An Optimization Enabled Deep Learning Based Multimodal Person Authentication System

[1]Pravin L Yannawar, Pardeshi S. R
Dr. Babasaheb Ambedkar Marathwada University,
Aurangabad, (MS), India
[1]*plyannawar.csit@bamu.ac.in*

Abstract

The practice of automatically recognizing the correct person using computational methods based on features maintained in computer systems is known as person authentication. Security, robustness, privacy, and non-forgery are the critical aspects of any person authentication system. Traditional biometric-based systems are dependent on the use of a single modality, which may be lacking in the ability to provide high security. These systems are vulnerable to noise and can be readily exploited. An optimization enabled deep learning based multimodal person authentication system is presented to solve these disadvantages. Here, a combination of brainwave signals and fingerprint images are utilized for providing improved security. A Deep Maxout Network (DMN) is utilized for performing person authentication on both the modalities and the output obtained is fused together using cosine similarity to attain the final result. The African vultures-Aquila Optimization (AVAO) algorithm is a unique optimization algorithm for updating the DMN weights. To construct the algorithm, the African Vulture Optimization Algorithm (AVOA) techniques are updated according to the extended exploration capabilities of the Aquila Optimizer (AO). The presented multimodal person authentication system achieves an accuracy of 0.926, sensitivity of 0.940, specificity of 0.928, and F1-score of 0.921, demonstrating exceptional performance. The experimental study also indicates the performance evaluation comparison of AVAO with the prevailing techniques such as Multi-task EEG-based Authentication, Multi model-based fusion, Multi-biometric system, and Visual secret sharing and super-resolution model on the basis of various metrics.

Keywords: Person authentication, multimodal, fingerprint, brain signal, Deep Max out Network.

1. INTRODUCTION

As technology advances daily, security measures are likewise becoming more sophisticated in relation to the technologies. The biometrics recognition system is currently the subject of active study, and it includes numerous biometric features, including biological and behavioural ones. Technology that measures and examines physical aspects of the human body for user authentication is referred to as biometrics..Traditional means of authentication like passwords, PINs, tokens, and smart cards are irrelevant for use with systems that demand a high level of security. The biometrics system is displacing traditional techniques by leveraging human physical or behavioural traits that really indicate a person's identity and have the advantages of being hard to copy, steal, and forge [1].The foundation of behavioral biometrics is the unique human behaviors like signature, keystroke, and voice. Identification of physical traits like the iris, face, or fingerprint is the subject of the study of physiological biometrics. These biometrics are very memorable, non-transferable, and distinctive. They are also extremely difficult to alter or steal. The steady uni-biometrics, however, are somewhat challenging to manufacture. The use of fake identities can lead to a number of security issues and high security threats[2].

Hence, a need for new efficient authentication techniques those are not vulnerable to falsification arises [3]. The security and robustness of the authentication approaches can be further improved by utilizing multimodal biometrics. Multimodal techniques combine two or more traits biometrics to create a robust system. It effectively overcomes the disadvantages faced by the unimodal systems, such as high error rates, spoof attacks, non-universality, inflexibility, noises and intra-class distinctions [4]. The fusion of the biometrics enhances the flexibility of the authentication scheme and also thwarts noisy information to have any adverse effect on the system performance. Moreover, the security is enhanced, due to the numerous authentication levels [5]. The hand-based authentication method has long been the focus of attention, and these systems are quite effective at identifying veins, hand form, hand geometry, palm prints, and fingerprints. These systems' dependability, simplicity, acceptance, and stability have made them very successful. Many government organizations, businesses, and corporations use these systems to provide security, keep track of attendance, and for other functions [6]. A Because of its great accuracy and acceptance, the fingerprint authentication system is the most widely used hand-based scheme. Additionally, the affordability and portability of fingerprint scanners have led to a huge increase in the number of applications [7]. Recently, difficult-to-forge non-physical signals like brainwaves have been used for person authentication [3].The brainwave signals can be investigated with the help of Electroencephalogram (EEG) where a simple electrode placed on the skin is used to measure the fluctuations of voltages on the scalp surface for recording the electrical activity of the brain [8]. The electrodes are placed on various positions on the scalp to measure the EEG. The major advantages of utilizing EEG for authentication is that the brain signals or the electrical activity of each individual is varied and is very difficult to manipulate or forge and is highly resistant to spoofing attacks[9]. EEG is a highly complex signal and in the current situation, where applications mostly depend on data with high complexity, the deep learning techniques are used .The deep learning methods are highly efficient in solving issues in various health related fields, such as public health, medical informatics, pervasive sensing, medical imaging, bioinformatics, etc [10]. The deep learning techniques are found to be advantageous in most applications using complex EEG signals, like Brain-Computer Interface (BCI), emotion recognition, sleep studies, seizure detection and insomnia diagnosis [11]. EEG signals are affected by the mental state, stress and mood of an individual, thereby making it extremely challenging to obtain these signals by threat or force [12]. Despite the various benefits of the fingerprint-based schemes, the technique is susceptible to presentation attacks (PAs) [13]. Also, the authentication systems that depend on EEG alone are highly instable and have less accuracy. Also, the EEG signals collected from the scalp have a weak Signal-to-Noise Ratio (SNR) and low resolution [14].

In this study, a multimodal authentication method is developed by fusing brain wave and fingerprint signals. These methods were picked because they are the most dependable and acceptable ones. After pre-processing for both modalities, the brainwave signals' features, and the processed fingerprint's minute details are identified. The output is then concurrently fed to the DMN for tuning using the developed AVAO algorithm. The acquired findings are then combined using Cosine similarity.

The main contributions of this paper focus on.

1. A **multimodal authentication system** development with the help of two modalities- brain waves and fingerprint images.

2. Development of a novel **AVAO algorithm** for person authentication by modifying the weights of the hidden neurons in the DMN. In order to improve the performance of the classifier, the AVAO algorithm was developed by altering the AVOA in relation to the AO. The rest of the paper is organized in the following structure: Section 2 reviews the literature on the various multimodal authentic systems and section 3 elaborates the introduced person authentication system. Section 4 details and discusses the experimental outcomes**.** Section 6 concludes the work and offers some perspectives.

2.LITERATURE REVIEW

A large number of researches have been conducted on the development of the authentication schemes using multi-modalities. In this research, eight of the prevailing researches are considered and the methods are detailed here. Wu Q *et al* [15] presented a multi-task EEG-based person authentication system by integrating the eye blinking and the EEG signals to create multimodality. Here, Rapid Serial Visual Presentation (RSVP) was utilized for obtaining unique EEG signal. The eye blinking and the EEG signals were subjected to the extraction of the morphological along with the Event-Related Potential (ERP) features, which was followed by score estimation using the back propagation neural network and Convolutional Neural Network (CNN). The technique offered high accuracy and privacy; however the technique failed to consider various aspects, like noisy surroundings, heart rate, mood, fatigue, etc. The drawback presented above are over come in [16], Aleem S *et al* proposed a multi-modal system based on fusion strategy, which utilized the face and fingerprint modalities for person authentication. The technique employed alignment-based elastic algorithm for finger print matching and Extended Local Binary Patterns (ELBP) for extraction of facial features. Local non-negative matrix factorization was made use of to reduce the ELBP feature space and finally fusion was executed. The technique was highly effective in reducing the redundant information; but it was unsuccessful in increasing the accuracy for its usage in real time applications. A highly accurate classification method was implemented in [17],Chanukya PS and Thivakaran TK presented a novel optimal neural network-based biometric image classification technique, which used fingerprint and ear modalities for person authentication. A modified region growing algorithm (MRG) was employed to extract the shape feature of ear as well as fingerprint images and Local Gabor Xor pattern (LGXP) was utilized for the calculation of the texture feature. In addition, an optimal neural network, trained by firefly algorithm was used in authentication. Though, the approach produced high accuracy, it failed to enhance the sensitivity of the technique. The problem of sensitivity was overcome in [18], Jijomon CM and Vinod AP introduced an EEG-based biometric identification method with auditory evoked potentials (AEPs), which utilizes the frontal electrodes to extract the AEPs and the signal is subjected to feature extraction. Finally, Gated Recurrent Unit (GRU), Long Short-Term Memory (LSTM) and one dimensional (1D)-CNN are utilized in authentication. The technique provided a very fast rate of data acquisition, but it was unsuccessful in utilization of consumer-grade devices for collecting data.

A low cost multi-biometric system was proposed by Khodadoust J *et al.* [19] for identification, which employs three biometric, such asfinger-knuckle-print, finger-vein, and fingerprint. Here, three different cameras were utilized for capturing the biometrics without any contact. The captured 2D images were converted to 3D images, and the 2D and the 3D images obtained were matched with the information stored in the database and the score level fusion was performed for detecting the user. The technique achieved high accuracy and the system was highly robust, but optimization was not considered to improve performance. An optimized method was developed in [20], Chakladar DD*et al* developed a multimodal Siamese Neural Network (mSNN) for enhancing the verification of user by utilizing the EEG signal and the signature. The spatial as well as temporal features of the signatures and EEG signals are fused to form a feature space, which is then forwarded to a Siamese network for verifying the user. The method was highly efficient in reducing the success of forgery attempts, but failed to enhance the computational burden. The drawback of computational complexity was overcome in [21], Muhammad A *et al* presented a secure fingerprint authentication technique by developing a fingerprint template protection method which uses super-resolution (SR) and visual secret sharing (VSS). The technique encrypted the fingerprint image captured during enrolment into “n” share and these shares were stored in separate databases. At the time of authentication, a multiple image super-resolution technique was utilized for restoring the secret fingerprint image from the shares present in the databases. Although, superior security and privacy was delivered, the technique was unsuccessful in enhancing the contrast of the reconstructed image. In order to avoid the drawback of using fingerprint modality, Bidgoly AJ *et al.* [22] developed a scheme where an EEG-based authentication scheme is introduced. Here, deep learning approaches were utilized for capturing the fingerprint of the EEG signal. A fingerprint function was utilized for storing the fingerprint of the EEG signal thereby preserving the privacy of the user. The technique produced high accuracy and was highly effective in ensuring privacy; however it failed to take into account deep learning techniques for enhancing the performance.

2.2. Challenges

The key issues faced by the prevailing techniques of authentication based on brain signals and fingerprint is listed as follows;

- A multi-modal system based on fusion strategy was developed in [16] for personal identification. Though, this method achieved higher recognition accuracy, the future challenge lies in making this technique more appropriate for usage in real-time application.
- A technique that is capable of applicable in real time application was introduced in [15], where a multi-task EEG-based person authentication system was developed for enhancing the robustness and accuracy of the system. Meanwhile, the major challenge lies in utilization of commercial EEG acquisition equipment for enhancing the system practicability.
- The issue faced in [15] was overcome by the EEG-based authentication scheme proposed in [22] ,which achieved high accuracy. However, the major challenge faced was that the method failed to consider utilization of other techniques for enhancing the privacy and universality of the technique.
- The enhanced privacy was achieved by the fingerprint template protection and fingerprint authentication scheme [21], which utilizes visual secret sharing and super-resolution. The scheme was unsuccessful in considering improved data hiding approaches for embedding more information in the shares, which remains a major challenge.
- Existing techniques of automated authentication system based on fingerprint have a major security concern owing to the database where the data is stored. Moreover, there is a high risk associated with forgery. On the contrary the EEG based authentication systems are highly instable and have low SNR and hence developing a system with a stable response in minimum time is crucial.

3. PROPOSED DEEP LEARNING BASED PERSON AUTHENTICATION TECHNIQUE - AVAO

In this paper, the two biometric modalities, such as brainwave signals and fingerprint image 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. The entire process is carried using the two modalities, namely fingerprint image and brain signal. In the fingerprint authentication module, initially data acquisition is performed, followed by pre-processing using ridge enhancement, then minutiae is detected using Hit or miss transform (HMT) and finally person authentication is executed with the DMN. Likewise, in the brain signal authentication module, the brain signals are first acquired from the dataset and then the signals are pre-processed with Gaussian filter, which is followed by feature extraction. After feature extraction, person authentication is done using DMN. The devised AVAO algorithm is used to adjust the weight factors of the DMN. The authenticated outputs obtained from both the modules are fused together using cosine similarity to obtain the final output. These processes are detailed in the following subsections

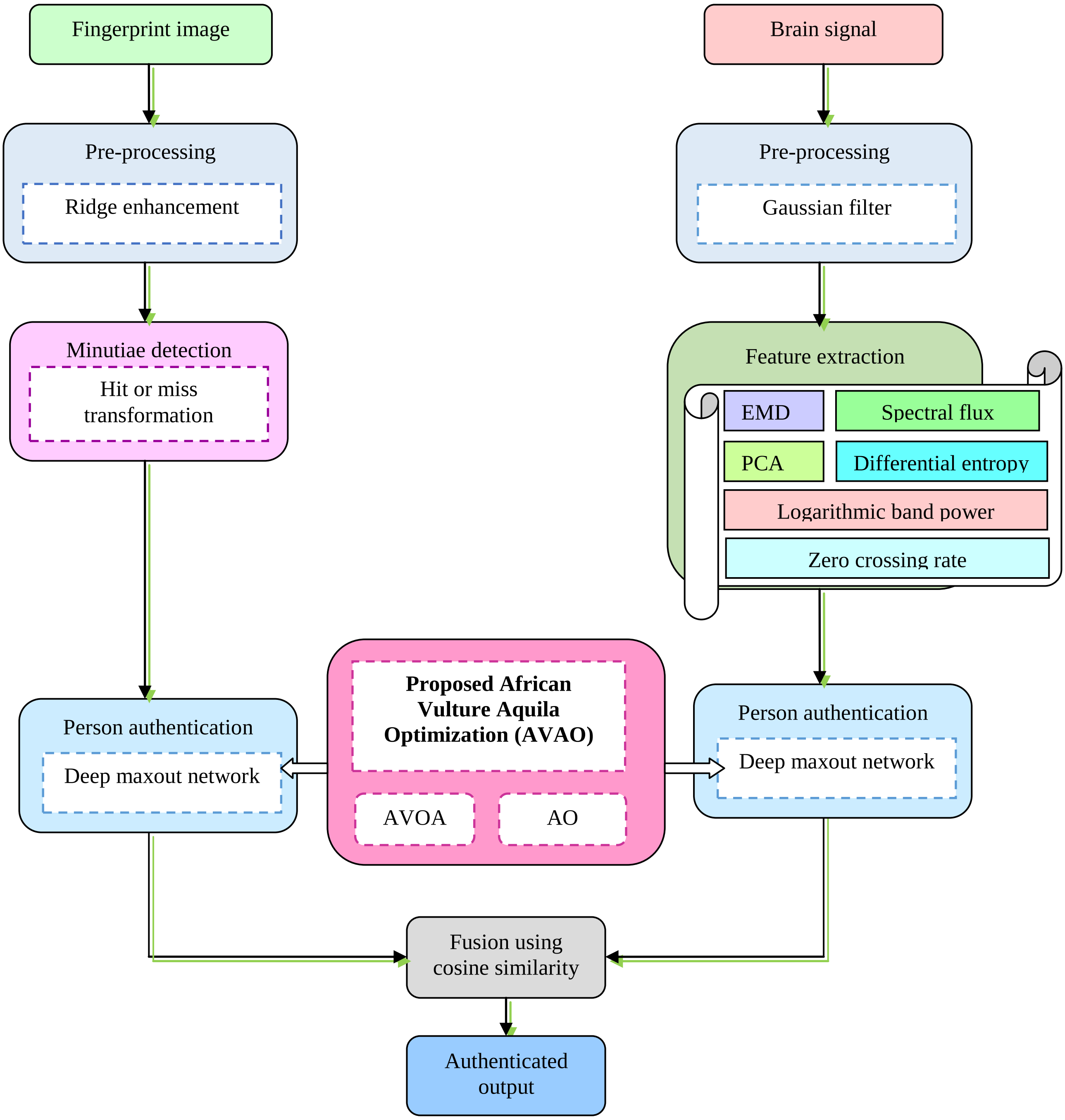


Figure 1. Schematic representation of the Proposed deep learning based person authentication technique – AVAO

3.1. Module for Fingerprint Authentication

The procedure of authenticating the fingerprint image is covered in this section. The most typical use of fingerprint pictures in the identification process is due to their singularity and invariance. The steps that must be taken in order to prepare the fingerprint image for authentication are listed below along with the authentication process

3.1. Acquiring Fingerprint images

Consider a the following dataset that is represented as

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

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

3.1.2. Pre-processing Fingerprint Images

The fingerprint image fp_i acquired from the database is subjected to pre-processing. Here, the ridges are obtained through pre-processing using a ridge enhancement [23] method. Without requiring any prior knowledge, ridge improvement is incredibly effective at removing pixel-by-pixel imperfections. From the low quality input, a number of techniques are applied to produce an enhanced quality image. By using dilation, which enlarges items in the fingerprint image by adding extra pixels to their interior and exterior boundary pixels, the image quality is improved. Following expression is used to obtain the ridge enhanced fingerprint image.

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

where, l denotes the structuring element. The pre-processed output thus obtained Rid_i is then passed to the minutiae detection phase.

3.1.3. Minutiae Detection Phase

The ridge enhanced image Rid_i is forwarded to the minutiae detection [24] phase where minutia points present in the ridge enhanced images are identified. Gray-scale Hit-Or-Miss Transformation (GHMT) is used here. The GHMT has the benefit of being adaptable and using both foreground and background information to identify the details. 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, the GHMT is modified using the template matching idea., 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. The terms $\min^2$ and $\max^2$ denote the second minimum as well as the maximum values of the gray-level substitution of binary erosion and dilation operation. The terms a_1 and a_2 are pixels in theforeground structuring element and background, respectively.

The sixteen pre-defined and orientated templates used by GHMT will identify the details. 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 $A^{\wedge}(x,y)$.

By utilising equation (3) pixel wise to conduct GHMT on both the original and the inverted image, the details are found. Each of the original and inverted photos for each template yields a total of sixteen filtered outputs. This can be expressed by,

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

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

where, $Ridinv_i$ denotes the inverted ridge enhanced image, B_{org}^{j} and B_{inv}^{j} 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.

Finding the highest pixel values among the outputs of filtering is how the minutiae points are found, and the highest pixel value that above the threshold is chosen as the minutiae, which can be expressed as,

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

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

3.1.4. Deep Maxout Network for Person Authentication

In the process of matching fingerprint images, the DMN [25] is used, and it performs authentication using the minutiae points found in the preceding stage. This section describes the DMN's structure as well as the newly developed AVAO algorithm, which is used to modify the DMN's weights.

3.1.4.1. DMN

A DMN is made up of many maxout layers connected consecutively, each of which contains hidden units that are divided into groups. Each layer employs the maxout function to produce concealed activations, and the resulting trainable activation functions. The minutiae points are passed as an input to the DMN whose activation functions can be given by,

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

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

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

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

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

where, h_e denotes the number of hidden units in the e^{th} layer, $k_{...st}$ and d_{st} signifies the weight and the bias of the layer. Moreover, the term 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.

3.1.4.2. Proposed AVAO algorithm

This work introduces a novel AVAO method that is used to update the weights of the hidden neurons in the DMN. The newly developed AVAO algorithm was developed by changing the AVOA's [26] methods in light of the AO's increased exploration capacity [27]. The population-based AVOA algorithm draws its inspiration from the foraging, navigation, and way of life of African vultures. The four steps of AVOA implementation include selection of the best vulture, estimation of starvation rate, exploration, and exploitation. The best and second-best solutions to any difficult situations are sought after by AVOA. The algorithm is highly adaptable and has a relatively simple computational structure. Additionally, the programme successfully strikes a balance between resonance and unpredictability. On the other hand, the AO method is applied in four steps, including expanded exploration, narrowed exploration, expanded exploitation, and narrowed exploitation, taking into account the predatory behaviour of Aquila. The AO method can successfully handle real-time applications and has a quick convergence rate. Thus, the AVAO algorithm achieved excellent efficiency and quick convergence by merging both the algorithms. Following are the steps in the proposed AVAO algorithm.

i) Initialization

Let us assume there are av number of vultures. The first step is to initialize 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 initialized, the best vulture is determined by considering the fitness of all the vultures. The value of fitness is calculated using mean square error given by 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 by various iterations.

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

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 modeled 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 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 utilized to select the approaches. The strategies are selected based on the following equations.

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

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

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

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]. The terms upb and lwb denotes the lower as well as the upper limits of the variable.

Substituting equation (20) in equation (18),

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

Here, $W(i) > R(i)$ and hence the above equation can be rewritten as,

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

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

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,

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

where,

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

Assume, $T=1$

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

Consider, $H_1\left(n+1\right)=R(i+1)$ (27)

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

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

Substituting equations (27), (28) and (29) in equation (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 equation (31) in equation (23),

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

$$R(i+1)+R(i+1)\times SR=\quad W(i)\left[1+Z\times SR+\left(1-\frac{n}{N}-rnd\right)\times SR\right] \tag{33}$$

$$R(i+1)\left[1+SR\right]=\quad W(i)\left[1+\left(Z+\left(1-\frac{n}{N}\right)-rnd\right)\times SR\right] \tag{34}$$

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

Here, N denotes the number of samples and rnd is a arbitrary number.

v) Exploitation:phase 1

Exploitation is performed in two phases depending on the value of SR. If the value of $\left|SR\right|$ 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 fight approach is performed.

a) Contest for food

The vultures are full and have high energy, if $\left|SR\right|\geq 0.5$. 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.

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

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

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,

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

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

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

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 utilized 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

(a) 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.

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

(b) 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.

vii) Feasibility evaluation

The optimal solution is calculated by finding the value of fitness. If the current solution found has the least fitness, then the existing solution is replaced by the current one.

viii) Termination

The above steps are kept reiterated till a best solution is achieved[28].

3.2. Module for Brain Signal Authentication

In this section, the process of person authentication using the brain signal is explained. Brain signals are measured by using the EEG, these signals offer highly efficiency in person authentication owing to their significant features, like impossibility in retrieving signals by force or coercion and high resistivity to spoofing attacks. The raw brain signals have to be processed before they can be utilised for authentication. These processes along with the authentication are detailed in the ensuing subsections.

3.2.1. Brain Signal Acquisition

Consider a dataset Br containing a total of n_b brainwave signals, which is given by the following expression,

$$Br = \left\{ br_1, br_2, ..., br_j, ..br_{n_b} \right\} \tag{45}$$

where, br_j represents the j^{th} brain signal of the person, which is subjected to preprocessing.

3.2.2. Brain Signal Pre-processing

The raw input brain signal br_j is forwarded to the pre-processing step, for eliminating the noises and the artifacts as well as the noise present in the signal. Also, the signal is processed to make it suitable for further operations. Here, a Gaussian filter [29] is employed in the pre-processing of the brain signals. The Gaussian filter is a linear filter, which is extremely effective in smoothing the input signals and is based on the Gaussian function with the probability density function given by,

$$G(z) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(z-\mu)^2 / 2\sigma^2} \tag{46}$$

Here, μ, σ signifies the mean and standard deviation of the distribution, and z represents the signal. Consider the output obtained be denoted by g_i , which is then forwarded to the feature extraction phase.

3.2.3. Feature Extraction

In this section, the significant features present in the brain signals are extracted. The brain signals obtained are continuous in nature and are recorded from the various locations on the brain by measuring the electrical fluctuations, which is a time series signal. The non stationary nature of the brain signals can be analysed efficiently by using the time-frequency domain. Therefore, the feature extraction can be performed by considering the frequency, time or spatial domains to obtain the feature vector. The significant features extracted during the process are detailed below.

i) Empirical mode decomposition (EMD)

EMD [30] refers to the process of obtaining frequency and amplitude pattern named Intrinsic Mode Function (IMF) present in the time series data. EMD is utilised in classifying the seizure and non-seizure brain signals. The EEG signal can be decomposed into multiple IMF using the EMD method, which is performed in two steps. Initially, the IMF is obtained followed by application of the Hilbert-Huang Transform (HHT) for obtaining the initial sequence of the instantaneous frequency spectrum. The EMD thus obtained is denoted as f_1.

ii) Spectral flux

Spectral flux is used to find the spectral variations that exist between consecutive frames. It can be calculated by considering the following equations [31].

$$Y[p] = FFT\left[g_i[q]\right] \quad p = 1,2,..P \quad q = 1,2,..,P \tag{47}$$

$$\hat{Y}[p] = \frac{Y[p]}{\arg\max\left[Y[p]\right]} \tag{48}$$

$$f_2 = \sum_{q=1}^{P}\left[\left|\hat{Y}[p]\right| - \left|\hat{Y}_{pf}[p]\right|\right]^2 \qquad (49)$$

where, $g_i[q]$ signifies the input signal, $Y[p]$ represents the Fast Fourier Transform (FFT) of $g_i[q]$, P denotes the frame length($P = 1024$), $\hat{Y}_{pf}[p]$ represents the spectral flux from the previous frame and f_2 signifies the spectral flux.

iii) Zero crossing rate

Zero crossing [32] denotes the point at which the consecutive samples in the signal have varied signs and denotes the frequency of the signal. The number of times a signal passes through the zero in a specific time interval is called zero crossing rate. The zero crossing rate can be given by the following expression,

$$f_3 = \sum_{n=-\infty}^{\infty} \left|\operatorname{sgn}[g(n)] - \operatorname{sgn}[g(n-1)]\right| v(k-n) \qquad (50)$$

Here, sgn denotes the signum function, which is given by

$$\operatorname{sgn}[g(n)] = \begin{cases} 1 & , g(n) \geq 0 \\ -1 & g(n) < 0 \end{cases} \qquad (51)$$

Where, $v(m)$ is a windowing function given by,

$$v(m) = \begin{cases} 1/2M & 0 \leq m \leq M-1 \\ 0 & otherwise \end{cases} \qquad (52)$$

Here, M denotes the number of samples.

iv) Principal Component Analysis (PCA)

PCA [33] refers to the statistical method of compressing the information from correlated variables in a large set to uncorrelated variables, while preserving the variability. It derives the principal components, which contain information present in the dataset and the components are derived in an order, such that majority of the variability is contained in the first components. These components are uncorrelated mutually to each other and are extracted as linear arrangement of the variables. PCA is executed on samples obtained from the signals on a specific interval of time and PCA is found by performing orthogonal transformation and is expressed as,

$$f_4 = \varphi^T g_i \qquad (53)$$

where, φ^T denotes the orthogonal transformation.

v) Differential entropy

Differential entropy (DE) [34] is feature that is used to evaluate the complex nature of discrete random variable. DE is utilized due to its simplicity and high selectivity that is offered while characterizing the EEG signal. DE is a significant feature that can be utilized in measuring extracting the important information in the raw brain signal, and is expressed as,

$$f_5 = \frac{1}{2}\log 2\pi\varepsilon\sigma_1{}^2 \qquad (54)$$

Here, ε represents the Euler's constant, and σ_1 designates the standard deviation of the processed brain signal g_i.

vi) Logarithmic band power

Logarithmic Band Power (LBP) [35] is utilized in extracting features of the EEG signals, which contains information related to the signal power in a particular range of frequencies. The signal power refers to the square of the amplitude of the brain signal at any instance. LBP can be calculated by,

$$f_6 = \log\left(\frac{1}{N}\sum_{m=1}^{N}|g_i(m)|^2\right) \tag{55}$$

Where, N represent the number of samples.

Finally, the feature vector FV will be formed by considering the various features, such as EMD f_1, spectral flux f_2, Zero crossing rate f_3, PCA f_4, DE f_5, and LBP f_6. The feature vector is given by,

$$FV = \{ f_1, f_2, f_3, f_4, f_5, f_6 \} \tag{56}$$

The feature vector FV is fed to the DMN for authentication.

3.2.4 Person Authentication with DMN

The DMN is utilized in the identification of the person using the brain signal. The feature vector FV obtained in the previous step is forwarded to the DMN, which is trained using the devised AVAO algorithm. The DMN and the AVAO algorithm are detailed in the sections 3.1.4.1 and 3.1.4.2 respectively. The output obtained is denoted by L_{br}.

3.3. Fusion using Cosine Similarity

In this step, the person authentication is executed by fusing the output acquired at the DMNs using the fingerprint image L_{fin} and brain signal L_{br} using cosine similarity. Cosine similarity is employed to identify the similarity between the two outputs by finding the cosine of the angle that exists between the two vectors. The final authenticated output is obtained by,

$$Out = \begin{cases} L_{fin} & ; L_{fin} == L_{br} \\ Out_{new} & ; otherwise \end{cases} \tag{57}$$

where, Out_{new} is obtained as,

$$Out_{new} = \begin{cases} L_{fin} & ; Ang_{fin} > Ang_{br} \\ L_{br} & ; Ang_{fin} < Ang_{br} \end{cases} \tag{58}$$

Ang_{fin} and Ang_{br} are calculated using,

$$Ang_{fin} = Cosim(L^t{}_{fin}, \alpha_1) \tag{59}$$

$$Ang_{br} = Cosim(L^t{}_{br}, \alpha_2) \tag{60}$$

Here, $Cosim$ designates the cosine similarity. $L^t{}_{fin}$ denote the output of DMN with respect to the fingerprint image in training and α_1 refers to the target with respect to the fingerprint image dataset. $L^t{}_{br}$ denote the output of DMN with respect to the brain signal in training and α_2 refers to the target with respect to the brain signal dataset. Cosine similarity can be generally expressed as,

$$Cosim = \frac{Out_{new}.\alpha}{\|Out_{new}\|\|\alpha\|} \tag{61}$$

The output achieved from the calculation of cosine similarity yields the authenticated output of the proposed AVAO optimized deep learning based multimodal person authentication system.

4. RESULTS AND DISCUSSION

The experimental outcomes of the Proposed deep learning based person authentication technique - AVAO are elaborated in this section together with the detailed analysis of the proposed method.

4.1. Experimental set up

The innovative AVAO enabled Deep learning approach for the efficient authentication of individual utilising fingerprint and brainwave signals 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 [36]. 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. The brain wave data set used in this paper is taken from Vision and Intelligent System Laboratory of Department of Computer Science and Information Technology, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad [37]. It consists of EEG Signal recordings of 10 subjects (i.e. 7 Male and 3 Female) in the age group of (20-25) . The cumulative size of the database is 12x10x10 = 1200 samples.

4.3. Performance measures

The efficiency of the proposed AVAO enabled Deep learning approach is measured using the efficiency metrics accuracy, sensitivity, specificity, F1 score and ROC. The next subsections go into more information about the parameters.

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,

$$Accuracy = \frac{tp + tn}{tp + tn + fp + fn} \tag{62}$$

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,

$$Specificity = \frac{tn}{tn + fp} \tag{63}$$

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,

$$Sensitivity = \frac{tp}{tp + fn} \tag{64}$$

4.3.4 F1 score

The **F1-score** combines the precision and recall of a classifier into a single metric by taking their harmonic mean

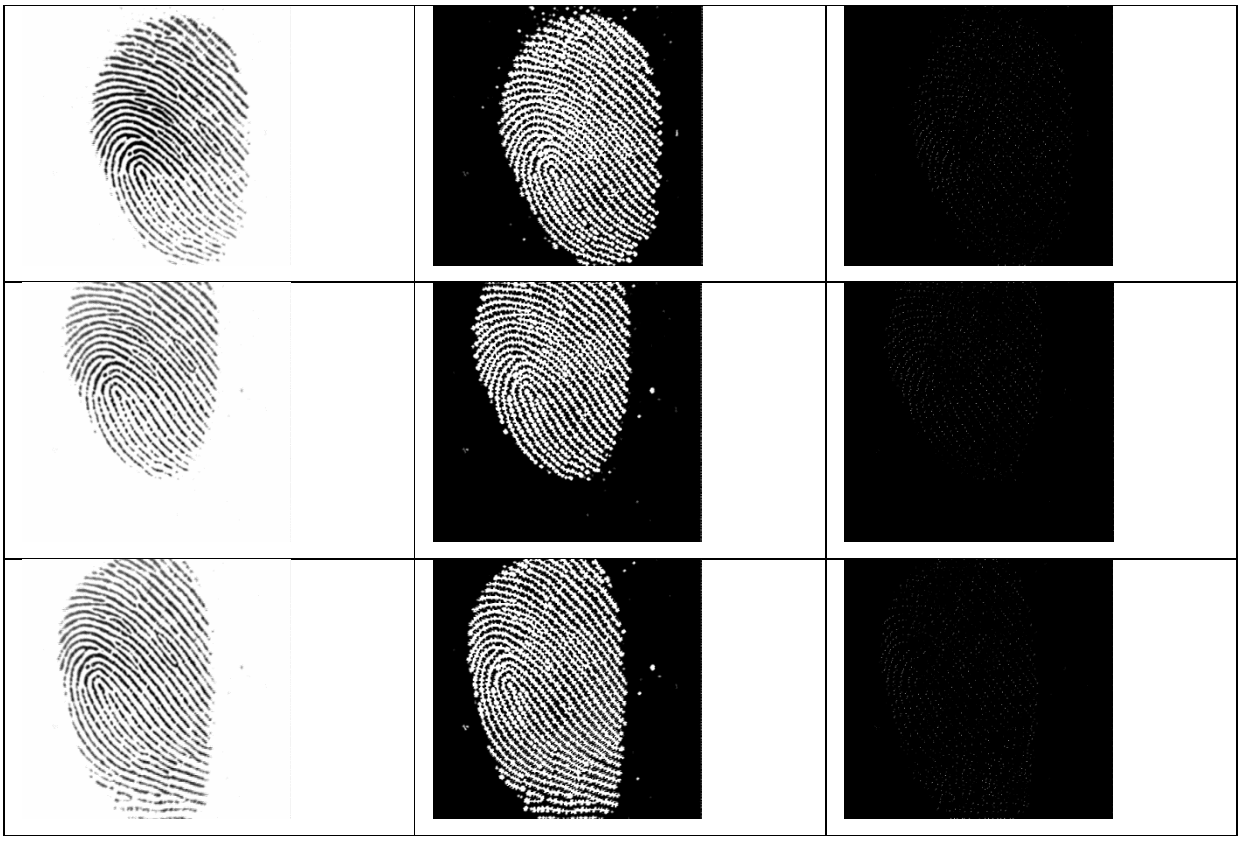
$$F1\ Score = 2*(Recall * Precision) / (Recall + Precision) \tag{65}$$

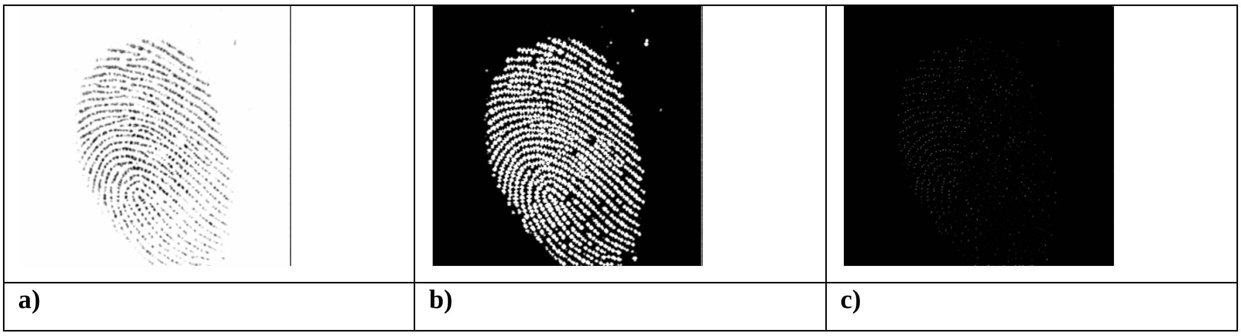
4.3.5 ROC

An ROC curve (receiver operating characteristic curve) is a graph showing the performance of a classification model at all classification thresholds. This curve plots two parameters: True Positive Rate and False Positive Rate. An ROC curve plots TPR vs. FPR at different classification thresholds. Lowering the classification threshold classifies more items as positive, thus increasing both False Positives and True Positives.

4.4. Experimental outcomes

In this section, the experimental results of the **Proposed deep learning based person authentication technique – AVAO** are portrayed. Figure 3 a) depicts the input fingerprint images, 3 b) shows the pre-processed images, figure 3c) illustrates the minutiae detection.





a) b) c)

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

4.5. Comparative methodologies

In this section, the proposed AVAO enabled deep learning based person authentication is evaluated for its performance by comparing it with the prevailing techniques, such as Multi-task EEG-based Authentication [15], Multi model-based fusion [16], Multi-biometric system [19], and Visual secret sharing and super-resolution model [21].

4.6. Comparative evaluation

The authentication schemes are analyzed based on various measures, like accuracy, specificity and sensitivity by considering different values of the training data percentages.

a) Analysis based on Fingerprint Image

Figure4 portrays the analysis based on fingerprint image for varying percentages of training data. In figure 4 a), the assessment with respect to accuracy is depicted. The proposed person authentication scheme using fingerprint achieved an accuracy of 0.896, whereas the existing technologies, such as multi-task EEG-based authentication, multi-biometric system, visual secret sharing and super-resolution model and the multi model-based fusion attained an accuracy value of 0.718, 0.758, 0.819 and 0.868 respectively for 60% of training data. This reveals that the proposed multimodal authentication system is better than the prevailing methods by 19.86%, 15.37%, 8.60% and 3.13%. Figure 4 b) illustrates the evaluation of the approaches while considering specificity. The values of specificity attained by the existing multi-task EEG-based authentication, multi-biometric system, visual secret sharing and super-resolution model and the multi model-based fusion, and the proposed AVAO optimized multimodal person authentication scheme is 0.720, 0.760, 0.817, 0.878 and 0.896, for training data of 70%. Thus, the proposed AVAO optimized multimodal person authentication scheme is shown to have achieved a performance improvement of 19.70%, 15.25%, 8.81% and 2.11% over the prevailing methods. The analysis of the techniques with respect to the sensitivity is displayed using figure 4c). The existing methods, like multi-task EEG-based authentication, multi-biometric system, visual secret sharing and super-resolution model and the multi model-based fusion measured sensitivity of 0.813, 0.829, 0.875 and 0.885, whereas the proposed AVAO optimized multimodal person authentication scheme computed a value of sensitivity at 0.925, when 80% of training data is considered. Thus, an enhancement in performance of 12.15%, 10.45%, 5.43% and 4.32% is produced by the devised technique. Figure 4 d) illustrates the evaluation of the approaches while considering F1-score. The values of F1-score attained by the existing multi-task EEG-based authentication, multi-biometric system, visual secret sharing and super-resolution model and the multi model-based fusion, and the proposed AVAO optimized multimodal person authentication scheme is 0.815, 0.836, 0.853, 0.877 and 0.901 for training data of 70%. Thus, the proposed AVAO optimized multimodal person authentication scheme is shown to have achieved a performance improvement of 10.5%, 7.75%, 5.62%, and 2.73% over the prevailing methods. The analysis of the techniques with respect to the roc is displayed using figure 4 e).

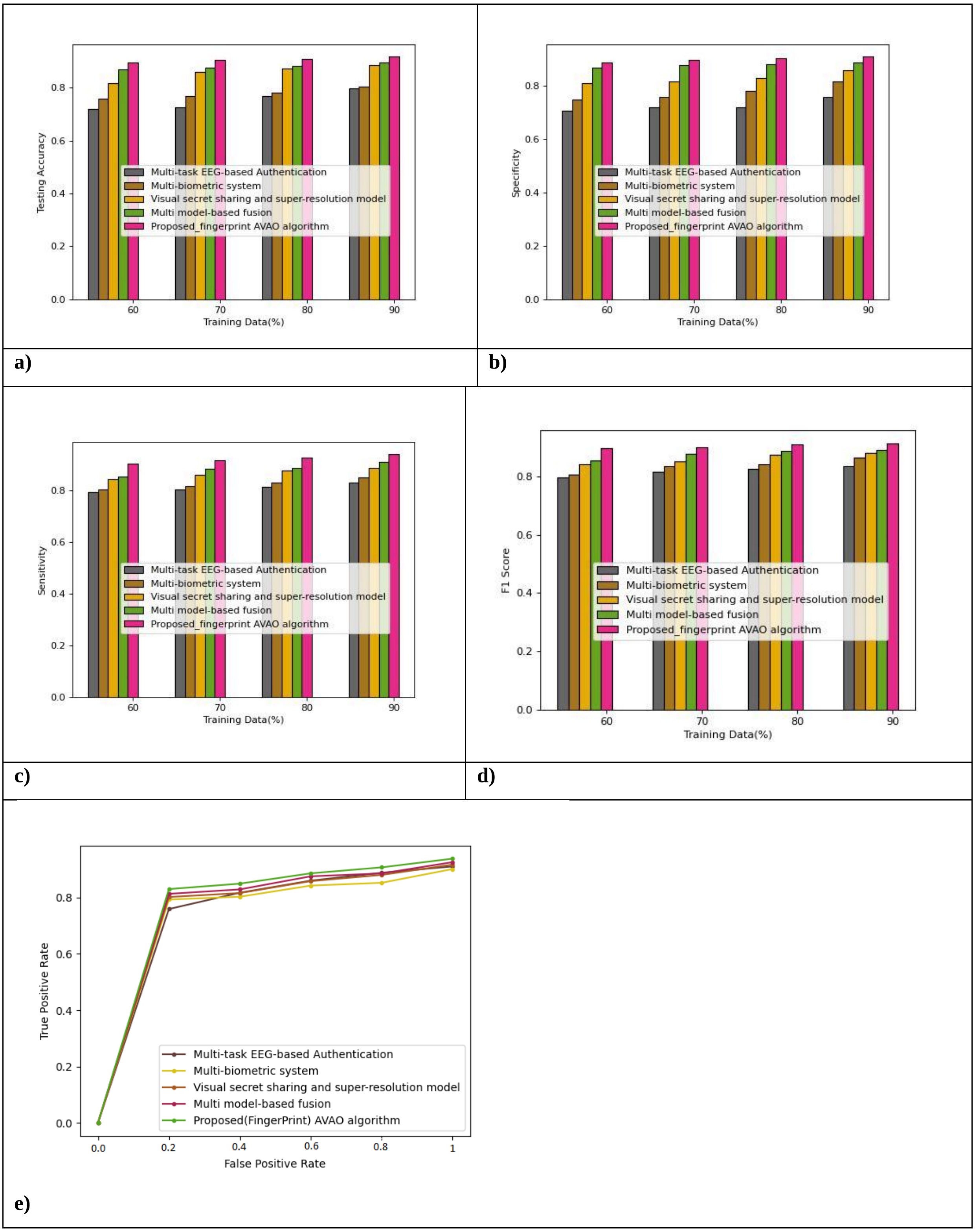
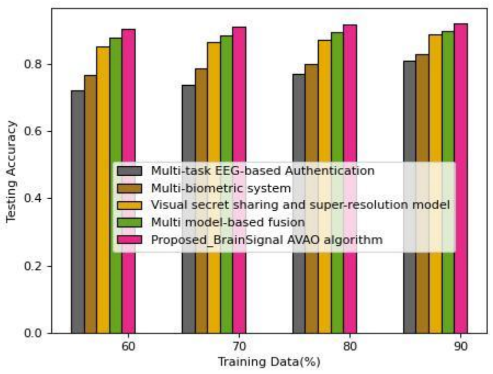


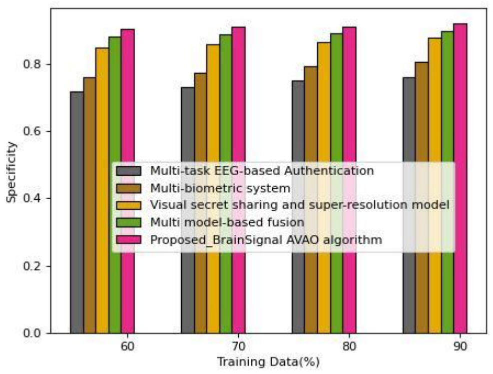
Figure 4. Assessment of the techniques using a) accuracy b) sensitivity c) specificity for varying training data d) F1-score e) roc

b) Analysis based on brain signal

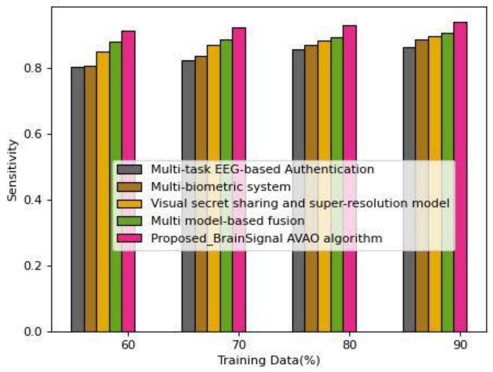
This section deals with the assessment of the person authentication schemes using brain signals for altering values of training data, which is displayed in figure 5. The assessment based on accuracy, specificity, sensitivity and F1-score are displayed using figure 5a, figure 5b, figure 5c and figure5d respectively. The analysis of the techniques with respect to the ROC curve is displayed using figure 5e. The proposed AVAO optimized multimodal person authentication scheme attains an accuracy of 0.918 when 80% of the training data is considered. But the existing techniques, like multi-task EEG-based authentication, multi-biometric system, visual secret sharing and super-resolution model and the multi model-based fusion produce an accuracy of 0.772, 0.801, 0.872 and 0.894 correspondingly, which is less than the proposed technique by 15.89%, 12.71%, 4.91% and 2.53%. While the percentage of training data is 70, the prevailing methods, such as multi-task EEG-based authentication, multi-biometric system, visual secret sharing and super-resolution model and the multi model-based fusion computed specificity values of 0.730, 0.775, 0.858 and 0.887. However, the proposed AVAO optimized multimodal person authentication scheme produced specificity of 0.910, which is higher than the exiting techniques by 19.79%, 14.88%, 5.72% and 2.57%. At 60% of training data, the devised AVAO optimized multimodal person authentication scheme achieved a value of sensitivity at 0.915, whereas the prevailing technique attain sensitivity values at 0.804 for multi-task EEG-based authentication, 0.808 for multi-biometric system, 0.851 for visual secret sharing and super-resolution model and 0.879 for multi model-based fusion. This depicts that the devised AVAO optimized multimodal person authentication scheme produces an enhancement in performance of 12.13%, 11.72%, 7.04% and 3.93% over the existing authentication techniques. While the percentage of training data is 70, the prevailing methods, such as multi-task EEG-based authentication, multi-biometric system, visual secret sharing and super-resolution model and the multi model-based fusion computed F1-score values of 0.818, 0.836, 0.865, and 0.871. However, the proposed AVAO optimized multimodal person authentication scheme produced F1-score of 0.901, which is higher than the exiting techniques by 10.14%, 7.75%, 4.16% and 3.44%.



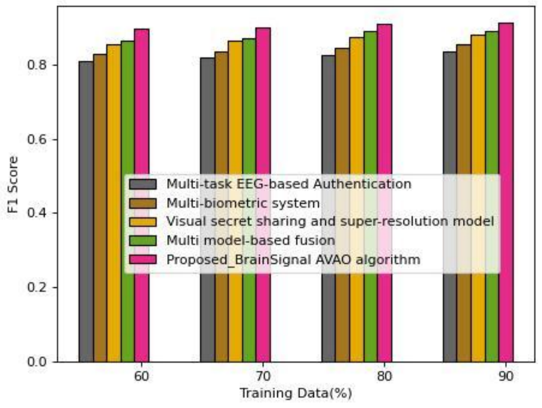
a)



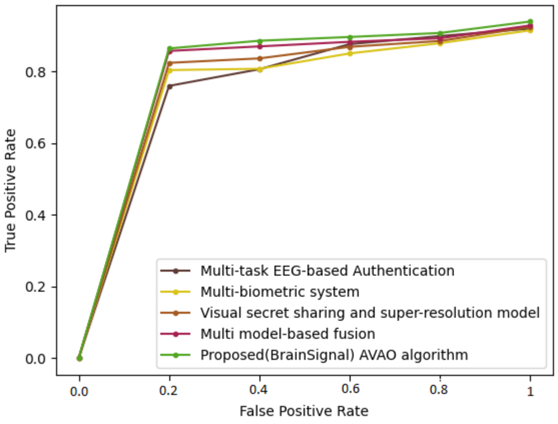
b)



c)



d)

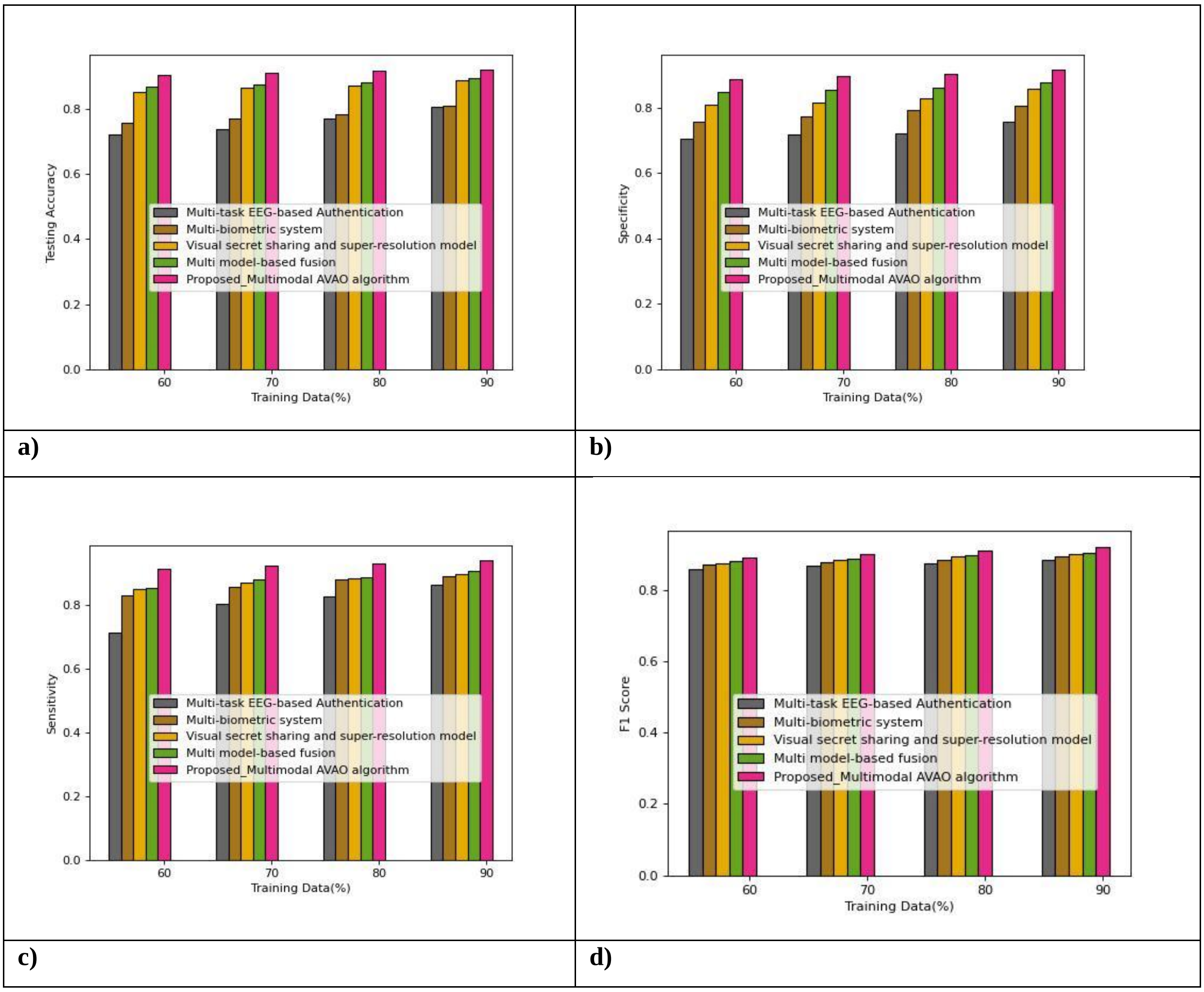


e)

Figure 5. Assessment of the techniques using a) accuracy b) sensitivity c) specificity for varying training data d) F1-score e) ROC curve.

c) Analysis based on Multimodalities

The evaluation of the authentication schemes based on multimodalities by altering the percentages of training data is depicted in figure 6. The evaluation of the approaches using the accuracy is displayed with the help of figure 6a). The devised AVAO optimized person authentication scheme attained a value of accuracy at 0.904 and the existing authentication techniques, like multi-task EEG-based authentication, multi-biometric system, visual secret sharing and super-resolution model and the multi model-based fusion achieve accuracy values of 0.723, 0.758, 0.851 and 0.868, with 60% of training data. From this it can be inferred that the devised technique attains a performance improvement of 20.09%, 16.18%, 5.90% and 4.05%. Likewise, the specificity based evaluation is depicted in figure 6 b). When 70% of training data is taken into account, the existing authentication techniques, such as multi-task EEG-based authentication, multi-biometric system, visual secret sharing and super-resolution model and the multi model-based fusion achieve values of specificity at 0.720, 0.775, 0.817, and 0.857, whereas the proposed AVAO optimized person authentication scheme obtained specificity of 0.896. Thus, the devised AVAO optimized person authentication scheme shows an improved performance of 19.70%, 13.59%, 8.81% and 4.45% over the prevailing schemes. In figure 6c), the analysis using sensitivity is displayed. The introduced AVAO optimized person authentication technique computes sensitivity of 0.929, but the prevailing approaches measure sensitivity values at 0.828 for multi-task EEG-based authentication, 0.879 for multi-biometric system, 0.883 for visual secret sharing and super-resolution model and 0.885for multi model-based fusion, for 80% training data. From this, the proposed technique is shown to have an enhanced performance of 10.88%, 5.40%, 4.92%, and 4.68% over the prevailing techniques. In figure 6 d), the analysis using F1-score is displayed. The introduced AVAO optimized person authentication technique computes F1-score of 0.919, but the prevailing approaches measure F1-score values at 0.883 for multi-task EEG-based authentication, 0.893 for multi-biometric system, 0.901 for visual secret sharing and super-resolution model and 0.902 for multi model-based fusion, for 90% training data. From this, the proposed technique is shown to have an enhanced performance of 4.07%, 2.9 %, 1.9 %, and 1.8% over the prevailing techniques.



a)

b)

c)

d)

Figure 6. Assessment of the techniques using a) accuracy, b) sensitivity, c) specificity for varying training data, d) F1-score.

4.7. Comparative Algorithms

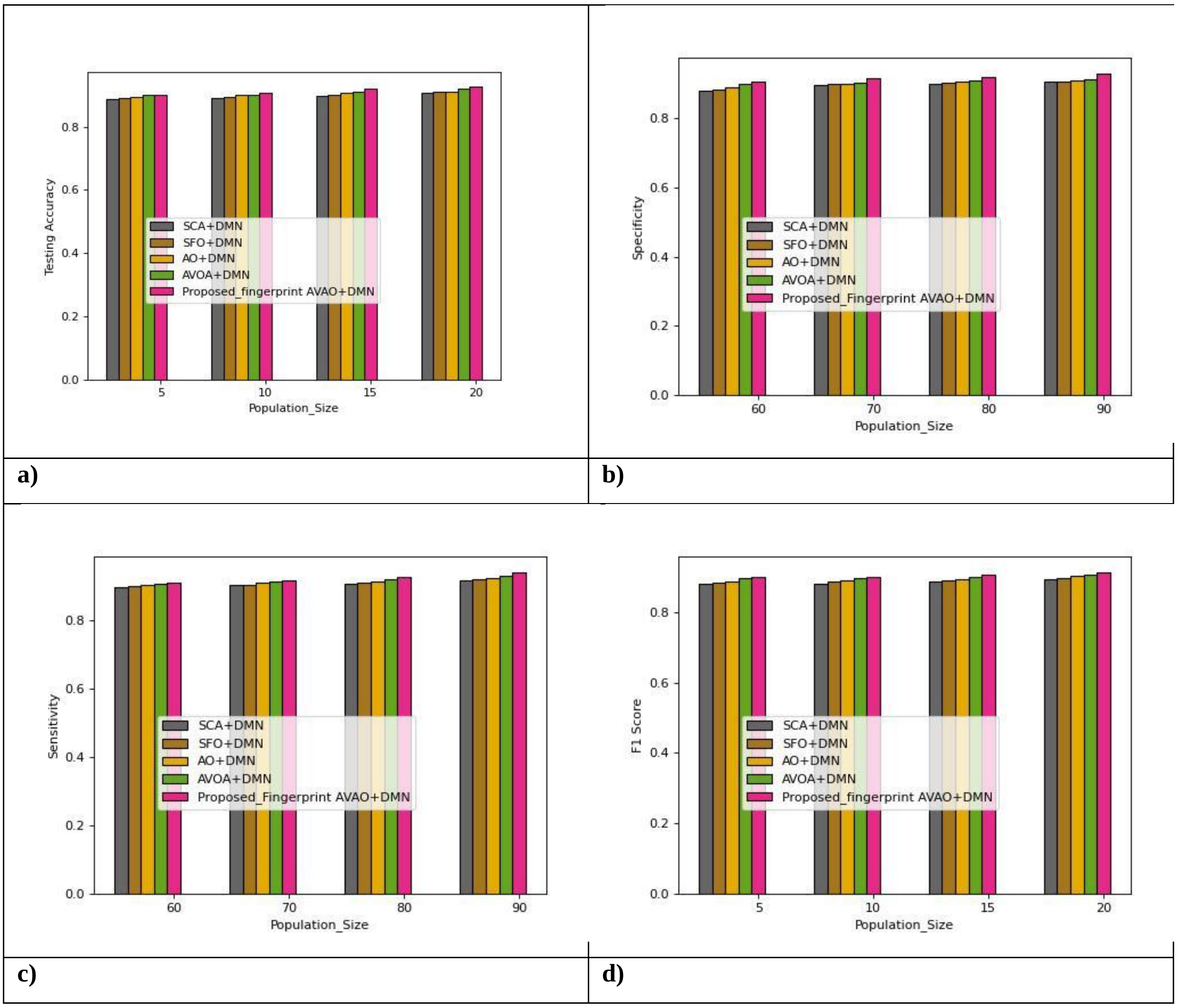
The performance of the devised AVAO algorithm in analyzed in comparison to the other existing algorithms, such as Sine Cosine Algorithm (SCA) [38] + DMN, Sail Fish Optimization (SFO)[39]+ DMN, AO [27]+ DMN, AVOA[26]+ DMN.

4.8. Algorithmic Analysis

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

4.8.1. Analysis using fingerprint image

Figure 7depicts the analysis of the various algorithms using fingerprint images. In figure 7 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 figure 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 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 7 d) 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, 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)

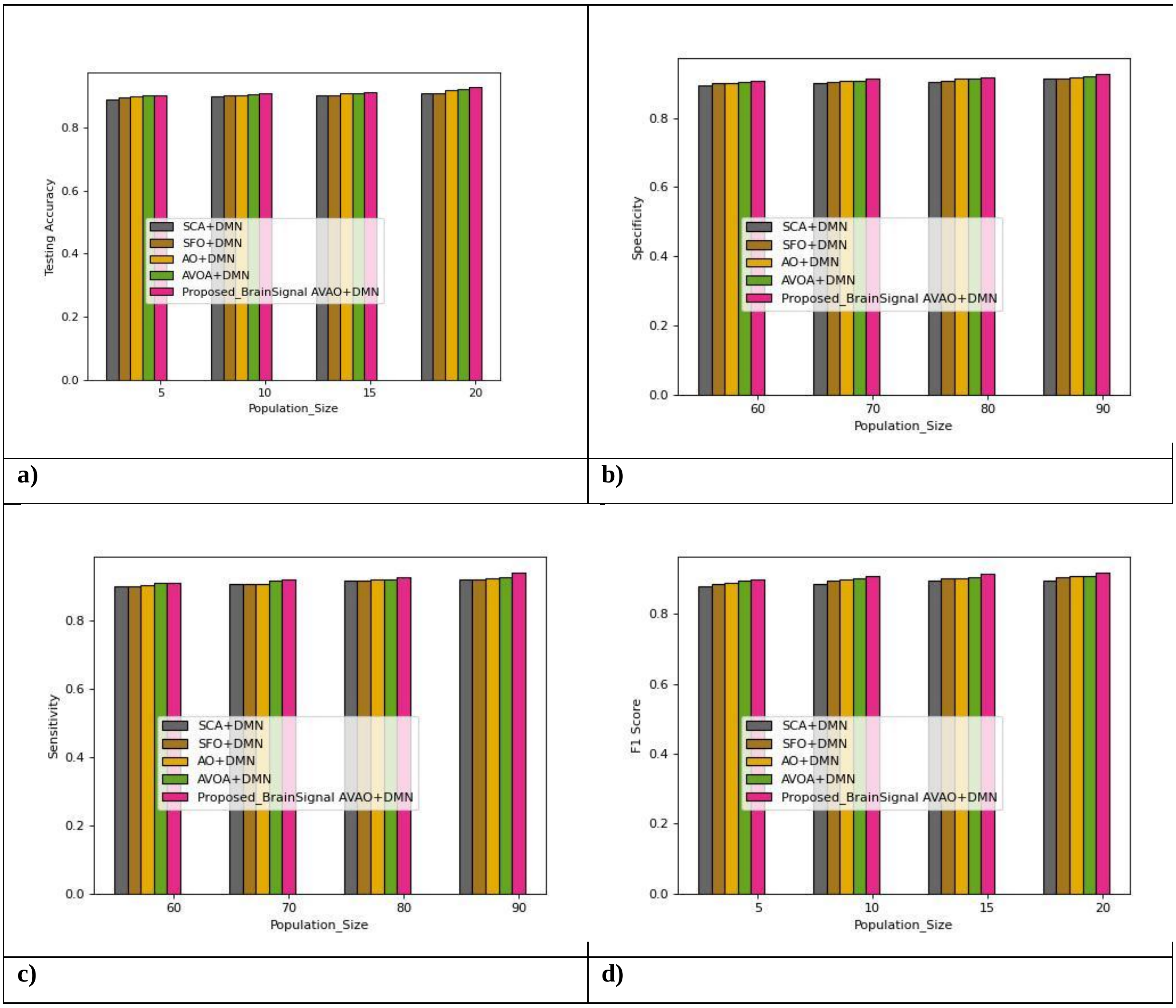
b)

c)

d)

Figure 7. Algorithmic evaluation using fingerprint image based on a) accuracy b) specificity and c) sensitivity d) F1-score.

In figure 8, the assessment of the algorithms with the brain wave signals is portrayed for altering population sizes. Figure 8 a) displays the assessment with respect to accuracy. The devised AVAO+DMN algorithm is shown to have obtained an accuracy of 0.908, whereas the prevailing SCA+DMN, SFO+DMN, AO+DMN and AVOA+DMN algorithms calculate accuracy of 0.899, 0.902, 0.901 and 0.907, when population size is 10. This illustrates that the introduced AVAO+DMN algorithm produced an improved accuracy by 1.06%, 0.75%, 0.77% and 0.10% over the conventional algorithms. The evaluation based on specificity is displayed in figure 8 b). The proposed AVAO+DMN algorithm is found to have attained a superior performance of 1.27%, 1%, 0.51% and0.19% more than the existing algorithms, by attaining a value of specificity at 0.918, wherein the prevailing algorithms, like SCA+DMN, SFO+DMN, AO+DMN and AVOA+DMN achieve lower values of specificity at 0.906, 0.908, 0.913 and 0.916, when population size is 15. Figure 8 c) depicts the sensitivity based evaluation of the algorithms. When the population size is 5, the values of sensitivity calculated by the various algorithms, such as SCA+DMN, SFO+DMN, AO+DMN, AVOA+DMN and the devised AVAO+DMN algorithm is 0.901, 0.901, 0.903, 0.910 and 0.911. From this it can be inferred that the proposed AVAO+DMN algorithm achieved a higher value of sensitivity than the prevailing algorithms by 1.10%, 1.02%, 0.83% and 0.08%. Figure 8 d) shows the evaluation based on F1-score. For the population size of 15, the values of F1-score, calculated by the various algorithms, such as SCA+DMN, SFO+DMN, AO+DMN, AVOA+DMN and the devised AVAO+DMN algorithm is 0.891, 0.901, 0.904, 0.907, and 0.916 respectively. This illustrates that the introduced AVAO+DMN algorithm produced an improved F1-score by 2.8%, 1.6%, 1.3% and 0.99% over the conventional algorithms.



a)

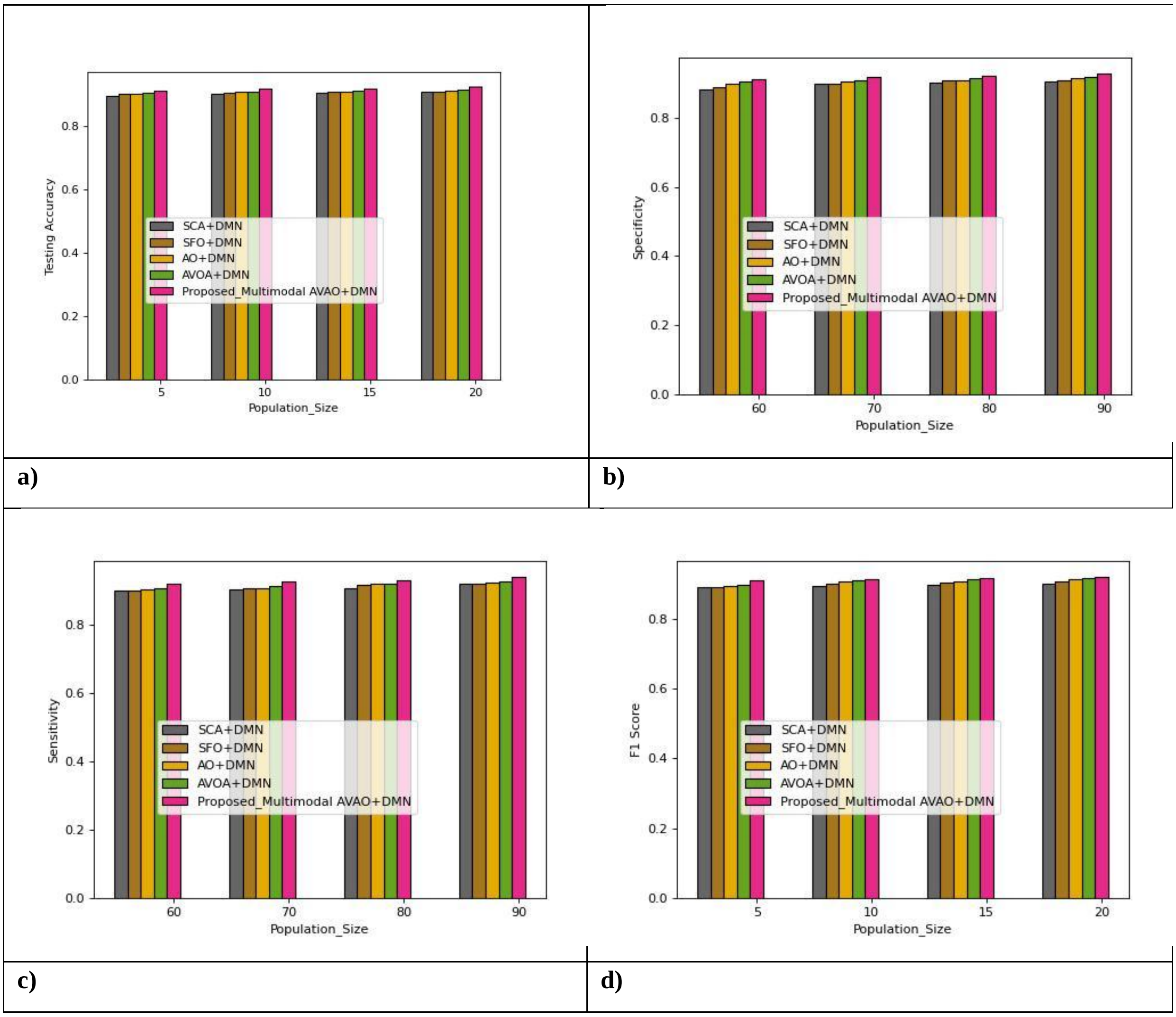
b)

c)

d)

Figure 8. Algorithmic evaluation using brain signals based on a) accuracy b) specificity and c) sensitivity d) F1-score.

In figure 9, the assessment of the algorithms on the basis of the modalities by considering various values of population sizes is displayed. The evaluation of the algorithms with respect to accuracy is demonstrated in figure 9 a). The existing SCA+DMN, SFO+DMN, AO+DMN and AVOA+DMN algorithms attain values of accuracy at 0.906, 0.909, 0.910 and 0.914, when the population size is 15. However, the proposed AVAO+DMN algorithm produces a higher accuracy of 0.921, thereby producing an enhanced performance of 1.65%, 1.34%, 1.15% and 0.80%. Figure 9 b) depicts the specificity analysis. When the population size is 5, the proposed AVAO algorithm attains a specificity of 0.913, which is higher than the values achieved by the prevailing algorithms by 3.40%, 2.45%, 1.42% and 0.74%. Meanwhile, the prevailing SCA+DMN, SFO+DMN, AO+DMN and AVOA+DMN algorithms attain only values of 0.882, 0.890, 0.900 and 0.906. In figure 9c), the analysis with respect to sensitivity is illustrated. The existing algorithms, such as SCA+DMN, SFO+DMN, AO+DMN and AVOA+DMN have attained values of sensitivity at 0.903, 0.906, 0.907 and 0.913, for population size of 10 and the introduced AVAO+DMN algorithm calculates sensitivity of 0.928. This reveals an enhanced performance of 2.67%, 2.35%, 2.17% and 1.60% by the proposed algorithm. In Figure 9 d), the analysis with respect to F1-score is depicted. . The existing algorithms, such as SCA+DMN, SFO+DMN, AO+DMN and AVOA+DMN have attained values of F1-score at 0.902, 0.909, 0.915, and 0.918 for population size of 20 and the introduced AVAO+DMN algorithm calculates F1-score of 0.921. This reveals an enhanced performance of 2.1%, 1.3%, 0.65% and 0.32% by the proposed algorithm.



a)

b)

c)

d)

Figure 9. Algorithmic evaluation using multimodalities based on a) accuracy b) specificity and c) sensitivity d) F1-score.

4.9. Comparative Discussion

This section deals with the comparison of the developed AVAO optimized multimodal person authentication scheme with the prevailing techniques on the basis of various metrics. Table 1 lists the various metrics and the corresponding values achieved by the existing and the introduced authentication techniques using fingerprint image, brain signals, and multimodality. The values are obtained when 90% of the training data is taken into account. From the table, the developed AVAO optimized multimodal person authentication scheme for brain signal modality is shown to attain a maximum value of accuracy, specificity, sensitivity, and F1-score at 0.920, 0.920, 0.940, and 0.912 respectively. The usage of two biometric modalities in the process of authentication accounts for high value of accuracy. Moreover, the specificity value is increased by the utilization of DMN in the classification process and the proposed AVAO algorithm used in the optimization leads to the increase in sensitivity.

Table 1. Comparative assessments of the various person authentication schemes

odalities	Metrics	Multi-task	Multi-	Visual	Multi	Proposed AVAO

		EEG-based authentication	**biometric system**	**secret sharing and super-resolution model**	**model-based fusion**	**optimized Deep Learning based Person Authentication**
Fingerprint image	***Accuracy***	0.797	0.806	0.886	0.895	0.918
	Specificity	0.759	0.817	0.860	0.888	0.910
	Sensitivity	0.830	0.849	0.886	0.907	0.938
	F1-score	0.836	0.863	0.881	0.890	0.912
Brainwave signal	***Accuracy***	0.809	0.828	0.887	0.899	0.920
	Specificity	0.760	0.807	0.877	0.899	0.920
	Sensitivity	0.865	0.886	0.897	0.908	0.940
	F1-score	0.836	0.853	0.881	0.891	0.912
Multi modality	***Accuracy***	0.806	0.809	0.887	0.895	0.920
	Specificity	0.759	0.807	0.860	0.879	0.917
	Sensitivity	0.865	0.889	0.897	0.907	0.940
	F1-score	0.886	0.893	0.901	0.902	0.919

Table 2 displays the comparative discussion of the algorithms. The devised AVAO+DMN algorithm is evaluated 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 0.929, sensitivity at 0.930, specificity at 0.940, and F1-score at 0.921.

Table 2. Comparative assessments of the algorithms

Modalities	**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	0.893	0.898	0.904	0.907	0.912
Brainwave signal	***Accuracy***	0.910	0.910	0.918	0.922	0.929
	Specificity	0.914	0.916	0.919	0.920	0.927
	Sensitivity	0.920	0.920	0.925	0.929	0.940
	F1-score	0.897	0.906	0.908	0.909	0.918
Multi modality	***Accuracy***	0.909	0.910	0.913	0.918	0.926
	Specificity	0.906	0.910	0.916	0.920	0.928
	Sensitivity	0.919	0.920	0.925	0.928	0.940
	F1-score	0.902	0.909	0.915	0.918	0.921

5. CONCLUSION

In this paper, an effective multimodal person authentication technique is created by utilizing the brain signals' highly safe nature and the fingerprint image's simplicity. Based on the brain signal and the fingerprint images, a DMN is used to identify the user. Prior to extracting characteristics from the brain signals and identifying the minute points in the fingerprint image, the two modalities are pre-processed. Then, utilizing the retrieved characteristics and identified minutiae points from the DMNs, person authentication is carried out. To construct the ideal weight factor for the DMN, a novel AVAO algorithm is developed, 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. The final authenticated output is produced by fusing the DMN outputs acquired using cosine similarity. Experimental results show that the devised AVAO technique achieved a higher accuracy of 0.926, specificity of 0.928, sensitivity of 0.940 and F1-score of 0.921. In future, the performance of the authentication scheme can be improved by considering other deep learning networks and more efficient optimization algorithms.

References

[1] Mouad M.H.Alia , *, Pravin L.Yannawarb A. T. Gaikwadc,"Multi-Algorithm of Palmprint Recognition System Based on Fusion of Local Binary Pattern and Two-Dimensional Locality Preserving Projection", ScienceDirect Procedia Computer Science 115 (2017) 482–492

[2]Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S. and Reich, C., "Continuous and transparent multimodal authentication: reviewing the state of the art", Cluster Computing, vol.19, no.1, pp.455-474, 2016.

[3] Puengdang, S., Tuarob, S., Sattabongkot, T. and Sakboonyarat, B., "EEG-based person authentication method using deep learning with visual stimulation", In proceedings of 2019 11th International Conference on Knowledge and Smart Technology (KST), pp. 6-10, IEEE, January2019

[4] Akhtar, Z., "Security of multimodal biometric systems against spoof attacks", Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy, pp.6, 2012.

[5] Kumar, K. and Farik, M., "A review of multimodal biometric authentication systems", Int. J. Sci. Technol. Res, vol.5, no.12, pp.5-9, 2016.

[6] 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.

[7] 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

[8] Maiorana E, Hine GE, La Rocca D, Campisi P., "On the vulnerability of an EEG-based biometric system to hill-climbing attacks algorithms' comparison and possible countermeasures", In2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), pp.1-6, September 2013.

[9] Bidgoly, A.J., Bidgoly, H.J. and Arezoumand, Z., "A survey on methods and challenges in EEG based authentication", Computers & Security, vol.93, pp.101788, 2020.

[10] Ravì, D., Wong, C., Deligianni, F., Berthelot, M., Andreu-Perez, J., Lo, B. and Yang, G.Z., "Deep learning for health informatics", IEEE journal of biomedical and health informatics, vol.21, no.1, pp.4-21, 2016.

[11]Wilaiprasitporn, T., Ditthapron, A., Matchaparn, K., Tongbuasirilai, T., Banluesombatkul, N. and Chuangsuwanich, E., "Affective EEG-based person identification using the deep learning approach", IEEE Transactions on Cognitive and Developmental Systems, vol.12, no.3, pp.486-496, 2019.

[12] Gui, Q., Jin, Z. and Xu, W., "Exploring EEG-based biometrics for user identification and authentication", In the proceedings of 2014 IEEE Signal Processing in Medicine and Biology Symposium (SPMB), pp. 1-6, IEEE, December 2014.

[13] Islam MS., "Heartbeat biometrics for remote authentication using sensor embedded computing devices", International Journal of Distributed Sensor Networks, vol.11, no.6, pp.549134, June 2015.

[14] Rahman, A., Chowdhury, M.E., Khandakar, A., Kiranyaz, S., Zaman, K.S., Reaz, M.B.I., Islam, M.T., Ezeddin, M. and Kadir, M.A., "Multimodal EEG and keystroke dynamics based biometric system using machine learning algorithms", IEEE Access, vol.9, pp.94625-946432021.

[15] Wu Q, Zeng Y, Zhang C, Tong L, Yan B., "An EEG-based person authentication system with open-set capability combining eye blinking signals", Sensors, vol.18, no.2, pp.335, February 2018.

[16] Aleem S, Yang P, Masood S, Li P, Sheng B., "An accurate multi-modal biometric identification system for person identification via fusion of face and finger print", World Wide Web, vol.23, no.2, pp.1299-317, March 2020.

[17] Chanukya PS, Thivakaran TK., "Multimodal biometric cryptosystem for human authentication using fingerprint and ear", Multimedia Tools and Applications, vol.79, no.1, pp.659-73, January 2020.

[18] Jijomon CM, Vinod AP., "Person-identification using familiar-name auditory evoked potentials from frontal EEG electrodes", Biomedical Signal Processing and Control, vol.68, pp.102739, July 2021.

[19] Khodadoust J, Medina-Pérez MA, Monroy R, Khodadoust AM, Mirkamali SS., "A multibiometric system based on the fusion of fingerprint, finger-vein, and finger-knuckle-print", Expert Systems with Applications, vol.176, pp.114687, August 2021.

[20] Chakladar DD, Kumar P, Roy PP, Dogra DP, Scheme E, Chang V., “A multimodal-Siamese Neural Network (mSNN) for person verification using signatures and EEG”, Information Fusion, vol.71, pp.17-27, July 2021.

[21] Muhammed A, Mhala NC, Pais AR., “A novel fingerprint template protection and fingerprint authentication scheme using visual secret sharing and super-resolution”, Multimedia Tools and Applications, vol.80, no.7, pp.10255-84, March 2021.

[22] Bidgoly AJ, Bidgoly HJ, Arezoumand Z., “Towards a universal and privacy preserving EEG-based authentication system”, Scientific Reports, vol.12, no.1, pp.1-2, February 2022.

[23] Görgel, P. and Ekşi, A., “Minutiae-Based Fingerprint Identification Using Gabor Wavelets and CNN Architecture”, Electrica, vol.21, no,3, 2021.

[24] Das D., “A minutia detection approach from direct gray-scale fingerprint image using hit-or-miss transformation”, InComputational intelligence in pattern recognition, pp.195-206, 2020.

[25] 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.

[26] AbdollahzadehB,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.

[27] 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

[28] Rasika Deshmukh and Pravin Yannawar “AVAO Enabled Deep Learning Based Person Authentication Using Fingerprint “ In proceedings of 2022 I st International Conference on Advances in Computer Vision and Artificial Intelligence Technologies, August 2022

[29] Kumar, A. and Sodhi, S.S., “Comparative analysis of gaussian filter, median filter and denoise autoenocoder”, In proceedings of 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 45-51, 2020.

[30] Mane, A.R., Biradar, S. and Shastri, R.K., “Review paper on feature extraction methods for EEG signal analysis”, Int. J. Emerg. Trend Eng. Basic Sci, vol.2, no.1, pp.545-552, 2015.

[31] Lee, S., Kim, J. and Lee, I., “Speech/audio signal classification using spectral flux pattern recognition”, In 2012 ieee workshop on signal processing systems, pp. 232-236, IEEE, October 2012.

[32] Shete, D.S., Patil, S.B. and Patil, S., “Zero crossing rate and Energy of the Speech Signal of Devanagari Script”, IOSR-JVSP, vol.4, no.1, pp.1-5, 2014.

[33] Castells, F., Laguna, P., Sörnmo, L., Bollmann, A. and Roig, J.M., “Principal component analysis in ECG signal processing”, EURASIP Journal on Advances in Signal Processing, pp.1-21, 2007.

[34] Li, J., Zhang, Z. and He, H., “Hierarchical convolutional neural networks for EEG-based emotion recognition”, Cognitive Computation, vol.10, no.2, pp.368-380, 2018.

[35] Aljalal, M., Djemal, R., AlSharabi, K. and Ibrahim, S., “Feature extraction of EEG based motor imagery using CSP based on logarithmic band power, entropy and energy”, In the proceedings of 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), pp. 1-6, IEEE, April 2018.

[36] CASIA Fingerprint Image Database

[37] EEG Dataset “Vision and Intelligent System Laboratory of Department of Computer Science and Information Technology, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad “

[38]Mirjalili, S., "SCA: a sine cosine algorithm for solving optimization problems," Knowledge-based systems, vol.96, pp.120-133, 2016.

[39] 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.