AVAO Enabled Deep Learning Based Person Authentication Using Fingerprint

Rasika Deshmukh[1] and Pravin Yannawar[2](✉)

[1] Department of Computer Science, Fergusson College (Autonomous), Pune, India
[2] Department of Computer Science, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, India
plyannawar.csit@bamu.ac.in

Abstract. Person authentication based on biometrics has been a major aspect accountable for providing security to cyberspace. The traditional biometric-based systems are based on the usage of single modality, which are potentially devoid of the capability to provide high security. A Deep Maxout Network (DMN) is utilized for performing person authentication on the basis of fingerprint. A novel optimization algorithm, named African vultures-Aquila Optimization (AVAO) algorithm is devised for updating the weights of the DMN. The strategies of the African Vulture Optimization Algorithm (AVOA) are modified according to the expanded exploration capability of the Aquila Optimizer (AO) to develop the proposed AVAO algorithm. The introduced optimization enabled deep learning based person authentication system achieved an accuracy of 0.927, sensitivity of 0.938 and specificity of 0.930,thereby showing superior performance.

Keywords: Person authentication · fingerprint · Deep Maxout Network · AVOA · AO

1 Introduction

Over the last few decades, a digital society has been developed around the globe in which the process of authentication is being made by considering each individual as a distinctive identifier. Authentication can be defined as, "Authentication is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity". Person authentication refers to the procedure of verifying an individual's identity and is highly vital for every individual in this current information world. With the tremendous increase in the number of digital devices, there is a growing concern on the security. Every system or organization requires one type of authentication or other to provide security. The conventional authentication schemes are being replaced rapidly owing to their high vulnerability as these techniques employ PINs, identity cards, passwords, security tokens, etc., which can be easily manipulated, forgotten, copied, stolen or forged. In the past years, there is growing trend in the usage of the biometric-based authentication techniques that use the biometrics or the physical traits of an individual for authentication [1, 2]. Biometrics based approaches can be classified as behavioural as well

R. Manza et al. (Eds.): ACVAIT 2022, AISR 176, pp. 327–346, 2023.
https://doi.org/10.2991/978-94-6463-196-8_26

as physiological, where the behavioral biometrics are based on the unique behaviour of humans, such as signature, keystroke and voice. The physiological biometrics deals with the distinctive physical traits, such as iris, face, or fingerprint. These biometrics are highly unique, unforgettable and non transferable, moreover they are highly difficult to be manipulated, or stolen.

The authentication system which has been hogging the lime light for a long time is those that are based on the hand are highly efficient in recognizing the veins, hand form, hand geometry, palm prints, and fingerprints. These systems are highly successful owing to their robustness, simplicity, acceptance and stability. These systems are being employed by a vast number of government agencies, industries and corporations for providing security, attendance resisters and other purposes [3]. Among the hand based schemes, the fingerprint authentication system is the most extensively utilised system because of its high accuracy and acceptability. Also, the inexpensive and compact nature of the fingerprint scanners has resulted in a tremendous growth in multiple applications [4]. Fingerprint matching is one of the most promising biometric recognition techniques, and it has long been utilised for person authentication [5]. In this paper, fingerprint is pre-processed and then the minutiae are detected from the processed fingerprint. The output obtained is then fed to the DMN, which is tuned by using the proposed AVAO algorithm.

The main contributions of this paper are as follows.

- A **person authentication scheme** is devised for generating the encodings of the fingerprint image.
- A novel **AVAO algorithm** is developed for modifying the weights of the hidden neurons in the DMN. The AVAO algorithm is devised by modifying the AVOA with respect to the AO for enhancing the performance of the classifier.

The rest of the paper is organized in the following structure: Section 2 reviews the literature on the various authentic systems and Sect. 3 elaborates the proposed method along with the AVAO algorithm. Section 4 discusses the experimental outcomes**.**

2 Motivation

Authentication systems have emerged as a highly critical aspect needed for providing security and privacy to the current digitally interconnected society. Even though there is a growing trend in the usage of biometrics, there exits various attacks that can hamper the security of the system. In this section, the existing techniques of authentication are elaborated with their advantages and their demerits, which formed a major inspiration in the development of an effective authentication technique.

2.1 Literature Review

A large number of researches have been conducted on the development of the authentication schemes using different modalities.

Table 1. Literature Review

Author	Trait	Dataset	Classification Technique	Fusion Level	Average Accuracy
Bouzouina and Hamami, 2017 [6]	Face, Iris	CASIA-IrisV3-Interval iris dataset and ORL face dataset	SVM	Feature level	98.8%
Hezil and Boukrouche, 2017 [7]	Ear, Palmprint	IIT Delhi-2 ear and IIT Delhi palmprint	K-NN, SVM, CRC_RLS.	Feature Level	80.53–100%
Chaudhary and Nath, 2016 [8]	Face, Iris, Fingerprint	CASIA iris dataset, NIST face and fingerprint dataset	SVM	Score Level	99.8%
Veluchamy and Karlmarx, 2017 [9]	Finger knuckle, Finger vein	IIT Delhi finger knuckle dataset and SDUMLAHMT finger vein dataset	SVM	Feature Level	96%
Al-Waisy et al., 2017 [10]	Pair of irises, Face	NIST, CASIA V1.0, MMU1 and SDUMLA-HMT	DBN, CNN	Score/ Rank level	99.91%–100%
Mouad.M.H.Ali et al., [11]	Fingerprint	FVC2000	minutiae matching algorithm	Feature Level	98.55%

3 Introduced Avao Enabled Deep Learning Based Person Authentication Technique

In this paper, fingerprint images are utilized to enhance the efficiency of the authentication system along with providing privacy and security. Figure 1 illustrates the schematic representation of the introduced person.

Authentication technique. Fingerprint authentication module comprises of data acquisition, pre-processing, minutiae detection and person authentication.

These processes are detailed in the following subsections.

3.1 Fingerprint Authentication Module

This section deals with the process of authentication of the fingerprint image. Fingerprint images are most commonly utilized in the process of identification owing to their singularity and invariance. They are extensively utilized as they possess numerous advantages, such as high accuracy, fast and easy operation. In order to make the fingerprint image suitable for authentication, a sequence of operations has to be executed, which are detailed below along with the authentication process.

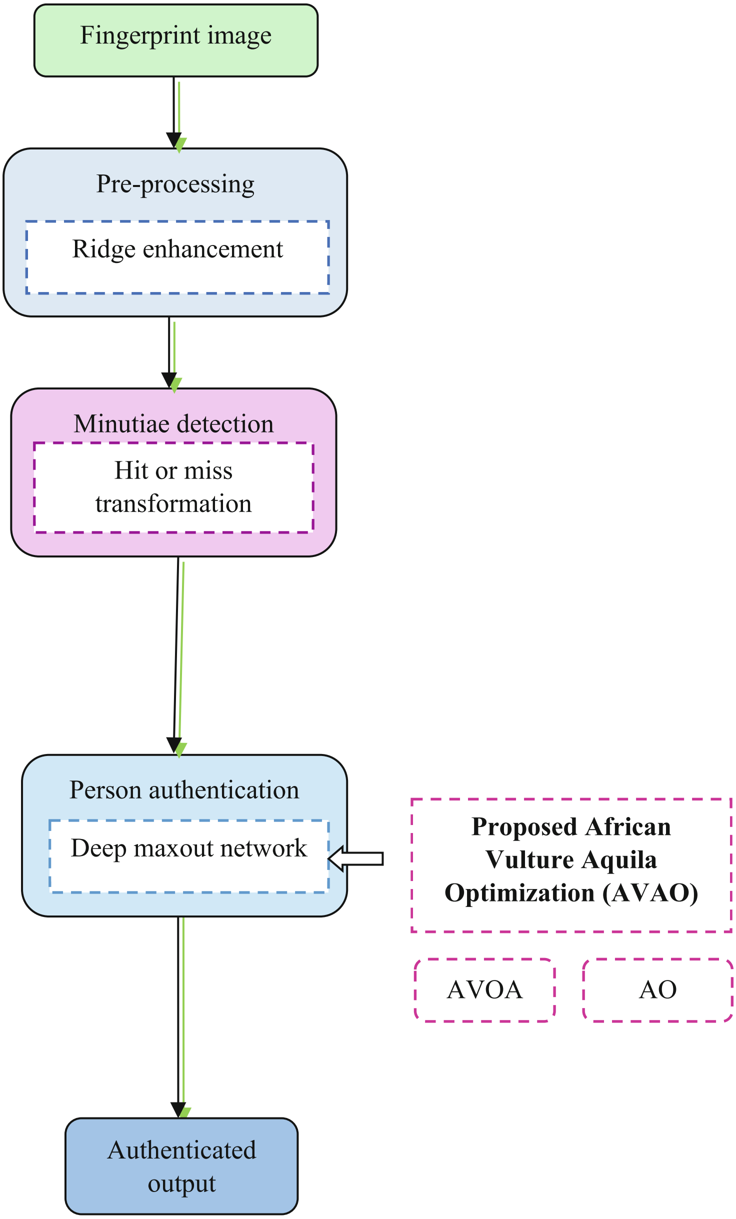


Fig. 1. Schematic representation of the introduced AVAO enabled deep learning based person authentication using fingerprint.

3.1.1 Fingerprint Image Acquisition

Consider a dataset *Fp* containing n_f fingerprint images and is represented by,

$$Fp = \left\{fp_1, fp_2, ..., fp_i, ..fp_{n_f}\right\} \tag{1}$$

where, fp_i denotes the i^{th} fingerprint image that will be fed to the preprocessing phase.

3.1.2 Fingerprint Image Pre-processing

The fingerprint image fp_i acquired from the database is subjected to pre-processing. The image acquisition modality has a high impact on the quality of the fingerprint image acquired. If the contrast between the background and the foreground is very poor, it affects the identification process. These noises and artifacts have to be eliminated to enhance the efficiency of identification, which is accomplished by means of pre-processing. Here, a ridge enhancement technique is utilized in pre-processing for obtaining the ridges. Ridge enhancement is highly efficient in smoothing the image without the need of any prior information. A set of processes are used to obtain an enhanced quality image from the poor quality input. The image quality is enhanced by enlarging the objects in the fingerprint image with the help of dilation, where the objects' interior and exterior boundary pixels are added with extra pixels. The ridge enhanced fingerprint image can be obtained by using the following expression.

$$Rid_i = fp_i \oplus l \tag{2}$$

where, l denotes the structuring element. The output obtained Rid_i is fed to the minutiae detection phase.

3.1.3 Minutiae Detection

The ridge enhanced image $Ridge_i$ is forwarded to the minutiae detection phase, where minutia points present in the ridge enhanced images are identified. Minutia refers to the points in the fingerprint, where the ridge lines bifurcate or end. Here, a Gray-scale Hit-Or-Miss Transformation (GHMT) is utilized. The GHMT offers the advantage of utilizing the foreground and the background information to identify the minutia and also it is flexible. GHMT technique is developed by inclusion of gray-scale erosion in the binary HMT technique, so as to make it suitable for gray-scale images. Moreover, template matching concept is utilized to modify the GHMT, whose expression can be represented by,

$$R_i \otimes (l_f, l_b) = \left[\min_{a_1 \in l_f}{}^2 (R_i + a_1)\right] - \left[\max_{a_2 \in l_b}{}^2 (R_i - a_2)\right] \tag{3}$$

Here, R_i specifies the gray-scale image, l_f denote the foreground structuring element and l_b is the background in which l_f is present. $\min^2$ and $\max^2$ denote the second minimum as well as the maximum values of the gray-level substitution of binary erosion and dilation operation.

GHMT utilizes sixteen templates, which are oriented and pre-defined for identifying the minutiae. The bifurcations of the ridges in the fingerprint are contained in the templates, which comprises of ridge line that has the background set and the valleys representing the foreground portion. These templates are efficient in detecting the bifurcations alone and do not detect the end point. The end points are identified by considering the inverted images, which is obtained by the following expression,

$$A^{\wedge}(x, y) = Pix_m - A(x, y) \tag{4}$$

Here, Pix_m represents the maximum value of pixel intensity in the original image. The pixel intensity of the original and the inverted images at (x, y) is represented by $A(x, y)$ and $A^{\wedge}(x, y)$.

The minutiae are identified by performing GHMT on both the inverted and the original image using Eq. (3) pixelwise. A total of sixteen filtered outputs are obtained for each of the original as well as the inverted images for each template. This can be expressed by,

$$B^j_{org} = Rid_i \otimes \left(l_f^{\theta_j}, l_b^{\theta_j}\right) \; where\ j \in \{1, 2, ..., 16\} \tag{5}$$

$$B^j_{inv} = Ridinv_i \otimes \left(l_f^{\theta_j}, l_b^{\theta_j}\right) \; where\ j \in \{1, 2, ..., 16\} \tag{6}$$

where, $Ridinv_i$ denotes the inverted ridge enhanced image, B^j_{org} and B^j_{inv} are the outputs obtained from the filtering of the original as well as inverted images and θ^j signifies the orientation of the templates or the structuring elements.

The minutia points are identified by finding the maximum values of the pixel among the outputs obtained from filtering and the pixel value higher than the threshold is selected as the minutiae, which can be represented as,

$$MP = MP \cup \{(x, y)\} \; if \max_{1 \le j \le 16} \left[B^j_{ori/inv}(x, y) > thresh\right] \tag{7}$$

Here, $B^j_{ori/inv}(x, y)$ gives the pixel intensity at (x, y) of the j^{th} output of the filtered original or inverted image, MP signifies the minutia points and $thresh$ denotes the threshold value. The minutia points MP are subjected to the DMN for person authentication.

3.1.4 Person Authentication with DMN

The DMN [12] is utilized in the process of fingerprint image matching, where the DMN utilizes the minutiae points MP detected in the previous step for performing authentication. This section details the structure of DMN and the introduced AVAO algorithm, which is employed for adjusting the weights of the DMN.

3.1.4.1 DMN

DMN is employed in the authentication process as they produce superior performance in resource constrained environments. A DMN comprises of numerous maxout layers which are connected successively, where the maxout layers contains hidden units which are partitioned into groups, which do not overlap each other. Each layer uses the maxout function to generate hidden activations and the activation functions generated are trainable. The minutia points are fed as the input to the DMN whose activation functions can be given by,

$$c_{s,t}^{1} = \max_{t\in[1,h_1]} MP^{T} k_{\ldots st} + d_{st} \tag{8}$$

$$c_{s,t}^{2} = \max_{t\in[1,h_2]} \left(c_{s,t}^{1}\right)^{T} k_{\ldots st} + d_{st} \tag{9}$$

$$\vdots$$

$$c_{s,t}^{e} = \max_{t\in[1,h_e]} \left(c_{s,t}^{e-1}\right)^{T} k_{\ldots st} + d_{st} \tag{10}$$

$$\vdots$$

$$c_{s,t}^{f} = \max_{t\in\left[1,h_f\right]} \left(c_{s,t}^{f-1}\right)^{T} k_{\ldots st} + d_{st} \tag{11}$$

$$b_s = \max_{t\in\left[1,h_f\right]} c_{s,t}^{f} \tag{12}$$

where, h_e denotes the number of hidden units in the e^{th} layer, $k_{\ldots st}$ and d_{st} signifies the weight and the bias of the layer. Morover,f represents the total number of layers in DMN and b_s denote the output of the maxout layer. From the above equations, it can be inferred that a max pooling function is applied and hence the maximum value obtained in each layer is fed to the successive ones. The activation used in the DMN has a high potential and can be used in approximating any random continuous activation function. When the number of hidden units is kept greater than 2, the DMN can efficiently approximate non linear functions too. The structure of DMN is depicted using Fig. 2.

3.1.4.2 Proposed AVAO Algorithm for tTaining DMN

A novel AVAO algorithm is introduced in this paper, which is used in the process of updating the weights of the hidden neurons in the DMN. The introduced AVAO algorithm is created by modifying the strategies of the AVOA [13] with respect to the expanded exploration capability of the AO [14]. The AVOA is a population based algorithm which is inspired by the navigation, foraging behaviors and the lifestyle of African vultures. AVOA is implemented in four steps, such as determination of the best vulture, determination of the starvation rate, exploration and exploitation. AVOA aims at finding the best solution and the second best solution to any complex problems. The algorithm has high flexibility and very low computational complexity. Moreover, the algorithm effectively balances variability as well as resonance. The AO algorithm is developed considering the predatory behaviour of Aquila and is implemented in four phases, such as expanded exploration, narrowed exploration, expanded exploitation and narrowed exploitation. The AO algorithm has a fast convergence rate and can effectively tackle

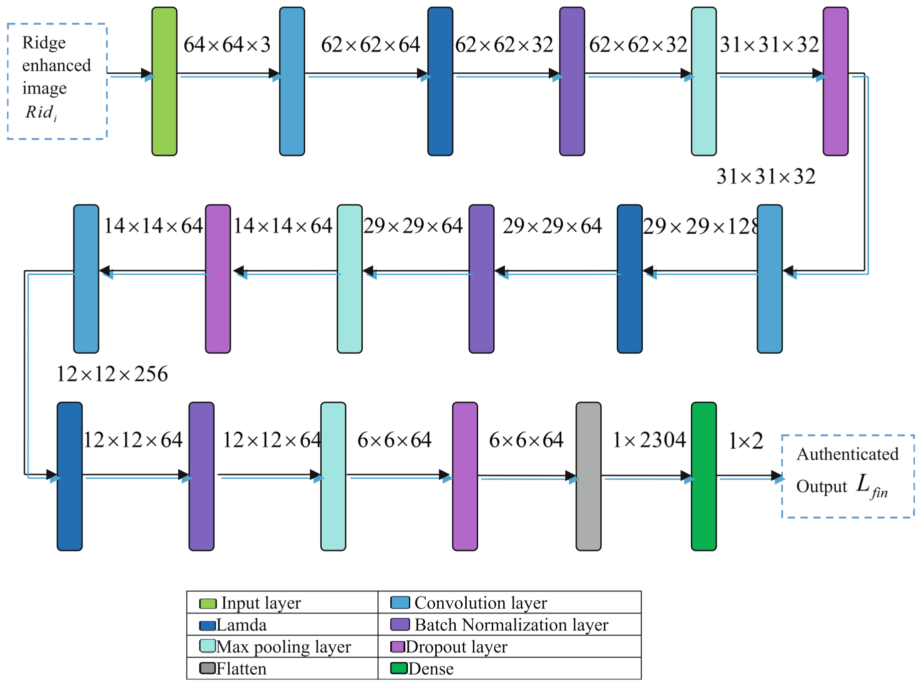


Fig. 2. Structure of DMN

real time applications. The following subsections details the various steps in the proposed AVAO algorithm.

i) ***initialization***

Let us assume there are *av* number of vultures. The first step is to initialise the population of vultures in the problem space and can be represented by,

$$V = \{V_1, V_2, ...V_i, ...V_{av}\} \tag{13}$$

where, V_i represents the i^{th} vulture in the population.

ii) ***Determine the best vulture***

Once the population is initialised, the best vulture is determined by considering the fitness of all the vultures. The value of fitness is calculated using the following equation.

$$\varepsilon = \frac{1}{n}\sum_{o=1}^{n}\left[U_o - U_o^*\right]^2 \tag{14}$$

Here, U_o represents the target output, U_o^* defines the output of the DMN and n designates the overall sample count.

After the fitness is computed, the best vulture of the first group is selected from the group with the best solution and the one with the second best value of fitness is considered the second group‘s best vulture. The best vultures are determined for every fitness iteration.

$$W(i) = \begin{cases} BestVulture_1, & if \;\; J_i = K_1 \\ BestVulture_2, & if \;\; J_i = K_2 \end{cases} \tag{15}$$

Here, K_1 and K_2 are factors that have to be calculated ahead of the search operation and has a value in the range [0,1] and the factors to be computed before the search mechanism with the measures between 0 and 1. The term J_i represents the probability of selecting the best vulture and is calculated using the roulette wheel.

iii) ***Determination of starvation rate of vultures***

Vultures normally fly to long distances in search of food when they are full and as a result they have high energy. But in case if they are hungry, they feel shortage of energy of exploring long distances and they become aggressive and seek the food near the powerful vulture. Thus, the rate at which the vulture is starving determines the exploration and exploitation phases and it can be mathematically modelled by using the following equations. The satiated vulture is given by,

$$SR = (2 \times rd_1 + 1) \times w \times \left(1 - \frac{itr_i}{maxitr}\right) + C \tag{16}$$

$$C = D \times \left(\mathrm{Sin}^{\beta}\left(\frac{\pi}{2} \times \frac{itr_i}{maxitr}\right) + \mathrm{Cos}\left(\frac{\pi}{2} \times \frac{itr_i}{maxitr}\right) - 1\right) \tag{17}$$

where, *itr* and *maxitr* denote the present iteration count and the overall count of iterations. w, rd_1 and D are arbitrary numbers in the range [0, 1], [−1, 1] and [−2, 2] respectively. Further, β is a parameter, whose value is fixed before the searching process and the probability of exploration enhances with the value of value β. The vultures hunt for food in varied spaces and the algorithm is in exploration phase, if the value of $|SRate| > 1$, otherwise the exploitation phase is encountered.

iv) ***Exploration phase***

Vultures have superior eyesight and possess high capability in identifying weak animals, while hunting for food. But, searching food is highly challenging and the vultures have to perform careful scrutiny of their surroundings for a long period over vast distances. Random areas are examined by the usage of two approaches. An arbitrary parameter I_1, which has a value in the range [0,1]is utilised to select the approaches. The strategies are selected based on the following equations.

$$R(i + 1) = W(i) - T(i) \times SR \; if \;\; I_1 \geq rd_I \tag{18}$$

$$R(i + 1) = W(i) - SR + rd_2 \times ((upb - lwb) \times rd_3 + lwb) \; if \;\; I_1 < rd_I \tag{19}$$

$$T(i) = |Z \times W(i) - R(i)| \tag{20}$$

Here, $R(i+1)$ denotes the vulture position vector, Z represents the coefficient vector. rd_I, rd_2 and rd_3 are random variable in the range [0, 1]. *upb* and *lwb* denote the lower as well as the upper limits of the variable.

Substituting Eq. (20) in Eq. (18),

$$R(i+1) = W(i) - |Z \times W(i) - R(i)| \times SR\ W(i) > R(i) \tag{21}$$

$$R(i+1) = W(i) - (Z \times W(i) - R(i)) \times SR \tag{22}$$

$$R(i+1) = W(i)[1 + Z \times SR] - R(i) \times SR \tag{23}$$

In the AO algorithm, Aquila identifies the position of the prey by exploring by soaring up and then determining the search area. The expanded exploration ability of the Aquila can be given by,

$$H_1(n+1) = H_{best}(n) \times \left(1 - \frac{n}{N}\right) + (H_r(n) - H_{best}(n) * rnd) \tag{24}$$

$$H_r(n) = \frac{1}{T}\sum_{i=1}^{T} H_i(n) \tag{25}$$

Where,

Assume, $T = 1$.

$$H_1(n+1) = H_{best}(n) \times \left(1 - \frac{n}{N} - rnd\right) + H(n) \tag{26}$$

$$H_1(n+1) = R(i+1). \tag{27}$$

Consider,

$$H(n) = R(i) \tag{28}$$

$$H_{best}(n) = W(i) \tag{29}$$

Substituting Eqs. (27), (28) and (29) in Eq. (26),

$$R(i+1) = W(i) \times \left(1 - \frac{n}{N} - rnd\right) + R(i) \tag{30}$$

$$R(i) = R(i+1) - W(i) \times \left(1 - \frac{n}{N} - rnd\right) \tag{31}$$

Substituting Eq. (31) in Eq. (23),

$$R(i+1) = W(i)[1 + Z \times SR] - R(i+1) \times SR + W(i) \times \left(1 - \tfrac{n}{N} - rnd\right) \times SR \tag{32}$$

$$R(i+1)+R(i+1)\times SR=W(i)\big[1+Z\times SR+\big(1-\tfrac{n}{N}-rnd\big)\times SR\big] \tag{33}$$

$$R(i+1)[1+SR]=W(i)\big[1+\big(Z+\big(1-\tfrac{n}{N}\big)-rnd\big)\times SR\big] \tag{34}$$

$$R(i+1)=\frac{W(i)\big[1+(Z+(1-\frac{n}{N})-rnd)\times SR\big]}{[1+SR]} \tag{35}$$

Here, N denotes the number of samples.

v) ***Exploitation: phase 1***

Exploitation is performed in two phases depending on the value of SR. If the value of $|SR|$ lies between 0.5 and 1, then phase 1 is executed. The first phase comprises of two techniques, such as rotating flight as well as siege-fight. A parameter I_2 is utilised in selecting the strategies, which has to be computed ahead of searching. The parameter is compared to a random variable rd_{I_2} to select the strategies. If $I_2 < rd_{I_2}$, then rotating flight approach is implemented, else siege flight approach is performed.

a) **Contest for food**

The vultures are full and have high energy, if $|SR| \geq 0.5$. When vultures accumulate on a single food source, brutal disputes can occur. The highly powerful vultures wouldn't share the food with the weak vultures, whereas the weak vultures attempt to exhaust the strong vultures by assembling around them and snatching the food leading to conflicts.

$$R(i+1)=P(i)\times(SR+rnd_4)-E(t) \tag{36}$$

$$E(t)=H(i)-W(i) \tag{37}$$

Here, rnd_4 is an arbitrary number in the range [0, 1].

b) **Rotating flight of Vultures**

A rotational flight is made by the vultures for modelling the spiral movement and a spiral motion is formed among the best two vultures and the other vultures and this can be modelled as,

$$P(i+1)=W(i)-(X_1+X_2) \tag{38}$$

$$X_1=W(i)\times\left(\frac{rnd_5\times R(i)}{2\pi}\right)\times \text{Cos}\,(R(i)) \tag{39}$$

$$X_2=W(i)\times\left(\frac{rnd_6\times R(i)}{2\pi}\right)\times \text{Sin}\,(R(i)) \tag{40}$$

where, rnd_5 and rnd_6 are arbitrary numbers in the range [0, 1].

vi) ***Exploitation: phase 2***

In the second phase, the food source is determined by using the siege and aggressive strife strategy, where, the other vultures aggregate over the food source following the motion of the best vultures. This phase is executed when $|SR| < 0.5$. A parameter I_3 is utilised in selecting the strategies, which has to be computed ahead of searching. The parameter is compared to a random variable rd_{I_3} to select the strategies. If $I_2 < rd_{I_2}$, then the cultures are accumulated over the food source, otherwise aggressive siege-flight strategy is performed.

(i) ***Accumulation of vultures over food source***

Here, close examination of the motion of all vultures to the source of food is carried out. When the vultures are hungry, they compete with each other over the food source. This can be represented as,

$$O_1 = BestV_1(i) - \frac{BestV_1(i) \times R(i)}{BestV_1(i) - R(i)^2} \times SR \tag{41}$$

$$O_2 = BestV_2(i) - \frac{BestV_2(i) \times R(i)}{BestV_2(i) - R(i)^2} \times SR \tag{42}$$

Here, $BestV_1(i)$ and $BestV_2(i)$ denote the best vultures of the first group and second group. The position of the vulture in the next iteration is given by.

$$R(i+1) = \frac{O_1 + O_2}{2} \tag{43}$$

(ii) ***Aggressive conflicting for food***

The chief vulture becomes famished, when $|SR| < 0.5$, and it becomes too fragile to compete with other vultures, which turn aggressive and move in multiple directions and head to the group head in their search for food. This is modelled as,

$$R(i+1) = W(i) - |E(t)| \times SR \times Levy(E) \tag{44}$$

Here, $E(t)$ specifies the distance between a vulture and anyone of the best vultures.

Step 8: Termination

The above steps are kept reiterated till a best solution is achieved. Algorithm 1 depicts the pseudo code of introduced AVAO algorithm.

Pseudo code of devised AVAO algorithm

```
Initialize the arbitrary population and number of iterations
While (stopping criteria is not attained) do
    Calculate fitness function with Equation (14)
    Consider $R_{BestV_1}$ as the position of first best vulture
    Consider $R_{BestV_2}$ as the position of second best vulture
        for (each vulture $(V_i)$) do
            Select $W(i)$ using Equation (15)
            Update $SR$ using Equation (16)
            if $(|SR| \ge 1)$ then
                if $(I_1 \ge rd_1)$ then
                    Update the position of vulture using Equation (18)
                else
                    Update the position of vulture using Equation (19)
            if $(|SR| < 1)$ then
                if $(|SR| \ge 0.5)$ then
                    if $(I_2 \ge rnd_{I_2})$ then
                        Update the position of vulture using Equation (36)
                    Else
                        Update the position of vulture using Equation (38)
                Else
                    if $(I_3 \ge rnd_{I_3})$ then
                        Update the position of vulture using Equation (43)
                    Else
                        Renew the location of vulture using Equation (44)
    Return $P_{BestV_1}$
Terminate
```

The output obtained from the DMN while using the fingerprint image is denoted as L_{fin}.

4 Results and Discussion

The experimental outcomes of the devised AVAO enabled Deep learning based person authentication are elaborated in this section together with the detailed analysis of the devised method.

4.1 Experimental Set up

The innovative AVAO enabled Deep learning approach for the efficient authentication of individual utilising fingerprint is implemented in Python platform on a system with the following specifications: Windows 10 PC, 2GB RAM and Intel i3 core processor.

4.2 Dataset Description

The fingerprint images are collected from the CASIA Fingerprint Image Database Version 5.0 [15]. The database comprises of images acquired from 500 individuals. Eight fingers were considered and a total of 40 images were taken from each individual, thus the database has 20,000 fingerprint images, which are stored as 8-bit gray-level BMP files. These images were taken with the help of URU4000 fingerprint sensors and have a resolution of 328*356.

4.3 Performance Measures

With the usage of the efficiency measures, such as like the accuracy, sensitivity and specificity, the effectiveness of the proposed AVAO enabled Deep learning approach is evaluated. The parameters are detailed in the ensuing subsections.

4.3.1 Accuracy

Accuracy can be defined as the ratio of the modalities successfully classified to the total number of modalities and is represented as,

$$Accuracy = \frac{tp + tn}{tp + tn + fp + fn} \tag{51}$$

where, *tp* indicate the number of genuine users who are authenticated correctly, *tn* specifies the number of illegal users classified as such, *fp* represent the number of non authorized users who are detected as authorized and *fn* signify the count of authorised users classified as non authentic.

4.3.2 Specificity

Specificity is also known as the True Negative Rate (TNR) and is the ratio of the true negatives to the count of the unauthorized users is expressed as,

$$Specificity = \frac{tn}{tn + fp} \tag{52}$$

4.3.3 Sensitivity

Sensitivity gives the measure of the positiveness of the system and is the ratio of the true positives to the total of the authorized users. It can be found by,

$$Sensitivity = \frac{tp}{tp + fn} \tag{53}$$

4.4 Experimental Outcomes

In this section, the experimental results of the introduced AVAO enabled deep learning based person authentication method are portrayed. Figure 3 a) depicts the input fingerprint images, 3 b) shows the pre-processed images, Fig. 3c) illustrates the minutiae detection.

The confusion matrix shows the classification of fingerprint dataset. The correctly classified samples percentage is 83.64% and 16.36% samples were misclassified for the population size 5. The performance of the proposed AVAO algorithm using the fingerprint image with different population sizes based on metrics, such as accuracy, specificity and sensitivity and F1-score is discussed in Sect. 4.6 (Fig. 4).

4.5 Comparative Algorithms

The performance of the devised AVAO algorithm in analysed in comparison to the other existing algorithms, such as Sine Cosine Algorithm (SCA) [16] + DMN, Sail Fish Optimization (SFO) [17] + DMN, AO + DMN, AVOA + DMN.

4.6 Algorithmic Analysis

The performance of the proposed AVAO algorithm using the fingerprint image with different population sizes based on metrics, such as accuracy, specificity and sensitivity and F1-score is as follows.

Figure 5 depicts the analysis of the various algorithms using fingerprint images. In Fig. 5 a), the algorithms are evaluate with respect to accuracy for varying population sizes. The existing algorithms, such as SCA + DMN, SFO + DMN, AO + DMN and AVOA + DMN attain an accuracy of 0.887, 0.892, 0.895 and 0.900, while the proposed AVAO + DMN algorithm attained an accuracy of 0.902, with a population size of 5. Thus, an improvement in performance of 1.67%, 1.09%, 0.70% and 0.23% is achieved. Figure 7b) depicts the evaluation while considering specificity. With a population size of 10, the developed AVAO + DMN algorithm calculates specificity of 0.918, but the prevailing SCA + DMN, SFO + DMN, AO + DMN and AVOA + DMN algorithms obtain specificity values at 0.898, 0.900, 0.900 and 0.905. This shows a performance improvement of 2.13%, 1.94%, 1.91% and 1.34% by the proposed algorithm over the existing algorithms. In Fig. 7c), the sensitivity-based analysis of the algorithms is depicted. The values of sensitivity achieved by the existing algorithms, namely SCA + DMN, SFO + DMN, AO + DMN and AVOA + DMN and the proposed AVAO + DMN algorithm is 0.906, 0.908, 0.912, 0.919 and 0.927 respectively for population size = 15. From this it

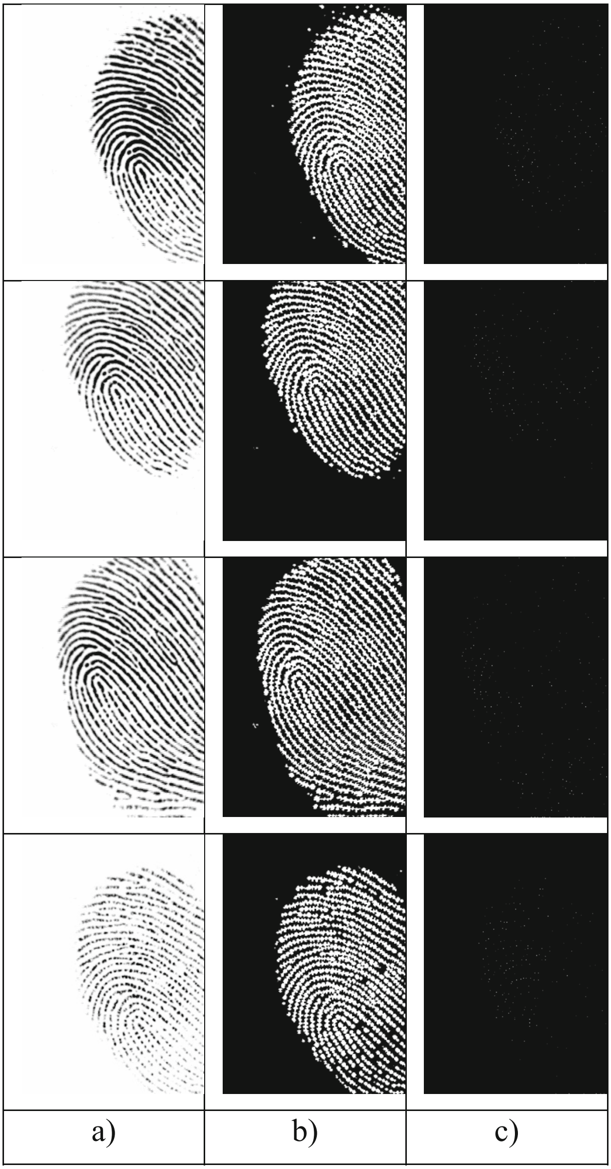


Fig. 3. Experimental results of the introduced AVAO enabled deep learning based person authentication a) input b) pre-processed c) minutiae detected images using fingerprint.

can be inferred that the proposed algorithm produced a higher value of sensitivity than the prevailing methods by 2.22%, 1.95%, 1.52% and 0.83%. Figure 5d) depicts the evaluation while considering F1-score. With a population size of 20, the developed AVAO + DMN algorithm calculates F1-score of 0.912, but the prevailing SCA + DMN, SFO + DMN, AO + DMN and AVOA + DMN algorithms obtain F1-score values at 0.893,

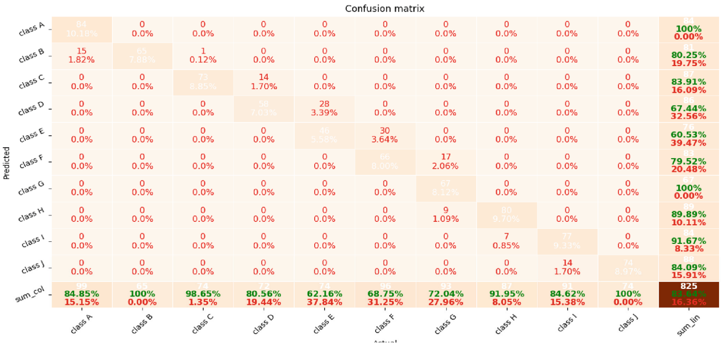
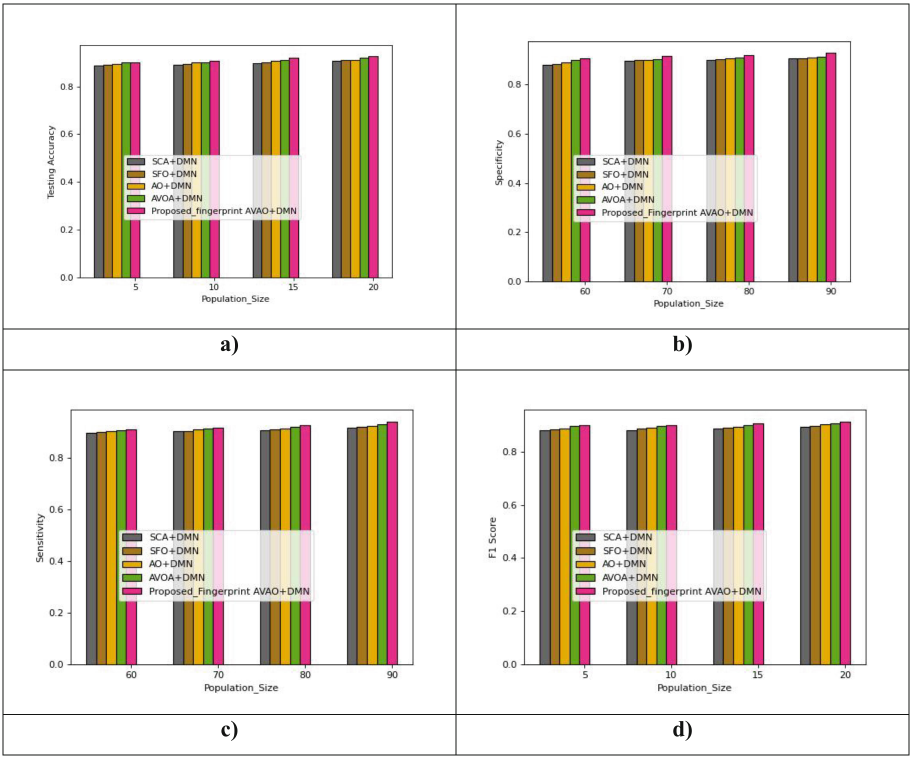


Fig. 4. Confusion Matrix for Fingerprint classification

0.898, 0.904, 0.907 respectively. This shows a performance improvement of 2.12%, 1.6%, 0.8% and 0.5% by the proposed algorithm over the existing algorithms.



a)

b)

c)

d)

Fig. 5. Algorithmic evaluation using fingerprint image based on a) accuracy b) specificity and c) sensitivity

Table 2. Comparative assessments of the algorithms

Modality	**Metrics**	**SCA + DMN**	**SFO + DMN**	**AO + DMN**	**AVOA + DMN**	**Proposed AVAO + DMN**
Fingerprint image	Accuracy	0.907	0.909	0.910	0.920	0.927
	Specificity	0.906	0.908	0.910	0.915	0.930
	Sensitivity	0.915	0.919	0.921	0.928	0.938
	F1-score	0.836	0.863	0.881	0.890	0.912

4.7 Comparative Discussion

This section deals with the comparison of the developed AVAO optimized person authentication scheme with the prevailing techniques on the basis of various metrics.

Table 1 displays the comparative discussion of the algorithms. The devised AVAO + DMN algorithm is with respect to accuracy, specificity and sensitivity by comparing it with the existing SCA + DMN, SFO + DMN, AO + DMN and AVOA + DMN algorithms. The values of the metrics correspond to the population size of 80 and from the table, the devised AVAO + DMN algorithm is shown to have attained the maximal value of accuracy at 0.927, sensitivity at 0.938,specificity at 0.930 and F1-score at 0.912 (Table 2).

5 Conclusion

In this paper, person authentication scheme is developed by exploiting simplicity of the fingerprint image. A DMN is utilized in authenticating the user based on the fingerprint images using supervised machine learning. The Fingerprint images are pre-processed first, after which the minutia points are identified. Then, person authentication is performed with the DMNs using the detected minutia points and features extracted. A novel AVAO algorithm is devised to generate the optimal weight factor of the DMN, where the AVAO is created by modifying the exploration ability of the African vulture in AVOA in accordance with that of the Aquila in AO. Experimental results show that the devised AVAO optimized deep learning based person authentication achieves a higher accuracy at 0.927, sensitivity at 0.938 and specificity at 0.930.

References

1. Zeynali M, Seyedarabi H., “EEG-based single-channel authentication systems with optimum electrode placement for different mental activities”, biomedical journal, vol.42, no.4, pp.261–7, August 2019.
2. Hammad, M., Pławiak, P., Wang, K. and Acharya, U.R., “ResNet-Attention model for human authentication using ECG signals”, Expert Systems, vol.38, no.6, pp.12547, 2021.
3. Tarawneh AS, Hassanat AB, Alkafaween EA, Sarayrah B, Mnasri S, Altarawneh GA, Alrashidi M, Alghamdi M, Almuhaimeed A., “DeepKnuckle: Deep Learning for Finger Knuckle Print Recognition”, Electronics, vol.11, no.4, pp.513, February 2022.

4. Jomaa RM, Islam MS, Mathkour H, Al-Ahmadi S., “A multilayer system to boost the robustness of fingerprint authentication against presentation attacks by fusion with heart-signal”, Journal of King Saud University-Computer and Information Sciences, January 2022.
5. Xuejun Tan∗, Bir Bhanu, “Fingerprint matching by genetic algorithms “, The Journal of The Pattern Recognition Society, Pattern Recognition 39 (2006) 465 – 477.
6. Bouzouina, Y. and Hamami, L.,” Multimodal biometric: Iris and face recognition based on feature selection of iris with GA and scores level fusion with SVM”, 2nd International Conference on Bio-engineering for Smart Technologies (BioSMART), pp. 1–7,2017
7. Hezil, N. and Boukrouche, A.,” Multimodal biometric recognition using human ear and palmprint”, IET Biometrics, 6(5), pp. 351–359, 2017
8. Chaudhary, S. ,Nath, R.,” A Robust Multimodal Biometric System Integrating Iris , Face and Fingerprint using Multiple SVMs”, International Journal of Advanced Research in Computer Science, 7(2), pp. 108–113, 2016
9. Veluchamy, S. , Karlmarx L. R.,” System for multimodal biometric recognition based on finger knuckle and finger vein using feature-level fusion and k-support vector machine classifier”, IET Biometrics,6(3), pp. 232–242, 2017
10. Al-Waisy, A. S. et al.,” A multimodal biometrie system for personal identification based on deep learning approaches”, Seventh International Conference on Emerging Security Technologies (EST). IEEE, pp. 163–168, 2017
11. Ali, Mouad MH, Vivek H. Mahale, Pravin 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), pp. 332–339. IEEE, 2016.
12. Sun W, Su F, Wang L., “Improving deep neural networks with multi-layer max out networks and a novel initialization method”, Neuro computing, vol.278, pp.34-40, February 2018.
13. Abdollahzadeh B, Gharehchopogh FS, Mirjalili S., “African vultures optimization algorithm: A new nature-inspired metaheuristic algorithm for global optimization problems”, Computers & Industrial Engineering, vol.158, pp.107408, August 2021.
14. Abualigah L, Yousri D, Abd Elaziz M, Ewees AA, Al-qaness MA, Gandomi AH., “Aquila Optimizer: A novel meta-heuristic optimization Algorithm”, Computers & Industrial Engineering, vol.157, pp.107250, July 2021
15. CASIA Fingerprint Image Database available at “https://mla.sdu.edu.cn/info/1006/1195.html”
16. Mirjalili, S., “SCA: a sine cosine algorithm for solving optimization problems,” Knowledge-based systems, vol.96, pp.120-133, 2016.
17. Shadravan, S., Naji, H.R. and Bardsiri, V.K., “The Sailfish Optimizer: A novel nature-inspired metaheuristic algorithm for solving constrained engineering optimization problems”, Engineering Applications of Artificial Intelligence, vol.80, pp.20-34, 2019.