ORIGINAL RESEARCH ARTICLE UHD JOURNAL OF SCIENCE AND TECHNOLOGY

Fingerprint Authentication using Shark Smell Optimization Algorithm

Bakhan Tofiq Ahmed[1], Omar Younis Abdulhameed[2]

[1]Department of Information Technology, Technical College of Informatics, Sulaimani Polytechnic University, Sulaimani, Kurdistan Region, Iraq, [2]Department of Computer Science, College of Science, University of Garmian, Kalar, Garmian, Kurdistan Region, Iraq

ABSTRACT

Recognition of people relying on biometric characteristics is a common phenomenon in our society. It has increased in recent years in most areas of life such as government, department, companies, and banks. Fingerprint identification is one of the most common and credible personal biometric identification methods. Extracting features are one of the most important steps in the fingerprint identification; the strength of any system depends mainly on this step, where whenever the features obtained are accurate whenever the identification process is more accurate. Therefore, an effective and efficient method must be used to extract the features. This paper solved two main problems that were (1) improving security by designing and implementing an accurate, efficient, and fast authentication system for the identification and verification process using an intelligent algorithm to extract the best features from the fingerprint image and (2) evaluating the strength of the Shark Smell Optimization (SSO) in the search space with a chosen set of metrics. This paper aims to extract the best features of the fingerprint image using an algorithm that depends on nature for its movement and work; therefore, the SSO was used. In this paper, the SSO algorithm is used to extract the features. SSO is a new meta-heuristic algorithm that uses smart methods and random movements to get its prey. These methods and movements were used to extract features from the fingerprint image which will be used later for identification and verification process. The proposed method is implemented through four phases, namely, create a database to store and organize data, image pre-processing using median filter, feature extraction using SSO algorithm, and matching process using euclidean distance. The results demonstrated the strength, accurate, credible, and effectiveness of the algorithm used by applying it on (150) real fingerprint samples taken from university students, where the results of false acceptation rate, false rejection rate, and correct verification rate were 0.00, 0.00666, and 99.334%, respectively.

Index Terms: Fingerprint Authentication, Feature Extraction, Swarm Intelligent, Shark Smell Optimization, ZKT eco device

1. INTRODUCTION

The rapid enhancement of technology and electronically life raised the need for an extra level of security. Security is an increasing necessity throughout the globe because a lack of security can result in great damage. Security is well-defined as the degree of resistance to, or defense from harm. Physical security, personal security, and information security are the main forms of security. In the security field, authentication term means to verify an individual to access system based on their identity [1].

Many decades ago user's identity had been verified through a traditional method called knowledge-based authentication (e.g., password, smart-card, or personal identity number)

Access this article online

DOI: 10.21928/uhdjst.v4n2y2020.pp28-39

E-ISSN: 2521-4217
P-ISSN: 2521-4209

Corresponding author's e-mail: Bakhan Tofiq Ahmed, Department of Information Technology, Technical College of Informatics, Sulaimani Polytechnic University, Sulaimani, Kurdistan Region, Iraq. E-mail: Bakhan.tofiq.a@spu.edu.iq

Received: 05-06-2020 Accepted: 16-07-2020 Published: 20-07-2020

which might be easily forgotten or stolen. However, a fast upgrading in technology has replaced the traditional method to a new one called biometric-based authentication because is more convenient in which there is no need to memorize secret codes like password, and more secure which is harder to be stolen because it based on the unique human biometric features unlike knowledge-based authentication [2].

Biometric derived from the two Greek words the first one is Bios which means "life" and the second is Metric which means "measure." A biometric is a recognizing pattern system that identifies an individual relied on a feature extracted from an exact physiological or behavioral representative that the individual owns, for instance, Face, Hands, Eyes, Ears, or Voice to distinguish each other. This technology provides more reliability than the traditional approaches because of body characteristics cannot be easily stolen, copied, or forging by an intruder [3].

Fingerprint authentication is the most widely and commonly used biometric authentication mechanism because of its distinctiveness, ease of use, and long-term stability. The fingerprint is a gifted feature for biometric identification and verification. A fingerprint is the pattern of ridges and valleys on the fingertip surface. In fact, each individual has distinct fingerprints and leftovers almost the same entire life. The fingerprint is the most prominent and widely utilized human's trait for implementing a personal authentication system due to its uniqueness [4], [5].

2. LITERATURE REVIEW

In this section, some of the up-to-date researches in this field are reviewed which is from 2014 to 2019. These reviewed works are enlisted below:

Mela *et al.* [6], this research proposed an efficient fingerprint authentication model using the Haar Wavelet Transform (HWT) and Local Ridge Attribute. In this investigation, Gabor Filter is used to eliminating noise from the fingerprint image. Then, local ridge features are extracted from the enhanced image by 1-level HWT and 2-Level HWT. Afterward, the invariant moment is used to select only the critical features (i.e., 19 features) from 98 extracted features. Finally, the matching phase has been done by absolute difference. The experiments are done using Fingerprint Verification Competition (FVC 2004) DB1 and DB2 datasets. Each database contains 80 low-quality fingerprint images. The experimental results indicated that the proposed model was able to signify low-quality fingerprint images and gave a high recognition accuracy of 94.37% when 1-level HWT is used, while recognition accuracy of 96.87% is achieved when 2-level HWT is used using two decomposition levels of wavelet.

Abidin *et al.* [7], in this study, Gabor Wavelet Transform (GWT) and K-Nearest Neighbor (K-NN) are used to constructing a fingerprint authentication model. The main aim of using GWT was to extract local features from the gray-scale fingerprint image. Then, K-NN classifier is utilized for the recognition task. The Hong Kong Polytechnic University High Resolution Fingerprint (PolyU HRF) database has been used to test the proposed model. The outcome of this research has shown that the constructed model was credible because it gained the accuracy of 94.5%.

Umma *et al.* [8], this paper developed a fingerprint authentication system by utilizing the speeded-up robust feature (SURF) algorithm and Nearest Neighbor Matching Approach (NNMA). In this investigation, SURF algorithm is used to extract local features from the fingerprint image. Later, NNMA is used to compare the features of the test fingerprint image against two or more exiting template image features in the database. For simulating the model, 128 fingerprint images are collected from the web. The recognition accuracy of the system was 88.3%.

Mouad *et al.* [9], in this study, a fingerprint authentication proposed using Minutiae Extractor Algorithm (MEA) to perform the identification and verification process. The work is done in a sequence that began from the pre-processing stage that comprised of (enhancement, binarization, and thinning). First, image enhancement is done using the Fast Fourier Transform to eliminate undesirable data to increase the clarity of the fingerprint image. Second, the MEA is utilized to extract the fingerprint features. Finally, the Minutiae Matching Algorithm with Euclidean Distance (ED) is performed in the matching stage. The model is tested on two various public fingerprint databases which are FVC2000 and FVC2002. The experimental result obtained from the FVC2000 database was 0.2049 false acceptation rate (FAR), 0.1944 false rejection rate (FRR), and 60.07% correct verification rate (CVR), while 0.0154 FAR, 0.0137 FRR, and 97.09% CVR from FVC2002.

Hong *et al.* [10], in this paper, a Convolutional Neural Network (CNN) is used to propose fingerprint recognition. CNN is a renowned feature learning and classification algorithm which is utilized to detect relevant feature on fingerprint images. An Affine Fourier Moment Matching is suggested in this

research as a method of matching. The algorithm evaluation is done using a public database, namely, Hong Kong PolyU HRF which consisted of 30 images. The constructed model has achieved a satisfactory accuracy of 88.6%.

Zainab *et al.* [11], this study proposed a fingerprint authentication that used local energy distribution with three different levels of HWT, namely, 1-D, 2-D, and 3-D (Dimension) HWT. The proposed system included the primary stages such as pre-processing, feature extraction, and matching features. Pre-processing consisted of Color Conversion, Segmentation, Binarization Thresholding. Before extracting significant feature, the image is decomposed into four sub-bands using 1-D, 2-D, and 3-D (HWT) separately. After that feature vector is extracted by computing Energy Local Distribution. Finally, feature matching is carried out by utilizing the Mean Square Difference and Mean Absolute Difference. The FVC2004 databases used to test the proposed system. FVC 2004 databases consist of four various datasets; each dataset has 80 fingerprint image samples. The proposed system achieved good accuracy which was 94%, 91%, and 94% when 1-D, 2-D, and 3-D HWT are used, respectively.

Israa *et al.* [12], in this investigation, the design of a fingerprint authentication system is suggested that relied on Filter Bank Based (FBB) algorithm. Fingerprint images were enhanced using the Fourier Domain Analysis Filtering and Segmentation as a Pre-processing stage. FBB algorithm is used in the feature extraction stage. Using K-NN technique and 70% threshold value, the matching stage has been done. K-NN classifier and 70% threshold value provide an appropriate matching result. A collection of 90 fingerprint images are used to evaluate the proposed model. The CVR, FAR, and FRR achieved from this work were 93.9683%, 0.012698, and 0.047619, respectively.

Aung *et al.* [13], a Neural Network (NN) Classifier is used to propose a fingerprint authentication system in this research. First, the input fingerprint image is acquired by the Digital Persona 4500 fingerprint scanner. Second, the images are enhanced using Contrast Stretching and 2 Morphological techniques such as Dilation and Erosion. Third, Minutiae Based Approach used to extract features from the region of interest of a fingerprint image. Afterward, features were fed into the NN for user recognition. According to the experimental consequences, the proposed fingerprint recognition system reached 96.5% accuracy.

Harinder *et al.* [14], in this paper, an enhancement fingerprint authentication is proposed which is based on Non-Subsampled Contourlet Transform (N-SCT) and Zernike Moments (ZMs). Four various stages were conducted in this work. First, the fingerprint image decomposition stage is done through NSCT to decompose the fingerprint images into NSCT sub-samples. Second, the fingerprint image features were evaluated through ZMs. Third; potential features were selected using the determination coefficient. Finally, a Weighted Support Vector Machine is used to train and test the selected features for the matching stage. Extensive experimental results depicted that the proposed system gave significant improvement in terms of accuracy which was nearly 95%.

Nature-inspired optimization algorithms, especially swarm-based algorithms, solve many scientific and engineering problems due to their flexibility and simplicity. These algorithms are applicable for optimization problems without structural modifications. This work presents a novel nature-inspired metaheuristic optimization algorithm called SSO to extract the best features from the user's fingerprint image. The results proved that the swarm intelligence (SI) algorithm gave better results than other algorithms.

3. SI

SI stands for Swarm-Intelligence is an artificial intelligent (AI) method relied on group behavior that originated in nature. The SI term was utilized by Beni in Cellular-Robotic-System for the 1st time where modest agents arranged themselves through neighborhood collaborations. SI is enumerated as the most critical optimization scheme. SI is the characteristic of a system when the cooperative agent behaviors locally cooperate with their environment such as Ant-Colony's searching, Bird's flocking, Bacteria's evolving, and Fishes schooling. SI compromises of several algorithms such as Ant-Colony Optimization, Particle-Swarm Optimization (PSO), Artificial-Bee-Colony (ABC), Bacterial-Foraging Optimization, Fire-Fly Algorithm (FA), and Artificial-Fish-Swarm Optimization, and Shark Smell Optimization (SSO) [15]. Some of the critical SI algorithms are shown in Fig. 1.

3.1. SSO Algorithm

SSO is counted as the modern SI algorithm which was founded in 2014 by Oveis Abedinia, Nima Amjady, and Ali Ghasemi, which can be considered one of the best optimization tools. The development of this algorithm has relied on the ability of the shark because it has superiority in catching prey using a strong smell sense in a short time. In fact, the shark is one of the most renowned and superior hunters in nature. The reason for this superiority is the shark's ability to find the prey in a short time based on its

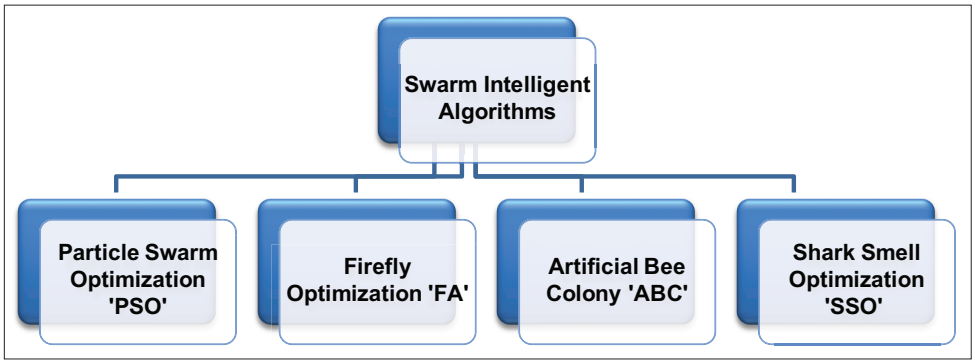

Fig. 1. Some algorithms of swarm intelligence [15].

strong smell sense in a large search space [16]. When prey is injured and blood is injected into the water, shark smells the odor of blood, and move toward the prey. The movement of shark toward prey is based mainly on the concentration and gradient of blood odor in the water particles.

The key factor that guides the shark toward its prey is concentration. Moreover, if the concentration is strong, the shark's movement will be increased [17], [18]. The pseudo code of the SSO Algorithm is described in the algorithm (1) below.

Algorithm (1): SSO description [16]

Begin

Step 1. Initialization

Set parameters NP, k_{max}, η_k, α_k, and (k=1, 2,…, k_{max})

Generate initial population with all individuals

Generate each decision randomly within the allowable range

Initialize the stage counter k = 1

For k= 1: k_{max}

Step 2. Forward Movement

Calculate each component of the velocity vector, $V_{i,j}$ (i=1,… NP, j=1,.. ND)

Obtain new position of shark based on forward movement, Y_i^{k+1} (i=1,…,NP)

Step 3. Rotational movement

Obtain the position of shark based on rotational movement, $Z_i^{k+1,m}$ (m = 1,…, M)

Select the next position of shark based on the two movements, X_i^{k+1} (i=1,…, NP)

End for k

Set k = k+1

Select the best position of shark in the last stage which has the highest OF value

End

3.2. The Steps of SSO Algorithm

SSO algorithm consists of four basic steps such as (initialization, forward movement, rotational movement, and position update), which can be listed as follows:

3.2.1. Initialization of SSO

To model the SSO algorithm, the population of the initial solution must be generated randomly within the search space.

Each of these solutions represents a particle of odor which shows a possible position of the shark at the beginning of the search process. The initial solution vector is shown in (1) and (2), respectively:

$$X^1 = \left[X_1^1, X_2^1, \ldots\ldots, X_{NP}^1 \right] \quad (1)$$

Where X_i^1 = ith initial position of the population vector and NP = population size. The related optimization problem can be expressed as:

$$X_i^1 = \left[X_{i,1}^1, X_{i,2}^1, X_{i,3}^1, .., X_{i,ND}^1 \right] \quad (2)$$

Where $X_{i,j}^1$ = jth dimension of the shark's ith position and ND = number of decision variables [19].

3.2.2. Forward movement of the SSO toward the target

When the blood is released in the water, the Shark in each position moves toward stronger odor particles with a velocity "V," to become closer to the prey (target). As a result, corresponding to the initial position vector, the velocity vector can be expressed by (3).

$$V^1 = \left[V_1^1, V_2^1, V_3^1, \ldots., V_{NP}^1 \right] \quad (3)$$

Each velocity vector has a dimensional component element as given in (4):

$$Vi^1 = \left[V_{i,1}^1, V_{i,2}^1, V_{i,3}^1, \ldots. V_{i,ND}^1 \right] \quad (4)$$

Hence, the velocity in each dimension is calculated by (5):

$$V_{i,j}^k = \eta k.\mathrm{R1}.\left.\frac{\partial(OF)}{\partial xj}\right|_{x_{i,j}^k} \quad (5)$$

Whereby: k= 1, 2,…., k_{max}, $\left.\frac{\partial(OF)}{\partial xj}\right|_{x_{i,j}^k}$ is a derivative of the objective function (OF) at the position $x_{i,j}^k$.

k_{max} = maximum number of stages for forwarding movement of the shark, k = number of stages, = a value in the interval (0, 1), and R1 = a random number in the interval (0, 1) [20].

The increase in shark's velocity is determined by the increase in the odor intensity. In each stage of $V_{i,j}^k$, the velocity limiter is employed by modifying (5) as shown in (6):

$$\mathrm{V}_{\mathrm{i,j}}^{\mathrm{k}} = \eta_{\mathrm{k}}.\mathrm{R1}.\left.\frac{\partial(\mathrm{OF})}{\partial \mathrm{xj}}\right|_{\mathrm{x}_{\mathrm{i,j}}^{\mathrm{k}}} + \alpha_{\mathrm{k}}.\mathrm{R2}.\mathrm{V}_{\mathrm{i,j}}^{\mathrm{k-1}} \quad (6)$$

Where $\beta\kappa$ is a velocity limiter ratio for stage k, αk is the inertia coefficient in (0, 1), and R2 like R1 is a random number in the interval (0, 1).

Due to forward movement of the shark, its new position is Y_i^{k+1} determined based on its previous position (X_i^k) and velocity (V_i^k), the new position of the shark is depicted by (7):

$$Y_i^{k+1} = X_i^k + V_i^k.\Delta \mathrm{t_k} \quad (7)$$

Where Δtk = is a time interval which is assumed to be 1 for simplicity [21]. The forward movement of the shark toward the prey is represented in Fig. 2.

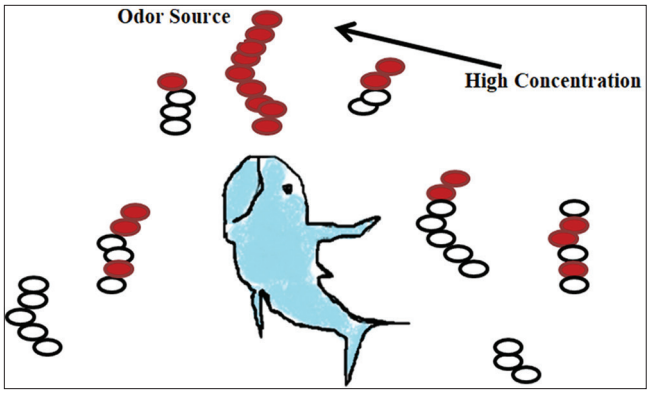

Fig. 2. Shark's forward movement [21].

3.2.3. Rotational movement of the SSO toward the target

The shark is also has a rotational movement which is used to find the stronger odor particles. This process is called the local search of the SSO algorithm modeled by (8).

$$Z_i^{k+1,m} = Y_i^{k+1} + \mathrm{R3}.Y_i^{k+1} \quad (8)$$

m = 1, 2,…, M, and R3 is a random number that can be considered in the interval (−1, 1). To model the rotational movement of the shark, the number of points M in the local search is connected to form closed contour lines, as shown in Fig. 3 [22].

3.2.4. Updating the particle position (Location)

The shark's search path will continue with the rotational movement as it moves closer to the point with a stronger

odor sense as revealed in Fig. 3. This specific feature in the SSO algorithm can be expressed as in (9).

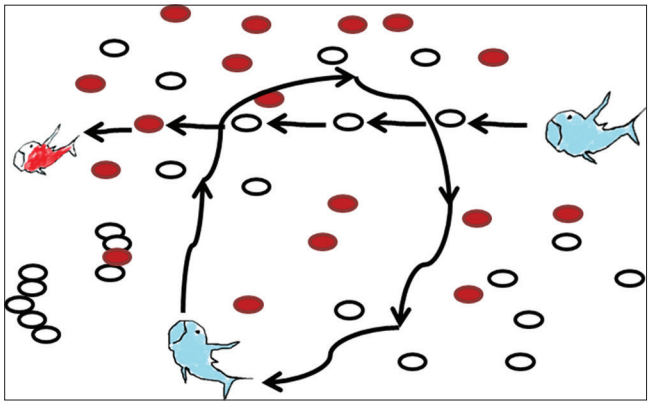

Fig. 3. Shark's rotational movement [23].

$$X_i^{k+1} = \arg\max\{OF(Y_i^{k+1}), OF\left(Z_i^{k+1,i}\right), .., OF(Z_i^{k+1,M})\} \quad (9)$$

Where: X_i^{k+1} represents the shark's next position with the highest value of the objective function (OF). The process will continue until k reaches the maximum value (best individual) in the given population in a search space chosen for an optimization problem [23].

4. THE PROPOSED METHOD

This section presents the critical stages of the proposed method, where the SSO algorithm is used to extract the best features from the user's fingerprint image.

All the stages of the proposed method have been implemented, designed, and written by java programming language because it is easy to write, compile, debug, and compatible with most of the platforms. For this, purpose Netbeans integrated development environment version 8.2 has been installed from oracle official website with Java Development Kit version 8u192. Microsoft Access 2010 is used to create a small database to store the user's features and biographic information. The graphs created by the proposed method. ZKTeco: ZK4500 fingerprint reader is used to acquire samples because it is an up-to-date and high-quality device. Furthermore, the proposed system was implemented using Windows 10 operating system 64-bit and computer with Intel® Core™ i7-7500U CPU running at a frequency of 2.90 GHz and (8) GB of RAM. The proposed method consists of four stages, namely, create a database to store and organize data, image pre-processing, feature extraction, and matching process. The detail of each stage has been illustrated

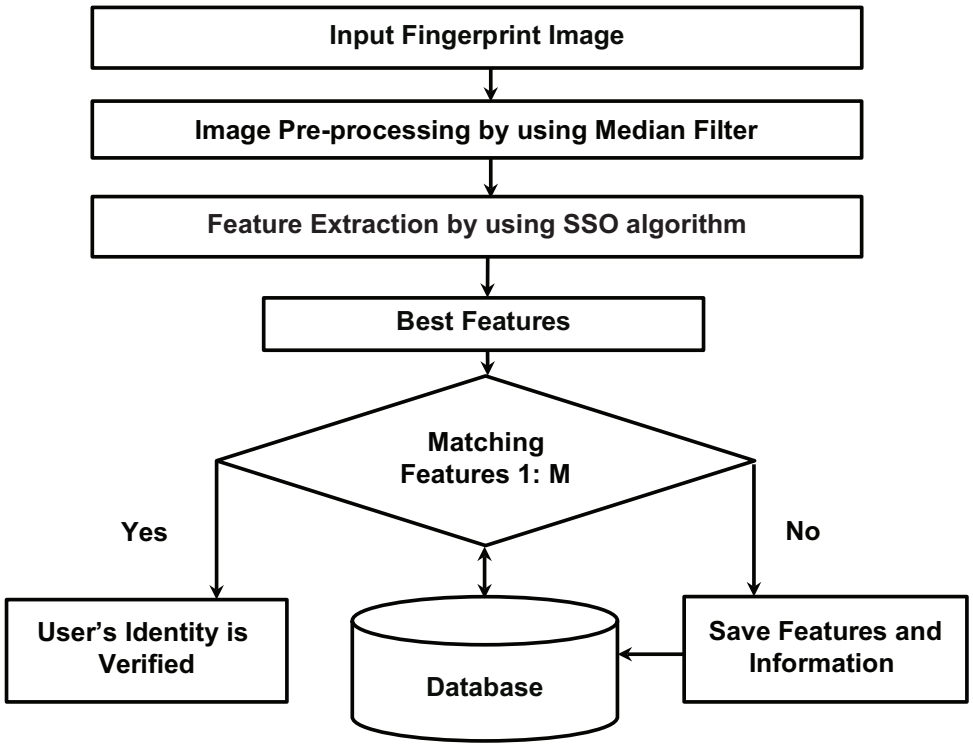

Fig. 4. Block diagram of the proposed method.

Fig. 5. Fingerprint image samples and ZKTeco device.

in the following subsections. Fig. 4 shows the block diagram of the proposed method.

4.1. Create a Database to Store and Organize Data

This is the first stage for handling this study, in which data acquisition is done using a newest and high-quality fingerprint device reader called (ZKT eco: ZK4500) which is the main requirement tool. Our dataset consists of merely (150) fingerprint images that were collected and acquired from various volunteer students of age ranging from 18 to 22 years at Technical College of Informatics (TCI) and Institute of Computer Science (ICS) at Sulaymaniyah city by the ZKTeco device. The taken real samples were resized to 128*128 and the format was also changed to Joint Photographic Experts Group. Furthermore, any image sizes with extensions bitmap, portable network graphics, and graphics interchange format can be handled by the proposed method. Fig. 5 demonstrates the ZKTeco device and some samples of fingerprint images. The database is created to store the information of the users and their seven features to be used later for the matching process.

4.2. Image Pre-processing Using Median Filter

This is the second stage of the proposed method. During live fingerprint scanning, a major issue that may be introduced is noise on the fingerprint image so that for removing and eliminating the noise from the fingerprint image and improve the performance and efficiency of the proposed system an efficient filter is required. In this stage, a (3*3) median filter is used as an efficient non-linear filter to remove noise from the user's fingerprint image. Therefore, an optimal image quality achieved after enhanced by utilizing the median filter

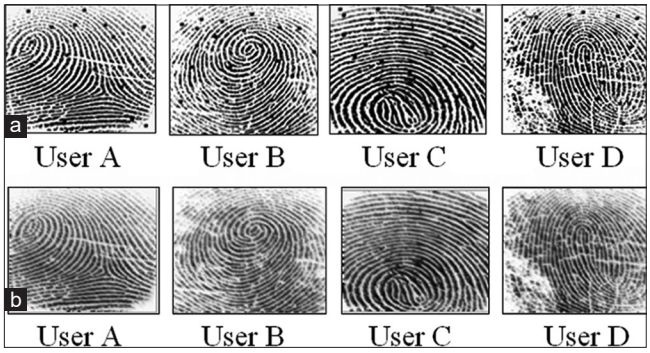

Fig. 6. (a) Original image and (b) fingerprint images before and after applying the median filter with mask (3*3).

which was ready for the feature extraction stage, as depicted in Fig. 6b.

4.3. Feature Extraction Using SSO Algorithm

In this stage, the SSO algorithm used to extract the best features from the user's fingerprint image. First, the SSO algorithm has applied to the fingerprint image. Second, the fitness or goodness has found for each location around the shark using fitness function (F). In this study, seven iterations have been applied by the SSO algorithm to extract seven best features from each user's fingerprint image where in each iteration only one feature extracted that has the highest fitness value. During the iteration of the algorithm, the shark's location has been updated to either forward according to seven or rotational according to eight. The determination of the shark's direction toward forwarding or rotational has relied on the fitness value of that location. The location that is visited by the SSO algorithm cannot be visited again. The applied SSO algorithm to find the best features is described in the algorithm (2) and the flowchart in Fig. 7.

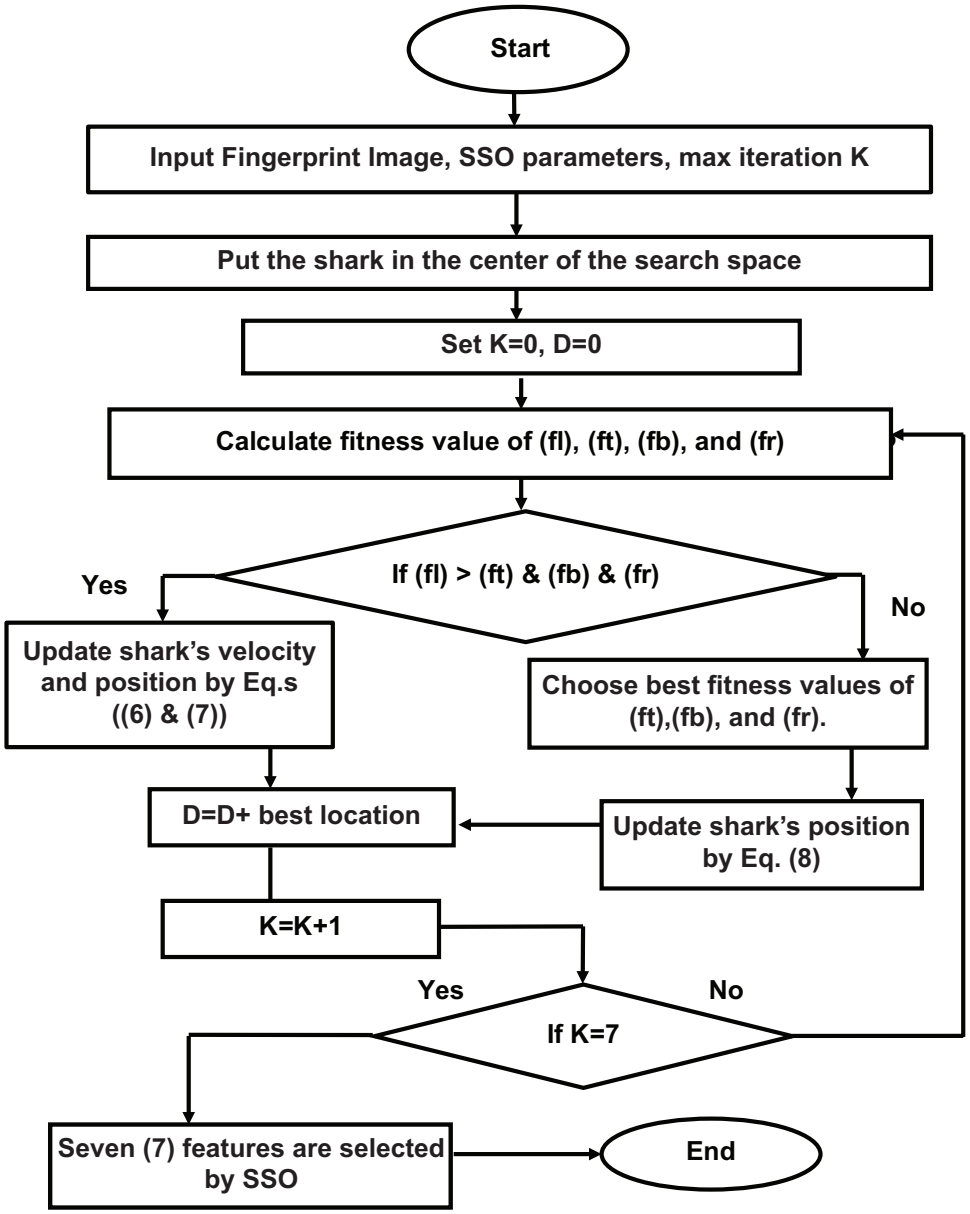

Fig. 7. Flowchart of the applied shark smell optimization algorithm.

4.4. Matching (Similarity) Process

This is the final stage and most significant stage of the proposed system because the reliability of any fingerprint authentication has relied on the matching process. The match (similar) operation is implemented using the ED calculated by (10) [24]. Similarity (matching) is carried out twice, the first is when entering the authorized user's data, where the fitness value of the user to be entered matches (similar) with all the fitness values of the database, this process called identification (1:M). The second takes place between the fitness value of the user claiming to be authorized and the fitness value of the authorized user that actually stored in the database, this process called verification (1:1).

$$\mathrm{ED}\left(\mathrm{p},\mathrm{q}\right) = \sqrt{\left(px - qx\right)^2 + \left(py - qy\right)^2} \qquad (10)$$

Where ED is the distance between point p and q at (x, y) coordinates.

Algorithm (2): Applied SSO algorithm for feature extraction

Input: User's Fingerprint Image, max iteration (k_{max}) = 7

Output: Selected 7 best features

Begin

Step 1: Set the SSO parameters (NP= 128, ND= 128, ηk=1, αk=1, Δt_k=1 and R1=R2=R3=1)

Step2: Put the shark in the center of the fingerprint image.

Step3: Calculate the fitness value of each location (ft, fb, fl and fr) around the shark by using fitness function (F).

Step4: If fitness (fl) > (fr) and (ft) and (fb) then

-Update Shark's velocity according to Eq. (6)

-Update Shark's position to forward movement according to Eq. (7)

Else

-Choose highest fitness value among (fr), (ft), (fb).

-Updating a shark's position to rotational movement according to Eq. (8)

Step5: new shark's position is identified

Step 6: If k is not equal to k_{max} then go to Step2

Step7: Seven (7) features are selected

End

End

5. RESULTS ANALYSIS AND DISCUSSION

In this section, the outcomes obtained from the proposed method have been explained in detail. The experimental results are tested with 150 fingerprint images and Fig. 8 shows only the first four samples. These samples are taken from students at both the TCI and the ICS at Sulaimani city using the ZKTeco device.

After loading the user's fingerprint image, it is pre-processed using a median filter with a mask (3*3) to remove the noise from the image without blurring the edges and other sharp details of the image. Both the original image and the filtered image for four various users are depicted in Fig. 6.

The proposed method used the SSO algorithm to extract seven best features from each user's fingerprint image and stored in the database for the matching process. Fig. 9 decomposes into four subfigures; each subfigure shows seven locations (best features) that are extracted by SSO for four users.

According to the results that are shown in the graphical representation of Fig. 9, it is confirmed that the SSO algorithm extracted seven best features depending on the fitness value of that location in a smart and random way.

Fig. 10 indicates the locations that are visited and chosen as features by the SSO algorithm after seven iterations for four fingerprint images. Since the unique features of each fingerprint

are located in the around of the center and those features are extracted indicated the efficiency of the algorithm used.

Table 1 displays the execution time elapsed in different iterations by the SSO algorithm to extract the best features. As a consequence, the SSO algorithm was highly efficient and required minimum time for extracting seven best features for each user's fingerprint image.

The elapsed execution time required for each stage of the proposed method for four users is tabulated in Table 2. According to the time execution results, the algorithm was highly efficient and fast. Based on the comparative results, the minimum and same time spent in both users (A) and (C) for features extraction when compared with the other users, followed by the user (B); however, the maximum time spent in user (D) for features extraction.

Moreover, the performance of the proposed method is evaluated and obtained from three renowned metrics, namely, FAR, FRR, and CVR. FAR, FRR, and CVR are calculated by (11), (12), and (13), respectively [25].

$$\text{FAR} = \text{number of FAR/total number of the test sample} \quad (11)$$

$$\text{FRR} = \text{number of false rejection/total number of the test sample} \quad (12)$$

$$\text{CVR} = (1\text{-FAR-FRR}) * 100\% \quad (13)$$

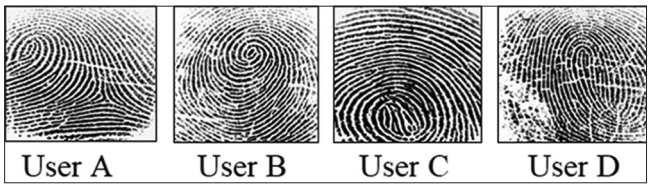

Fig. 8. Test fingerprint image samples for four users.

TABLE 1: Execution time and different iterations for SSO algorithm

Iteration no.	Time (s)
1	1
3	3.2
5	5.4
7	8

s=Second

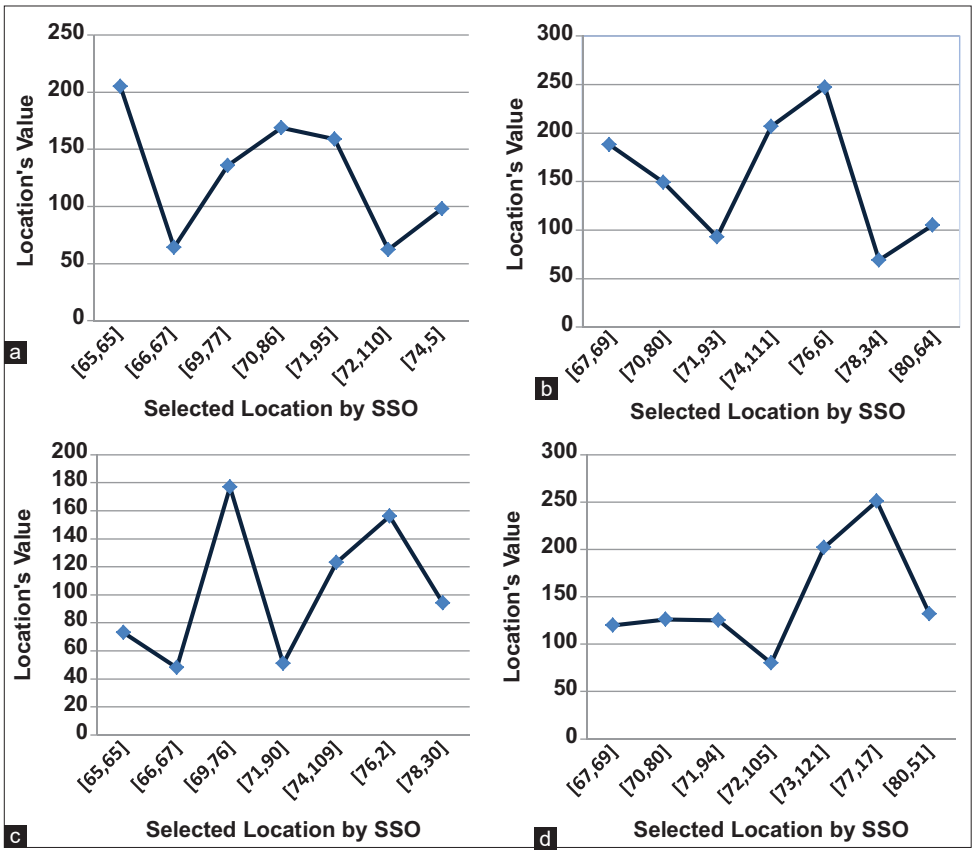

Fig. 9. (a-d) Relationship between the locations and their values for four users.

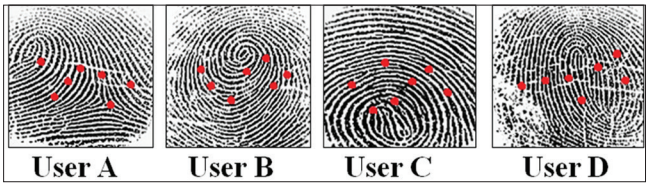

Fig. 10. Best locations that are visited by shark smell optimization algorithm.

TABLE 2: Execution time for each stage of the proposed method

No.	User	Pre-processing (s)	Features extraction (s)	Features matching (s)
1	A	11	7	8
2	B	12	8	9
3	C	11	7	8
4	D	11	9	10

For evaluating the performance of the proposed method, we tested our system using (15), (50), (100), and (150) user's fingerprint image, respectively. As a consequence, the system was extremely accurate according to FAR, FRR, and CVR which were 0.00, 0.00, and 100%, respectively, when (15) and (50) users used for the test. However, when we tested our system by incrementing the number of users to (100) and (150), solely (1) user was falsely rejected as an unauthorized user out of (100) and (150) users, as presented in Table 3.

TABLE 3: Performance of the proposed method

Fingerprint Image No.	Error rate metrics		
	FAR	FRR	CVR %
15	0.00	0.00	100
50	0.00	0.00	100
100	0.00	0.01	99
150	0.00	0.00666	99.334

FAR: False acceptation rate, FRR: False rejection rate, CVR: Correct verification rate

Ultimately, Table 4 displays the comparison that has been done in terms of error rate metrics between the performance of the proposed method and previous methods that are proposed by other researchers that are reviewed in the literature review. The performance of the proposed method was higher than the other methods when tested using the datasets of Mahale *et al.* [9] and Dakhil and Ibrahim [12] due to using an intelligence algorithm for feature extraction, as shown in Table 4.

TABLE 4: A comparison between the performance of the proposed method and previous methods

Ref.	Algorithm used	FAR	FRR	CVR%
[9]	Minutiae extractor algorithm (MEA)	0.0154	0.0137	97.09
[12]	Filter bank based (FBB) algorithm and K-nearest neighbor (K-NN)	0.012698	0.047619	93.9683
Proposed method	SSO algorithm	0.00	0.0125	98.75

FAR: False acceptation rate, FRR: False rejection rate, CVR: Correct verification rate

Moreover, the results that are shown in Table 4 proved that using a SI algorithm for proposing a fingerprint authentication system achieved higher CVR than the other algorithms used in the previous methods.

6. CONCLUSION AND FUTURE WORK

In this paper, a credible fingerprint authentication was proposed using a new SI algorithm named SSO. Conclusions that can be inferred from this study are listed as the following:

- Fig. 6 showed that the median filter was a good filter for noise elimination and image enhancement.
- Fig. 9 indicated that the 7 locations (best features) that are extracted by the SSO algorithm had high fitness value and were chosen in a smart and random way.
- Table 2 presented that the proposed method was fast and each stage elapsed minimum execution time.
- Table 3 presented that the proposed method was an excellent fingerprint authentication that based on intelligent algorithm because it gave higher CVR which was 99.334% and lower FAR and FRR which were 0.00 and 0.00666, respectively.
- According to Table 4, the performance of the proposed method was higher than the previous methods which proved that using an intelligence algorithm to propose fingerprint authentication gives a higher CVR rate than the traditional algorithms.

For future study, we intend to examine, practice, and mix more than one SI algorithms for instance: ABC, FA, PSO, and SSO variations such as chaotic binary SSO (CBSSO) algorithm to propose more complex unimodal fingerprint biometric authentication to achieve a better rate of FAR, FRR, and CVR.

7. AKNOWLEGMENT

The authors would like to thank the volunteer students at TCI and ICS at Sulaymaniyah city for their unconditional participation to give their fingerprint images during data collection.

REFERENCES

[1] O. J. Ayangbekun and A. P. Ajigboteso. "Simulation of an authorization system using access cards with chips and fingerprint". *IJRIT International Journal of Research in Information Technology*, vol. 2, no. 10, pp. 601-610, 2014. Available from: https://www.researchgate.net/publication/329538683_Simulation_of_an_Authorization_System_Using_access_cards_with_chips_and_fingerprint. [Last accessed on 2019 Oct 28].

[2] C. Wang, Y. Wang, Y. Chen, H. Liu and J. Liu. "User authentication on mobile devices: Approaches, threats and trends". *Computer Networks*, vol. 170, pp. 107-118, 2020.

[3] C. Rathgeb and A. Uhl. "A survey on biometric cryptosystems and cancelable biometrics". *EURASIP Journal on Information Security*, vol 1, p. 3, 2011.

[4] E. Chandra and K. Kanagalakshmi. "Noise elimination in fingerprint image using median filter". *The International Journal of Advanced Networking and Applications*, vol. 2, no. 6, pp. 950-955, 2011. Available from: http://www.citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.419.1632&rep=rep1&type=pdf. [Last accessed on 2019 Nov 01].

[5] S. K. Sahoo, T. Choubisa and S. M. Prasanna. "Multimodal biometric person authentication: A review". *IETE Technical Review*, vol. 29, no. 1, pp. 54-75, 2012.

[6] M. G. Abdul-Haleem, L. E. George and H. M. Al-Bayti. "Fingerprint recognition using haar wavelet transform and local ridge attributes only". *International Journal of Advanced Research in Computer Science Software Engineering*, vol. 4, no. 1, 2014. Available from: https://www.researchgate.net/publication/335025795_Fingerprint_Recognition_Using_Haar_Wavelet_transform_and_local_ridge_attributes_only. [Last accessed on 2019 Sep 17].

[7] A. Çalışkan and Ö. F. Ertuğrul. "Wavelet Transform Based Fingerprint Recognition". In *2015 23nd Signal Processing and Communications Applications Conference*, pp. 1481-1484, 2015.

[8] U. H. L. Akter. "Speeded-up Robust Feature Extraction and Matching for Fingerprint Recognition". *2nd International Conference on Electrical Engineering and Information and Communication Technology*, 2015.

[9] V. H. Mahale, M. M. Ali, P. L. Yannawar and A. T. Gaikwad. "Fingerprint Recognition for Personal Identification and Verification Based on Minutiae Matching". In: *IEEE 6th International Conference on Advanced Computing*, pp. 332-339, 2016.

[10] H. R. Su, K. Y. Chen, W. J. Wong and S. H. Lai. "A Deep Learning Approach Towards Pore Extraction for High-Resolution Fingerprint Recognition". In: *2017 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 2057-2061, 2017.

[11] Z. J. Ahmed and L. E. George. "Fingerprints recognition using the local energy distribution over haar wavelet subbands". *International Journal of Science Research*, vol. 6, no. 9, pp. 979-986, 2017.

[12] I. G. Dakhil and A. A. Ibrahim. "Design and implementation of fingerprint identification system based on KNN neural network". *Journal of Computer Communications*, vol. 6, no. 3, pp. 1-18, 2018.

[13] A. Kyaw and Z. L. Aung. "A robust fingerprint recognition technique applying minutiae extractors and neural network". *International Journal of Engineering Research and Advanced Technology*, vol. 5, no. 3, pp. 78-87, 2019.

[14] H. Kaur and H. S. Pannu. "Zernike moments-based fingerprint recognition using weighted-support vector machine". *Modern Physics Letters B*, vol. 33, no. 21, pp. 1950245.

[15] M. Mavrovouniotis, C. Li and S. Yang. "A survey of swarm intelligence for dynamic optimization: Algorithms and applications". *Journal of Swarm and Evolutionary Computation*, vol. 33, pp. 1-22, 2017.

[16] S. Mohammad-Azari, O. Bozorg-Haddad and X. Chu. "Shark smell optimization (SSO) algorithm". In: *Advanced Optimization by Nature-Inspired Algorithms*, Springer, Berlin, pp. 93-103, 2018.

[17] M. Ehteram, H. Karami, S. F. Mousavi, A. El-Shafie and Z. Amini. "Optimizing dam and reservoirs operation based model utilizing shark algorithm approach". *Journal Knowledge-Based Systems*, vol. 122, pp. 26-38, 2017.

[18] O. W. Salami, I. J. Umoh, E. A. Adedokun, M. B. Mu'azu and L. A. Ajao. "Efficient Method for Discriminating Flash Event from DoS Attack during Internet Protocol Traceback using Shark Smell Optimization Algorithm. In: *2019 2nd International Conference of the IEEE Nigeria Computer Chapter*, pp. 1-10, 2019.

[19] H. Hosseinzadeh and M. Sedaghat. "Brain image clustering by wavelet energy and CBSSO optimization algorithm". *Journal of Mind and Medical Sciences*, vol. 6, no. 1, pp. 110-120, 2019.

[20] N. Gnanasekaran, S. Chandramohan, P. S. Kumar and A. M. Imran. "Optimal placement of capacitors in radial distribution system using shark smell optimization algorithm". *Ain Shams Engineering Journal*, vol. 7, no. 2, pp. 907-916, 2016.

[21] O. Abedinia, N. Amjady and A. Ghasemi. "A new metaheuristic algorithm based on shark smell optimization". *Complexity*, vol. 21, no. 5, pp. 97-116, 2016.

[22] H. Hosseinzadeh. "Automated skin lesion division utilizing Gabor filters based on shark smell optimizing method". *Evolving Systems*, 43, pp. 1-10, 2018.

[23] S. A. Juma. "*Optimal Radial Distribution Network Reconfiguration Using Modified Shark Smell Optimization*". MSc. Thesis, Jkuat-Pausti. Available from: http://www.ir.jkuat.ac.ke/bitstream/handle/123456789/4854/Shaibu_Ali_Juma_EE300-0012%20%2017_Thesis%20Report.pdf?sequence=1&isAllowed=y.

[24] K. M. Sagayam, D. N. Ponraj, J. Winston, E. Jeba and A. Clara. "Authentication of biometric system using fingerprint recognition with euclidean distance and neural network classifier". *International Journal of Innovative Technology Exploring Engineering*, vol. 8, no. 4, pp. 766-771, 2019.

[25] T. W. A. Khairi. "Secure mobile learning system using voice authentication". *Journal of Engineering Applied Sciences*, vol. 14, no. 22, pp. 8180-8186, 2019.