diffusion Search (SDS)

SDS is based on distributed computation, in which the operations of simple computational units, or agents, are inherently probabilistic. Agents collectively construct the solution by performing independent searches, followed by the diffusion of information through the population. Positive feedback promotes better solutions by allocating to them more agents for their exploration. Limited resources induce strong competition from which the largest population of agents corresponding to the best-fit solution rapidly emerges [23].

SDS searches for and finds the best match of a given model in a given search space; for example, a particular word (the model) in a text document (the search space). During the searching process, each agent operates entirely independently of the other agents, only reconvening to exchange information about what they have found. There is no concept in SDS of the time taken for an agent to travel to its hypothesis position, only spatial concerns (the size of the search space); there is, however, the cost of evaluating the hypothesis once selected: the cost of the test function. During SDS, each agent is able to access the entirety of the search space and also to carry with it information about the entirety of its target model.

The standard SDS algorithm is shown as follows:

Initialisation phase All agents generate an initial hypothesis while Halting criteria not satisfied do

Test phase All agents perform hypothesis evaluation Diffusion phase All agents deploy a communication strategy Re *late phase Optional* ; *active agents with*

the same hypothesis randomly deactivate Halt phase Evaluation of halting criteria
end while

Initialization Phase: During the initialization phase, all agents randomly select a hypothesis from the search space. All agents are set to inactive. All agents are given access to
the target model. The random initialization of hypothesis positions can be biased in favour of some positions, given what can be described as a-priori knowledge [24].

Test Phase: During the test phase, the agent determines whether it should set itself to be active or inactive. This is achieved by applying a test function to its current hypothesis. This test function is a partial evaluation of the hypothesis position. The test function will differ depending on the application domain. Agents are set to active if this partial evaluation of the hypothesis returns success; otherwise, they remain inactive.

Diffusion Phase: During the diffusion phase, agents exchange hypothesis information. The idea is for active agents to disseminate their current hypothesis to inactive agents. There are three differing strategies for this dissemination, termed recruitment strategies: passive recruitment, active recruitment and a combination of the two. This exchanging of information leads to agents with good hypotheses recruiting inactive agents to their position. Eventually, large numbers of agents congregate around the best hypothesis (or hypotheses if the related phase is used) available in the search space. The standard SDS recruitment strategy deployed is passive.

Relate Phase: The relate phase is an optional phase, introduced if multiple models are extant in the search space. The technique allows a degree of dynamic re-allocation of agents and the maintenance of multiple clusters of active agents around multiple good hypotheses. The relate phase can also assist with dynamic search spaces, allowing clusters of agents to re-align themselves successfully with the correct hypothesis. The relate phase has two modes: context free and context sensitive [25].

Halting Phase: After each test and diffuse iteration (and optionally, relate phase), the SDS process determines whether the agent population has reached a state that determines the completion of the search: the halting criteria. Ideally, the search will stop as soon as the best hypothesis (or hypotheses) in the search space is found. This can be difficult to ascertain, particularly with noisy data.

Weak Halting Criteria: Weak halting criteria states that SDS should stop when a certain percentage of all agents are active, regardless of their hypothesis. Once above this threshold, the population should then stabilize at a certain level. This stabilization can be seen as the population of active agents remaining steady, with a margin of tolerance, for a certain number of iterations. Once these criteria have been met, the search stops.

Strong Halting Criteria: This defines the halt state as being concerned with the percentage of active agents in the largest cluster; i.e., looking at the hypothesis that has the most agents clustered around it and applying the same threshold/tolerance rule as with the weak halting state, but looking instead at the percentage of agents that are active within this largest cluster.

3.6 Proposed Hybrid BFO-SDS Algorithm

Both the BFO algorithm and SDS have their own advantages and they both work well for a wide range of optimization problems. In this work, it propose a new hybrid algorithm

based on BFO algorithm and SDS by combining some of the advantages of both algorithms. It call the proposed approach the hybrid BFO-SDS algorithm that combines the attraction mechanism of BFO algorithm with the mixing ability of SDS so as to increase the speed of convergence and the diversity of the population. The major difference between BFO algorithm and SDS is how new individuals are generated and then used at each iteration [26].

Among the many components of algorithms, intensification and diversification (also called exploitation and exploration) are the two major components of any meta-heuristic algorithm. In order to explore the search space on a global scale, meta-heuristic algorithms need to generate a diverse range of solutions using diversification or exploration strategy. Intensification or exploitation strategy can guide the individual to search in a local region, based on the prior knowledge or the new information found during the search process that a current good solution is found in this region. An algorithm's solution accuracy and convergence rate can be enhanced by balancing intensification and diversification properly.

The global convergence of BFO algorithm can also be considered as a disadvantage. If the gradient information is available, the BFO algorithm may not exploit it properly. Other disadvantages of BFO algorithm can be in its chemotaxis and its elimination and dispersal events. The step length or the swim length in chemotaxis does not vary with the convergence to the optimal solution during the optimization process which increases the computational time and reduce precision. The elimination and dispersal event makes a bacterium which has found or nearly found an optimal position escape. So, a hybrid SI technique called BFO-SDS technique was presented is to modify those disadvantages by performing a variable or an adaptive swim size,

and limiting the range of the elimination and dispersal of bacteria, and hence, improving the computational time and precision [27].

This work justifying the merging SDS and BFO is the partial function evaluation deployed in SDS, which may mitigate the high computational overheads entailed when deploying a BFO algorithm onto a problem with a costly fitness function. In BFO, during chemotaxis, the bacterium which is close to a noxious substance takes a larger chemotactic step to move towards nutrient substances. Before each move, it is ensured that the bacterium moves in the direction of increasing nutrient substance concentration; i.e. a region with smaller objective function value [28]. After this, each SDS agent, on the other hand, has hypothesis and status. Every BFO bacterium is an SDS agent too together termed psAgents. In the psAgent, SDS hypotheses are defined by the BFO positions and a status which determines whether the psAgent is active or inactive. The produced vector probabilistically interchanges its components with the original vector. Offspring vector replaces the original one if the objective function value is smaller for it. The process is repeated several times over the entire population in order to obtain the optimal solution.

In the test-phase of a SDS [29], each agent has to partially evaluate its hypothesis. The fitness of each psAgents bacterium personal best is compared against that of a random psAgent; if the selecting psAgent has a better fitness value, it will become active, and otherwise it is flagged inactive. On average, this mechanism will ensure 50% of psAgents remain active from one iteration to another. In the Diffusion Phase, each inactive psAgent picks another psAgent

randomly, if the selected psAgent is active, the selected psAgent communicates its hypothesis to the inactive one; if the selected psAgent is inactive too, the selecting psAgent generates a new hypothesis at random from the search space. In the proposed technique, after each n number of BFO function evaluations, one full SDS cycle is executed.

The flowchart for hybrid BFO-SDS algorithm as shown in figure 1.

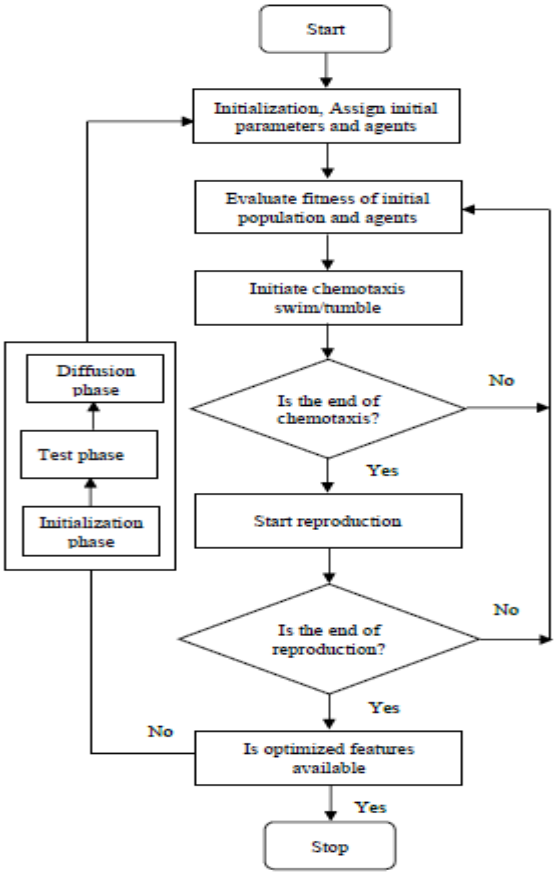

Figure 1 Flowchart for Hybrid BFO-SDS Algorithm

4.RESULTS AND DISCUSSION

Experiments conducted using ORL database and the input from the webcam. The first experiment utilizes ORL database to test the accuracy of the proposed BFO-SDS supported Eigen face method. The result is compared with the conventional Eigen face method with regular PCA decomposition. ORL database contains dissimilar facial expression, frontal and slanted facial images, varied lighting condition, and different facial accessories. These four factors are mostly present in the real-world environment. Moreover, ORL database contains 40 subjects and 10 facial images per subject. This database size is the closest to fit the condition of which the continuous authentication system is going to work in. Hence, the ORL database is chosen to be the data source in the first experiment. In this experiment, six images per user are used to be the training image, and the rest four images are employed to be the test images. Therefore, there are total 240 training images and 160 test images, respectively. The images are cropped within the face region and resized to the size of 48 × 48. The results showed in figures 2 & 3.

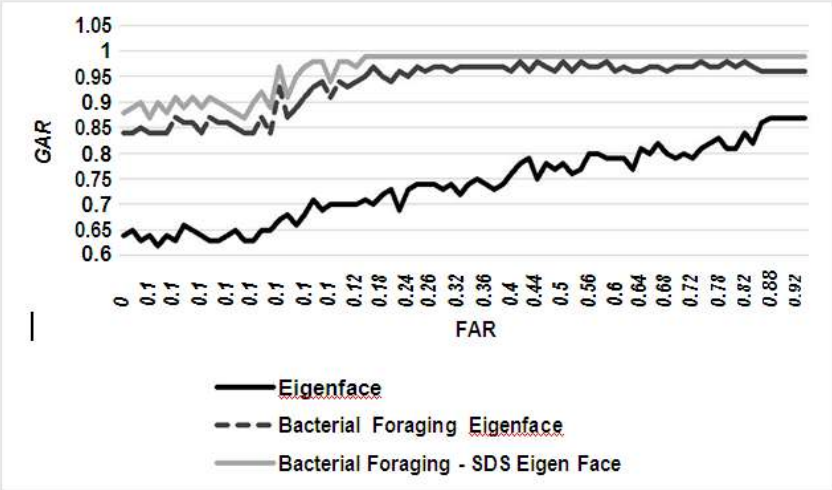

Figure 2 False Acceptance Rate

From the figure 2, it can be observed that the bacterial foraging - SDS Eigen face has higher average FAR by 26.66% for Eigen face and by 3.19% for bacterial foraging - Eigen face.

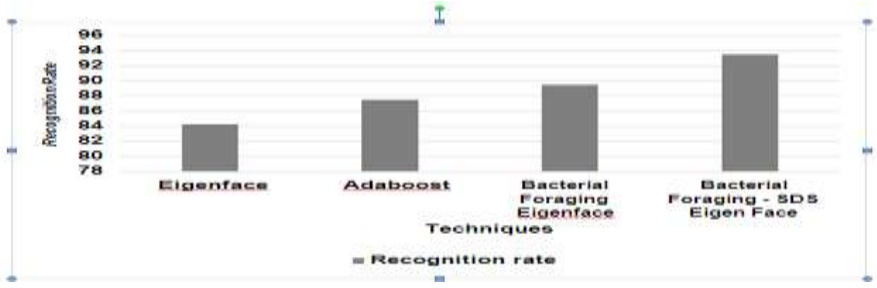

Figure 3 Recognition Rate

From the figure 3, it can be observed that the bacterial foraging - SDS Eigen face has higher recognition rate by 10.4% for Eigen face, by 6.62% for AdaBoost and by 4.37% for bacterial foraging Eigen face.

5.CONCLUSION

The continuous authentication system that is widely used for continuously monitoring a user's identity on a mobile device is based on face recognition. In this work, proposed LBP, Adaboost, Eigen face and a hybrid SI technique called BFO-SDS to solve integer multi-objective problems etc. The proposed technique effectively overcomes the drawbacks of BFO technique, such as the partial optimism, which causes the less exact at the

regulation of its speed and the direction. It also, overcomes the drawbacks of SDS technique. BFO-SDS technique also, increases the efficiency of the solution process, improves the performance scalability, and increases the diversification of solutions at the same time, reducing the execution time. Results show the bacterial foraging - SDS Eigen face has higher average FAR by 26.66% for Eigen face and by 3.19% for bacterial foraging - Eigen face. The bacterial foraging - SDS Eigen face has higher recognition rate by 10.4% for Eigen face, by 6.62% for AdaBoost and by 4.37% for bacterial foraging Eigen face.

REFERENCES

1. Chirchi, V. R. E., Waghmare, D. L., & Chirchi, E. R. (2011). Iris biometric recognition for person identification in security systems. International Journal of Computer Applications, 24(9), 1-6.

2. Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. International Journal of u-and e-Service, Science and Technology, 2(3), 13-28.

3. Narhe, S. I. T. S. Review on Biometric Authentication Methods. International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 11, November 2015. pp: 252-255.

4. Mondal, S., & Bours, P. (2015). A computational approach to the continuous authentication biometric system. Information Sciences, 304, 28-53.

5. Niinuma, K., & Jain, A. K. (2010, April). Continuous user authentication using temporal information. In Proc. SPIE (Vol. 7667, No. 1, p. 76670L).

6. Frank, M., Biedert, R., Ma, E., Martinovic, I., & Song, D. (2013). Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE transactions on information forensics and security, 8(1), 136-148.

7. Mosenia, A., Sur-Kolay, S., Raghunathan, A., & Jha, N. K. (2017). CABA: Continuous authentication based on BioAura. IEEE Transactions on Computers, 66(5), 759-772.

8. Fister Jr, I., Yang, X. S., Fister, I., Brest, J., & Fister, D. (2013). A brief review of nature-inspired algorithms for optimization. arXiv preprint arXiv:1307.4186.

9. Temper, M., Tjoa, S., & Kaiser, M. (2015, July). Touch to Authenticate—Continuous Biometric Authentication on Mobile Devices. In Software Security and Assurance (ICSSA), International Conference on (pp. 30-35). IEEE.

10. Shen, C., Zhang, H., Yang, Z., & Guan, X. (2016, October). Modeling multimodal biometric modalities for continuous user authentication. In Systems, Man, and Cybernetics (SMC), 2016 IEEE International Conference on (pp. 001894-001899). IEEE.

11. Kumar, A., & Kumar, A. (2016). Adaptive management of multimodal biometrics fusion using ant colony optimization. Information Fusion, 32, 49-63.

12. Tsai, P. W., Khan, M. K., Pan, J. S., & Liao, B. Y. (2014). Interactive artificial bee colony supported passive continuous authentication system. IEEE Systems Journal, 8(2), 395-405.

13. Papavasileiou, I., Smith, S., Bi, J., & Han, S. (2017, July). Gait-Based Continuous Authentication Using Multimodal Learning. In Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2017 IEEE/ACM International Conference on (pp. 290-291). IEEE.

14. Keerthana, G., Mahalakshmi, P., Nandhini, M., & Rao, B. D. (2016). Soft Biometrics Based on Continuous Authentication for Standalone Workstation. Biometrics and Bioinformatics, 8(6), 139-142.

15. Arun, D. R., Columbus, C. C., & Meena, K. (2016). Local Binary Patterns and Its Variants for Finger Knuckle Print Recognition in Multi-Resolution Domain. Circuits and Systems, 7(10), 3142.

16. Marcel, S., & Rodriguez, Y. (2004). Biometric face authentication using pixel-based weak classifiers. Lecture notes in computer science, 24-31.

17. Zhang, X., & Gao, Y. (2009). Face recognition across pose: A review. Pattern Recognition, 42(11), 2876-2896.

18. Perlibakas, V. (2004). Distance measures for PCA-based face recognition. Pattern Recognition Letters, 25(6), 711-724.

19. Wang, J., Plataniotis, K. N., & Venetsanopoulos, A. N. (2005). Selecting discriminant eigenfaces for face recognition. Pattern Recognition Letters, 26(10), 1470-1482.

20. Singh, A., & Kumar, S. (2012). Face recognition using pca and eigen face approach (Doctoral dissertation).

21. Jakhar, R., Kaur, N., & Singh, R. (2011). Face recognition using bacteria foraging optimization-based selected features. International Journal of Advanced Computer Science and Applications, 1(3).

22. Yadav, D., Vatsa, M., Singh, R., & Tistarelli, M. (2013). Bacteria foraging fusion for face recognition across age progression. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 173-179).

23. al-Rifaie, M. M., Bishop, J. M., & Blackwell, T. (2012). Information sharing impact of stochastic diffusion search on differential evolution algorithm. Memetic Computing, 4(4), 327-338.

24. Williams, H., & Bishop, M. (2014). Stochastic diffusion search: a comparison of swarm intelligence parameter estimation algorithms with ransac. Algorithms, 7(2), 206-228.

25. al-Rifaie, M. M., & Bishop, J. M. (2013). Stochastic diffusion search review. Paladyn, Journal of Behavioral Robotics, 4(3), 155-173.

26. Zhang, L., Liu, L., Yang, X. S., & Dai, Y. (2016). A novel hybrid firefly algorithm for global optimization. PloS one, 11(9), e0163230.

27. Kora, P., & Kalva, S. R. (2015). Hybrid bacterial foraging and particle swarm optimization for detecting Bundle Branch Block. SpringerPlus, 4(1), 481.

28. Elaydi, H. A., & AlSbakhi, M. A. (2017). Hybrid FLC/BFO Controller for Output Voltage Regulation of Zeta Converter. Journal of Engineering Research and Technology, 4(2).

29. El-henawy, I. M., & Ismail, M. M. (2014). A Hybrid Swarm Intelligence Technique for Solving Integer Multi-objective Problems. International Journal of Computer Applications, 87(3).