International Journal of Advances in Intelligent Informatics
Vol. 6, No. 2, July 2020, pp. 123-134
ISSN 2442-6571

Fingerprint recognition based on shark smell optimization and genetic algorithm

Bakhan Tofiq Ahmed [a,1,*], Omar Younis Abdulhameed [b,2]

[a] Department of Information Technology, Technical College of Informatics, Sulaimani Polytechnic University, Sulaimani, Kurdistan Region, Iraq
[b] Department of Computer Science, College of Science, University of Garmian, Kalar, Garmian, Kurdistan Region, Iraq
[1] bakhan.tofiq.a@spu.edu.iq; [2] omar.y@garmian.edu.krd
* corresponding author

ARTICLE INFO

Article history
Received May 9, 2020
Revised June 26, 2020
Accepted June 28, 2020
Available online July 12, 2020

Keywords
Fingerprint recognition
Swarm intelligence
Shark smell optimization
Genetic algorithm
Chebyshev polynomial first kind

ABSTRACT

Fingerprint recognition is a dominant form of biometric due to its distinctiveness. The study aims to extract and select the best features of fingerprint images, and evaluate the strength of the Shark Smell Optimization (SSO) and Genetic Algorithm (GA) in the search space with a chosen set of metrics. The proposed model consists of seven phases namely, enrollment, image preprocessing by using weighted median filter, feature extraction by using SSO, weight generation by using Chebyshev polynomial first kind (CPFK), feature selection by using GA, creation of a user's database, and matching features by using Euclidean distance (ED). The effectiveness of the proposed model's algorithms and performance is evaluated on 150 real fingerprint images that were collected from university students by the ZKTeco scanner at Sulaimani city, Iraq. The system's performance was measured by three renowned error rate metrics, namely, False Acceptance Rate (FAR), False Rejection Rate (FRR), and Correct Verification Rate (CVR). The experimental outcome showed that the proposed fingerprint recognition model was exceedingly accurate recognition because of a low rate of both FAR and FRR, with a high CVR percentage gained which was 0.00, 0.00666, and 99.334%, respectively. This finding would be useful for improving biometric secure authentication based fingerprint. It is also possibly applied to other research topics such as fraud detection, e-payment, and other real-life applications authentication.

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

Biometric derived from the two Greek words, the first is Bios, which means "life", and the second is the 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. This technology provides more reliability than the traditional approaches because of body characteristics cannot be stolen, copied, or forging easily by an intruder [3]–[5]. Fingerprint recognition is the most widely used biometric form due to its uniqueness and long term stability. The pattern of ridges and valleys on the fingertip surface is known as fingerprint [6][7]. A fingerprint recognition system can provide two kinds of identity management functionalities, namely, identification and verification [8][9]. Swarm-Intelligence (SI) is an Artificial-Intelligent (AI) method that relied on group behavior that originated in nature. It has a system characteristic when the cooperative agent behaviors locally cooperate with their environments, such as Ant-Colony's searching, Bird's flocking, Bacteria's evolving, and Fishes schooling [10][11]. In addition, the SI compromises of several algorithms like Ant-Colony Optimization, Particle-Swarm Optimization, Artificial-Bee-Colony, Bacterial-Foraging Optimization, Fire-Fly Algorithm, and Artificial-Fish-Swarm Optimization, and Shark Smell Optimization Algorithm [12].

Many researchers proposed fingerprint recognition depending on the traditional algorithms. Dakhil and Ibrahim [13] proposed a fingerprint recognition system that relied on Filter Bank Based (FBB) algorithm. The fingerprint images were enhanced by using the Fourier Domain Analysis Filtering and Segmentation. The Filter Bank Based (FBB) algorithm is used for the feature extraction stage, and the matching process has done by using K-Nearest Neighbor (K-NN) technique and 70% threshold value.

A collection of 90 fingerprint images is used to evaluate the CVR, FAR, and FRR which were 93.9683%, 0.012698, and 0.047619, respectively. Oo and Aung [14], in this research paper, a Neural Network (NN) Classifier is used to propose a fingerprint recognition system. Firstly, the Digital Persona 4500 fingerprint scanner acquired the input fingerprint image. Secondly, the images are enhanced using Contrast Stretching and 2 Morphological techniques such as Dilation and Erosion. Thirdly, Minutiae Based Approach used to extract features from the region of interest (ROI) of the fingerprint image. Afterward, features were fed into the Neural Network for user recognition. According to experimental consequences, the system attained 96.5% of CVR. Kaur *et al.* [15], proposed a novel similarity measure-based random forest (NRF). Additionally, a dual-tree complex wavelet transform (D-TCWT) is used for feature extraction. However, the information gain-based feature selection technique is used for feature selection. The proposed system gave 98.03% of accuracy.

From the previous works, it has been found that the development of proficient fingerprint recognition is still an open era of research, and swarm intelligence algorithms will give a higher CVR than the traditional algorithms. Hence, the primary aim of this study is to construct a credible fingerprint recognition using an intelligent algorithm. Furthermore, the proposed method mimics Shark's ability called shark smell optimization integrated with the genetic algorithm to attain the highest correct verification rate (CVR), lowest false accept rate (FAR), and false reject rate (FRR).

The organization of the other sections in this study as follows: the brief theoretical concepts about the SSO algorithm, GA, and CPFK with the main phases of the proposed model have been discussed in Section 2. In Section 3, the experimental results obtained from the proposed model was explained in detail. Ultimately, Section 4 is about the conclusion.

2. Method

This section presents the stages of the proposed model, where the Shark Smell Optimization (SSO) algorithm is used to extract features, and a Genetic Algorithm (GA) is used to select the best features among the extracted features from the user's fingerprint image. The proposed model consists of seven stages, namely, enrollment (input), image preprocessing, feature extraction, weights generation, feature selection, creation of a user's database, and matching process. Each stage has been illustrated in detail, as in Fig. 1.

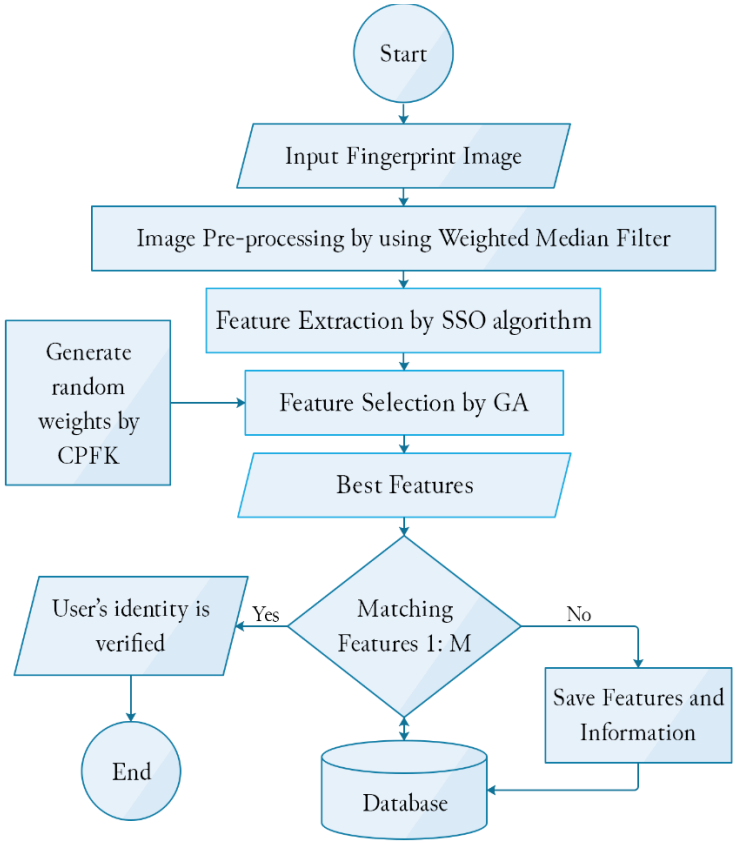

Fig. 1. Flowchart of the proposed model.

2.1. Enrollment (input) stage

Enrollment is the first stage, where the fingerprint images are enrolled in the proposed model. The enrolled fingerprint images were collected and acquired from 150 various volunteer students of the Technical College of Informatics (TCI) and Institute of Computer Science (ICS) at Sulaimaniya city, Iraq, age ranging from 18 to 22 years, by using the fingerprint reader device called ZKTeco sensor with high resolution (500 dpi). The proposed model handles images with the size (128 * 128) pixels and JPEG extension. However, it also can handle any image size with BMP, TIF, and PNG extensions. Fig. 2 presents some fingerprint image samples and the ZKTeco device.

Fig. 2. User's fingerprint image samples and ZKTeco device.

2.2. Image preprocessing by using the weighted median filter

During live fingerprint scanning, noise is a major issue that may appear on the fingerprint image. An efficient filter is required to remove the noise and improve the proposed model performance and efficiency. A (3*3) weighted median filter mask is used to scan over the entire image of size (128*128) to eliminate noisy pixels. It is a standard median filter extension and is widely used because it effectively removes salt, pepper noise, and edge-preserving. It replaces the original gray level of a pixel by the weighted median value in its neighborhood after assigning weight to each pixel value in the original image [16][17]. Therefore, an optimal image quality achieved after utilizing the WMF.

2.3. Feature extraction by using SSO algorithm

Shark Smell Optimization (SSO) has relied on the Shark's ability because it has superiority in catching prey by using a strong smell sense in a short time [18]–[20]. SSO algorithm consists of four basic steps as follows:

1) Initialization of SSO

The initial solution of a population of the SSO algorithm must be generated randomly within the search space. Each of these solutions represents a particle of odor which shows a possible Shark position at the beginning of the search process. The initial solution vector is shown in (1) and (2), respectively, where X_i^1 = ith initial position of the population vector and NP = population size.

$$X^1 = [X_1^1, X_2^1, \dots\dots, X_{NP}^1] \tag{1}$$

The related optimization problem can be expressed as:

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

where $X_{i,j}^1$ were jth dimension of the Shark's ith position, and ND for the decision variables number [21].

2) Forward movement of the SSO toward the target

When the blood is released in the water, the Shark with a velocity "V" moves toward stronger odor particles in each location, to become closer to the prey (target). So the velocity in each dimension is calculated by (3).

$$V_{i,j}^k = \eta\mathrm{k}.\,\mathrm{R1}.\frac{\partial(OF)}{\partial xj}\Big|_{x_{i,j}^k} \tag{3}$$

where k= 1, 2, ..., k_{max}, $\frac{\partial(OF)}{\partial xj}\Big|_{x_{i,i}^k}$ is a derivative of the objective function (OF) at the position $x_{i,j}^k$, k_{max} is the maximum number of stages for forwarding movement of the Shark, k is the number of stages, ηk is a value in the interval [0, 1], and $R1$ for a random number in the interval [0, 1] [22]. The increase in the odor intensity determines the increase in Shark's velocity. Because of having inertia, the acceleration of Shark is limited. Therefore, the current Shark's velocity relays on its previous velocity, which can be employed by modifying (3) as shown in (4).

$$V_{i,j}^k = \eta_{\mathrm{k}}.\,\mathrm{R1}.\frac{\partial(OF)}{\partial xj}\Big|_{x_{i,j}^k} + \alpha_{\mathrm{k}}.\,\mathrm{R2}.\,\mathrm{V}_{\mathrm{i,j}}^{\mathrm{k}-1} \tag{4}$$

where αk is the inertia coefficient in the interval [0, 1], $\mathrm{V}_{\mathrm{i,i}}^{\mathrm{k}-1}$ Shark's previous velocity and $R2$, like $R1$ is a random number in the interval [0, 1]. Due to Shark's forward movement, its new position is Y_i^{k+1} determined relied on its previous position (X_i^k) and velocity (V_i^k). Thus, the new position of the Shark can be defined as in (5).

$$Y_i^{k+1} = X_i^k + V_i^k.\Delta\mathrm{t_k} \tag{5}$$

where Δtk is a time interval, which is assumed to be 1 for simplicity [23].

3) Rotational movement of the SSO toward the target

The Shark is also has a rotational movement, which is used to find stronger odor particles. This process of the SSO algorithm is called local search, which can be described as in (6).

$$Z_i^{k+1,m} = Y_i^{k+1} + R3.\,Y_i^{k+1} \tag{6}$$

where m = 1, 2,..., M, and R3 is a random number in the interval [−1, 1]. In the local search, many points (M) are connected to form closed contour lines and model the Shark's rotational movement in the search space [24].

4) Updating the particle position

The Shark's search path will continue with the rotational movement as it moves closer to the point with a stronger odor sense. This characteristic in the SSO algorithm can be expressed as in (7).

$$X_i^{k+1} = \arg\max\{ OF(Y_i^{k+1}), OF(Z_i^{k+1,i}), .., OF(Z_i^{k+1,M})\} \quad (7)$$

where X_i^{k+1} represents the next position of the Shark with the highest objective function (OF) value [25].

In this stage, the SSO algorithm is used to extract the user's fingerprint image's best features. Firstly, identify the starting position of the Shark, which is determined to be in the center of the filtered image. Secondly, the fitness or goodness has found for each location around the Shark by using fitness function (F). Thirdly, apply the SSO algorithm to extract the best features. In this study, 21 features have been extracted by the SSO algorithm from each user's fingerprint image by applying 21 iterations. Each iteration has only one feature extracted with the highest fitness value. During the iteration, the Shark's location has been updated either to forward according to (5) or rotational according to (6) based on the fitness value. If the fitness value of the location in Shark's forward movement is higher than the fitness value of locations Shark's rotational movement, then Shark's position is updated according to (5). Otherwise, it is updated, according to (6). The determination of Shark's direction toward forwarding or rotational relies on the fitness value of that location; also, the locations that are visited by the SSO algorithm cannot be revisited. The algorithm 1 (Fig. 3) shows the steps of applied SSO for feature extraction.

Algorithm 1: Applied SSO Algorithm for Feature Extraction

1. **Input:** User's Fingerprint Image, max iteration (kmax) = 21
2. **Output:** Extracted 21 best features
3. **Begin**
4. **Step1:** Set the SSO parameters (NP= 128, ND= 128, $\eta k = 1$, αk=1, Δt_k=1 and R1=R2=R3=1)
5. **Step2:** Put the Shark in the center of the fingerprint image.
6. **Step3:** While (kmax is not satisfied) do
7. **Step4:** Calculate the fitness value of each location (ft, fb, fl, and fr) around the Shark by using fitness function (F)
8. **Step5:** If fitness (**fl**) > (**fr**) **and** (**ft**) **and** (**fb**) **then**
9. Update Shark's velocity by using Eq. (4)
10. Update Shark's position to forward movement according to Eq. (5)
11. **Else**
12. Choose highest fitness value among (fr), (ft), (fb).
13. Updating a shark's position to rotational movement according to Eq. (6)
14. **Step6:** New Shark's position is identified
15. **End while**
16. **Step7:** 21 features are extracted
17. **End**

Fig. 3. Applied SSO Algorithm for Feature Extraction

2.4. Random weight generation by using CPFK

Based on its name, CPFK is firstly introduced by a well-known Russian Mathematician named Pafnuty Lvovich Chebyshev (P.L.C) in 1854 [26]. CPFK is a prototype of a chaotic map. It is described as Fk(x) of the first type which is a polynomial of x with degree k, can be calculated as in (8).

$$Fk(x) = cos(k\,cos^{-1}x) \quad or \quad Fk(cos\theta) = cos(k\theta) \quad for\ x = cos\theta \tag{8}$$

where x represents a variable in the interval [-1,1], and k is positive number or (non-negative integer). They can be recursively generated with the following formulas: Let k= 0,1,2,3. Then, these can be obtained: $cos0\theta = 1$, $cos1\theta = cos\theta$, $cos2\theta = 2cos2\theta - 1$, and $cos3\theta = 4cos3\theta - 3cos\theta$. Let $cos\theta$ = x. Then, these can be attained: F0(x) = 1, F1(x) = x, F2(x) = 2x2 −1, F3(x) = 4x3 −3x, Fk+1(x) = 2xFk(x) − Fk−1(x). As a result, CPFK map *Fk*: [−1, 1]⟶[−1, 1] of degree *k*, when *k*>1 [27][28].

CPFK has been performed as a random generation algorithm. The main objective of using CPFK is to generate random numbers (weights) according to equation (8) that are required to initialize the population of GA. The steps of CPFK for random weight generation are presented in the algorithm 2 (Fig. 4).

Algorithm 2: Applied CPFK algorithm for Random Weights Generation
1. **Input:** k=5, x0= 0.2, required max iteration (I max), where k is the CPFK degree at point x0
2. **Output:** Generated random numbers (weights)
3. **Begin**
4. **Step 1:** Set I=0
5. While (I <= I max)
6. Begin
7. Fk(x1) = cos (k $\cos^{-1} x0$)
8. x0=x1
9. I= I+1
10. End
11. **End**

Fig. 4. Applied CPFK algorithm for Random Weights Generation

2.5. Feature selection by using GA

Genetic Algorithm (GA) is an adaptive heuristic search algorithm relies on the evolutionary ideas of natural selection and genetics [29][30]. This method involves the improvement of a population of chromosomes, where each chromosome denotes a potential solution. Each chromosome consists of numerous genes; their number is varying according to the optimization problem. The genes of each chromosome are encoded either by binary digits (0 or 1) or real number [31][32]. This algorithm performs through five critical phases, namely, initialize population, fitness value calculation, selection operation, crossover operation, and mutation operation [33].

In this stage, GA is used as an efficient feature selection algorithm to select the best seven features among 21 extracted features by SSO for each user. The features that are attained the highest fitness value according to fitness function (F) are the best. Each user has 21 features, where it is divided into three equal groups, which are (x1, x2, and x3). GA starts with a random initial population of weights that are generated by using CPFK, as explained in subsection (2.4). The fitness value is calculated for each group, according to (9) and (10).

$$Y' = \sum_{i,j=1}^{n} Xi * Wj \tag{9}$$

where X represents 21 features divided into three equal groups (x1, x2, and x3), W denotes weights, and i = j=1, 2,...., n=7.

$$F(C) = 1/|Y - Y'| \tag{10}$$

where F(C) represents fitness function, while |Y-Y'| is absolute error, Y represents the best location (highest pixel value) in the image, and Y' is calculated by (9). After calculating the fitness value for each group, the main phases of GA are applied. Because GA works by an iterative method, it will generate a new generation until it reaches the maximum iteration. Consequently, the seven best features selected

by GA for each user are multiplied by seven weights and stored in the database with its fitness values. The Algorithm 3 (Fig. 5) indicates the steps of applied GA for feature selection.

Algorithm 3: **Applied GA for Feature Selection**

1. **Input:** x1, x2, x3 as features, max generation ($G_{\max}$) = 40
2. **Output:** Selected 7 best features by GA
3. **Begin**
4. **Step1:** Generate random initial population of (weights) Wj^0 by using CPFK, as shown in the algorithm (2).
5. **Step2:** Calculate the fitness value for each (x1, x2, and x3) according to Eq. (9) and Eq. (10).
6. While ($G_{\max}$ not satisfied) do
7. Perform selection operation by selecting 2 (weights) Wj^0 (e.g., $W1^0$, $W3^0$) as a parent that obtained the highest fitness value.
8. Perform crossover operation by recombining some weights of a parent ($W1^0$) with some weights of a parent ($W3^0$) to create a new individual weight called offspring.
9. Perform mutation operation by altering one weight from offspring by a particular mutation rate (i.e., weight divided by 2) to create a new individual called a mutant.
10. Accept the new population (or new generation) by placing a new individual (mutant) with old individuals (parents) in the new population to produce a new generation.
11. **End while**
12. **Step3:** 3 new weights are produced defined as (W1), (W2), and (W3)
13. **Step4:** Get new fitness value defined as (fW1), (fW2), and (fW3)
14. **Step5:** Choose and store the best fitness
15. **End**

Fig. 5. Applied GA algorithm for Feature Selection

2.6. Creation of a user's database

Before proposing the model, a database is created to store the information's users and their seven features to be used later for the matching process.

2.7. Matching (similarity) process

This is the final and most significant stage of the proposed model because the reliability of any fingerprint recognition relies on the matching process. In this study, the match (similar) operation is implemented by using the Euclidean Distance (ED). ED is a distance measurement used to calculate the similarity ratio between two points that can be computed by mathematical formulation as revealed in (11), where ED is the Euclidean distance between point p and q at (x, y) coordinates [34].

$$ED\ (p,q)\ =\ \sqrt{(px-qx)^2+(py-qy)^2} \tag{11}$$

ED is used because it is the only Metric that is the same in all directions, that is, rotation invariant. Similarity (matching) is carried out twice. The first is when entering the authorized user's data, where the fitness value of the user compares to all the fitness values of the database, this process called identification (1:M). The second takes place between the user's fitness value claiming to be authorized, and the authorized user's fitness value stored in the database, this process called verification (1:1).

3. Results and Discussion

The dataset has been prepared by collecting 150 real fingerprint image samples, as depicted in Fig. 2. One hundred fifty fingerprint samples are used to test the efficacy of the proposed model. The filtered image has been achieved after applying a weighted median filter on the user's fingerprint image, both original image and the filtered image for four users (A), (B), (C), and (D) has been depicted in Fig. 6.

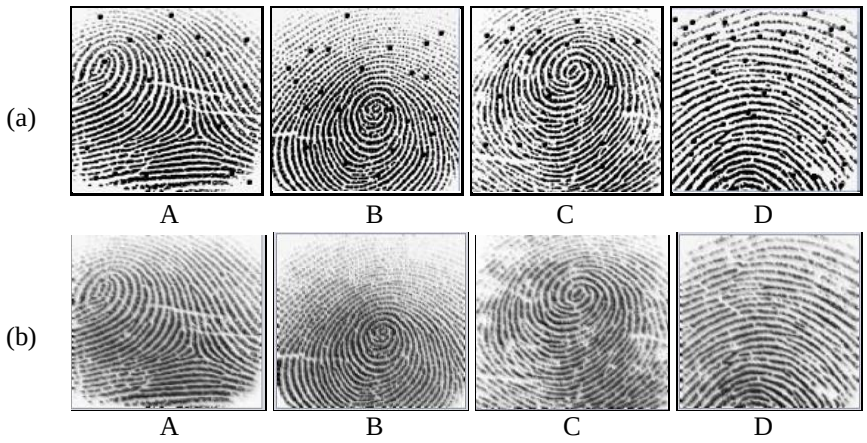

Fig. 6. Result of applying a weighted median filter on a noisy image; (a) original noisy image and (b) filtered image.

The proposed model uses SSO algorithm to extract 21 features from each user's fingerprint image. Fig. 7 decomposes into four subfigures, and each subfigure shows 21 locations (best features) that are extracted by SSO for four users.

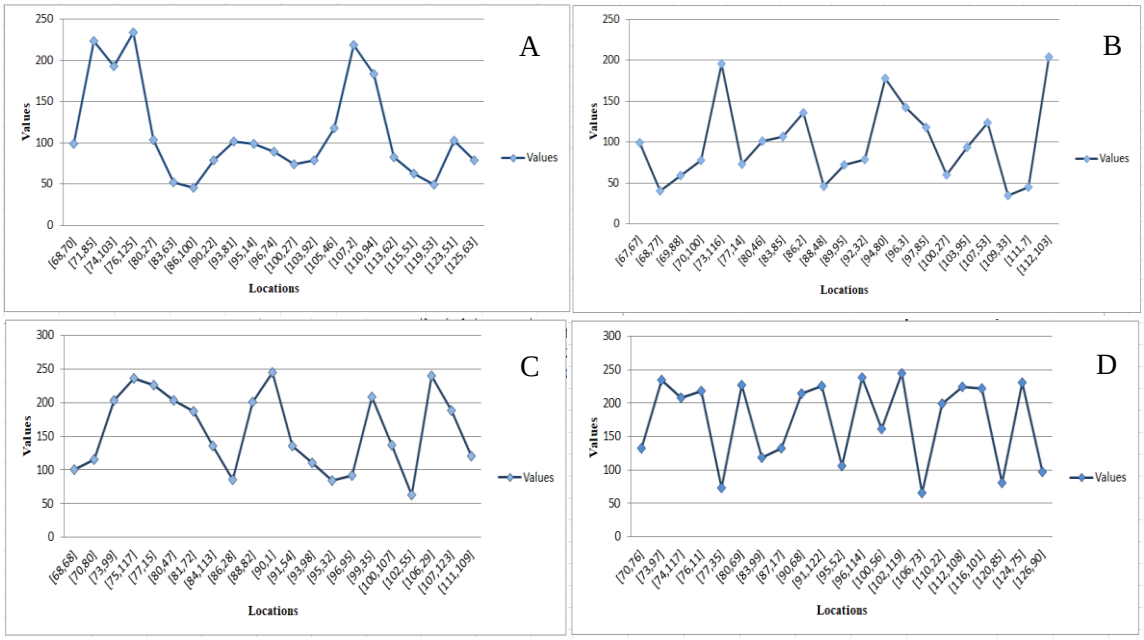

Fig. 7. The relation between locations and their values for users.

Some of the random weights that are generated by Chebyshev Polynomial First Kind (CPFK) are demonstrated in Table 1.

Table 1. Weight's value that is randomly generated by CPFK

No.	Weight values	No.	Weight values	No.	Weight values	No.	Weight values	No.	Weight values
1	**0.37828**	8	0.33285	15	0.97646	22	0.56216	29	0.90267
2	0.60490	9	0.53723	16	0.27129	23	0.89062	30	0.62474
3	0.94269	**10**	**0.85558**	17	0.45532	24	0.67158	31	0.96235
4	0.44644	11	0.78921	**18**	**0.72768**	25	0.99366	**32**	**0.34699**
5	**0.71332**	12	0.93713	19	0.99499	26	0.17472	33	0.55774
6	0.99904	13	0.47324	20	0.16709	**27**	**0.35613**	34	0.88461
7	0.14370	14	0.75656	21	0.35000	28	0.57127	35	0.69374

In Table 1 is shown that CPFK was an efficient random generation algorithm because it generated a sequence of different weights without duplication. In this study, feature selection is done by using GA because it is efficient, fast, and able to find optimal solutions in a short time. Therefore, the seven best features selected by GA for four users with its fitness values are displayed in Table 2.

Table 2. The features and fitness values for users

User	Feature 1	Feature 2	Feature 3	Feature 4	Feature 5	Feature 6	Feature 7	Fitness values
A	0.19117	0.37023	0.59255	0.92889	0.51177	0.81735	0.88603	519.04372
B	0.33672	0.54279	0.86363	0.76464	0.96862	0.31377	0.51050	79.3516
C	0.93973	0.46079	0.73651	0.99085	0.19082	0.36991	0.59207	122.83995
D	0.22558	0.40353	0.64441	0.97832	0.26106	0.44302	0.70778	255.02494

According to Table 2, each user had distinctiveness features that were selected by GA that indicated the efficiency of the algorithm used. Ultimately, performance of the proposed model is measured and evaluated by three renowned metrics, namely, False Acceptance Ratio (FAR), False Rejection Ratio (FRR), and Correct Verification Rate (CVR). FAR, FRR and CVR [35] can be calculated as:

$$FAR = number\ of\ false\ acceptation\ /\ total\ number\ of\ the\ test\ sample \quad (12)$$

$$FRR = number\ of\ false\ rejection\ /\ total\ number\ of\ the\ test\ sample \quad (13)$$

$$CVR = (1 - FAR - FRR) * 100\ \% \quad (14)$$

To evaluate the proposed model performance, we tested our model by using 15, 50, 100, and 150 fingerprint images that are taken from the private dataset, respectively. As a consequence, the proposed model was extremely accurate according to FAR, FRR, and CVR metric, as tabulated in Table 3.

Table 3. Evaluating the proposed model performance through error rate metrics.

Image No.	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**

The highest rate of CVR has been attained that proved the credibility of the proposed model, as in Table 3. Table 4 displays the comparison that has been done between the performance of the proposed model and previous models that are proposed by other researchers. The proposed model achieved higher CVR than the previous models.

Table 4. A Comparison between the performance of the proposed model and previous models.

Ref.	Algorithm Used	FAR	FRR	CVR%
Ali et al. [36]	Minutiae Extractor Algorithm (MEA)	0.0154	0.0137	97.09
Dakhil and Ibrahim [13]	Filter Bank Based (FBB) algorithm and K-Nearest Neighbor (K-NN)	0.012698	0.047619	93.9683
Oo and Aung [14]	Neural Network (NN)	-	-	96.5
Kaur *et al.* [15]	Novel similarity measure-based random forest (NRF)	-	-	98.03
Proposed Model	**SSO and GA**	**0.00**	**0.00666**	**99.334**

The execution time for each stage of the proposed model is shown in Table 5. It can be seen that the execution times were in good performance. It means that the proposed model is efficient.

Table 5. Execution time for each stage of the proposed model

No.	User	Preprocessing (sec)	Weights Generation (sec)	Features Extraction (sec)	Features Selection (sec)	Matching Features (sec)
1	A	11	6	21	28	28
2	B	11	6	19	30	27
3	C	12	6	20	30	28
4	D	11	6	21	29	27

4. Conclusion

In this paper, a credible and efficient fingerprint recognition model is proposed using a shark smell optimization (SSO) algorithm and a genetic algorithm (GA). In this section, valuable findings have been reached at which were used weighted median filter (WMF) was a good filter for noise elimination and image enhancement. The locations that are chosen by the SSO algorithm have high fitness value and were chosen intelligently and randomly. The Chebyshev Polynomial First Kind (CPFK) was a powerful number generation algorithm because it generated a series of random numbers that are different in a very short time. The seven best features that were selected by GA from each user were quite adequate for authenticating the user's identity. Furthermore, the proposed model was an excellent fingerprint recognition based on intelligent algorithms as it offered a higher CVR of 99.334%, and lowered FAR and FRR of 0.00 and 0.00666, respectively. It means that the performance of the proposed model was better than previous versions, which revealed that the proposed fingerprint recognition despite the better CVR rate than comparable algorithms. In addition, it also showed the best execution time because each stage elapsed a minimum time.

Acknowledgment

The authors would like to thank the volunteer students of the Technical College of Informatics and Institute of Computer Science at Sulaimani city, Iraq, for their unconditional participation in giving their fingerprint images during data collection.

Declarations

Author contribution. All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.
Funding statement. This work has not achieved any fund.
Conflict of interest. The authors declare no conflict of interest.
Additional information. No additional information is available for this paper.

References

[1] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," 2019, doi: 10.3390/sym11020141.

[2] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User authentication on mobile devices: Approaches, threats and trends," *Comput. Networks*, vol. 170, pp. 107-118, 2020, doi: 10.1016/j.comnet.2020.107118.

[3] F. Belhadj, "Biometric system for identification and authentication," National High School of Computer Science (ESI), 2017, available at: Google Scholar.

[4] S. S. Harakannanavar, P. C. Renukamurthy, and K. B. Raja, "Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends," *Int. J. Adv. Netw. Appl.*, vol. 10, no. 4, pp. 3958–3968, 2019, doi: 10.35444/IJANA.2019.10048.

[5] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Secur.*, vol. 2011, no. 1, p. 3, Dec. 2011, doi: 10.1186/1687-417X-2011-3.

[6] M. M. H. Ali, V. H. Mahale, P. Yannawar, and A. T. Gaikwad, "Overview of fingerprint recognition system," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 2016, pp. 1334–1338, doi: 10.1109/ICEEOT.2016.7754900.

[7] E. Chandra and K. Kanagalakshmi, "Noise Elimination in Fingerprint Image Using Median Filter," *Int. J. Adv. Netw. Appl.*, 2011, available at: Google Scholar.

[8] M. Hammad, Y. Liu, and K. Wang, "Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2018.2886573.

[9] S. Sahoo, T. Choubisa, and S. Mahadeva Prasanna, "Multimodal Biometric Person Authentication : A Review," *IETE Tech. Rev.*, vol. 29, no. 1, pp. 54-75, 2012, doi: 10.4103/0256-4602.93139.

[10] I. Fister, X. S. Yang, J. Brest, and D. Fister, "A brief review of nature-inspired algorithms for optimization," *Elektrotehniski Vestnik/Electrotechnical Review*, vol. 80, no. 3, pp. 1-7, 2013, available at: Google Scholar.

[11] S. Kumar, D. Datta, and S. K. Singh, "Swarm Intelligence for Biometric Feature Optimization," pp. 830–863, doi: 10.4018/978-1-5225-0788-8.ch032.

[12] M. Mavrovouniotis, C. Li, and S. Yang, "A survey of swarm intelligence for dynamic optimization: Algorithms and applications," *Swarm Evol. Comput.*, vol. 33, pp. 1–17, Apr. 2017, doi: 10.1016/j.swevo.2016.12.005.

[13] I. G. Dakhil and A. A. Ibrahim, "Design and Implementation of Fingerprint Identification System Based on KNN Neural Network," *J. Comput. Commun.*, vol. 06, no. 03, pp. 1–18, 2018, doi: 10.4236/jcc.2018.63001.

[14] A. K. Oo and Z. L. Aung, "A Robust Fingerprint Recognition Technique Applying Minutiae Extractors and Neural Network," *Int. J. Eng. Res. Adv. Technol.*, vol. 5, no. 3, pp. 78–87, 2019, doi: 10.31695/IJERAT.2019.3402.

[15] H. Kaur, G. Kaur, and H. S. Pannu, "Novel similarity measure-based random forest for fingerprint recognition using dual-tree complex wavelet transform and ring projection," *Mod. Phys. Lett. B*, vol. 34, no. 02, p. 2050022, Jan. 2020, doi: 10.1142/S0217984920500220.

[16] T. Logeswari and M. Duraisamy, "An exploration of sturdiness of ant colony optimization technique on brain tumor image segmentation," *Int. J. Appl. Eng. Res.*, vol. 10, no. 2, pp. 4329-4342, 2015, available at: Google Scholar.

[17] A. Sindhu and V. Radha, "A Novel Histogram Equalization Based Adaptive Center Weighted Median Filter for De-noising Positron Emission Tomography (PET) Scan Images," in *2018 3rd International Conference on Communication and Electronics Systems (ICCES)*, 2018, pp. 909–914, doi: 10.1109/CESYS.2018.8724108.

[18] S. Mohammad-Azari, O. Bozorg-Haddad, and X. Chu, "Shark Smell Optimization (SSO) Algorithm," in *Advanced Optimization by Nature-Inspired Algorithms: Springer*, 2018, pp. 93–103, doi: 10.1007/978-981-10-5221-7_10.

[19] M. Ehteram, H. Karami, S.-F. Mousavi, A. El-Shafie, and Z. Amini, "Optimizing dam and reservoirs operation based model utilizing shark algorithm approach," *Knowledge-Based Syst.*, vol. 122, pp. 26–38, Apr. 2017, doi: 10.1016/j.knosys.2017.01.026.

[20] 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 (NigeriaComputConf)*, 2019, pp. 1–10, doi: 10.1109/NigeriaComputConf45974.2019.8949671.

[21] H. Hosseinzadeh and M. Sedaghat, "Brain image clustering by wavelet energy and CBSSO optimization algorithm," *J. Mind Med. Sci.*, vol. 6, no. 1, pp. 110–120, Apr. 2019, doi: 10.22543/7674.61.P110120.

[22] N. Gnanasekaran, S. Chandramohan, P. S. Kumar, and A. Mohamed Imran, "Optimal placement of capacitors in radial distribution system using shark smell optimization algorithm," *Ain Shams Eng. J.*, vol. 7, no. 2, pp. 907–916, Jun. 2016, doi: 10.1016/j.asej.2016.01.006.

[23] 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, doi: 10.1002/cplx.21634.

[24] H. Hosseinzadeh, "Automated skin lesion division utilizing Gabor filters based on shark smell optimizing method," *Evol. Syst.*, pp. 1-10, Nov. 2018, doi: 10.1007/s12530-018-9258-4.

[25] S. A. L. I. Juma, "Optimal Radial Distribution Network Reconfiguration Using Modified Shark Smell Optimization," MSc. Thesis, Pan African University Institute for Basic Sciences, Technology and Innovation, 2018, available at: Google Scholar.

[26] A. Goswami, G. Choudhury, and H. K. Sarmah, "Contributions of Russian Mathematicians in the Development of Probability: A Historical Search," *Int. J. Stat. Syst.*, vol. 14, no. 1, pp. 1–27, 2019, available at: Google Scholar.

[27] M. Filippi, A. Pagani, M. Petrolo, G. Colonna, and E. Carrera, "Static and free vibration analysis of laminated beams by refined theory based on Chebyshev polynomials," *Compos. Struct.*, vol. 132, pp. 1248–1259, Nov. 2015, doi: 10.1016/j.compstruct.2015.07.014.

[28] N. Karjanto, "Properties of Chebyshev polynomials," *arXiv Prepr. arXiv2002.01342*, pp. 127-132, 2020, available at: Google Scholar.

[29] R. A. Welikala *et al.*, "Genetic algorithm based feature selection combined with dual classification for the automated detection of proliferative diabetic retinopathy," *Comput. Med. Imaging Graph.*, vol. 43, pp. 64–77, Jul. 2015, doi: 10.1016/j.compmedimag.2015.03.003.

[30] S. Mirjalili, "Genetic Algorithm," in *Evolutionary algorithms and neural networks: Springer,* 2019, pp. 43–55, doi: 10.1007/978-3-319-93025-1_4.

[31] H. Heidari and A. Chalechale, "A new biometric identity recognition system based on a combination of superior features in finger knuckle print images," *TURKISH J. Electr. Eng. Comput. Sci.*, vol. 28, no. 1, pp. 238–252, Jan. 2020, doi: 10.3906/elk-1906-12.

[32] P. Kaur and J. Kaur, "Finger print Recognition Using Genetic Algorithm and Neural Network," *Int. J. Comput. Eng. Res.*, vol. 3, no. 11, pp. 41–46, 2013, available at: Google Scholar.

[33] M. Demri, "Multimodal biometric fusion using evolutionary techniques," 2012, available at: Google Scholar.

[34] K. Martin Sagayam, D. Narain Ponraj, J. Winston, J. C. Yaspy, D. Esther Jeba, and A. Clara, "Authentication of biometric system using fingerprint recognition with euclidean distance and neural network classifier," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 4, pp. 766-771, 2019, available at: Google Scholar.

[35] T. Wala Aldeen Khairi, "Secure Mobile Learning System using Voice Authentication," *J. Eng. Appl. Sci.*, vol. 14, no. 22, pp. 8180–8186, Oct. 2019, doi: 10.36478/jeasci.2019.8180.8186.

[36] M. M. H. Ali, V. H. Mahale, P. Yannawar, and A. T. Gaikwad, "Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching," in *2016 IEEE 6th International Conference on Advanced Computing (IACC)*, 2016, pp. 332–339, doi: 10.1109/IACC.2016.69.