International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 15, No.1 (Feb-24)

https://dx.doi.org/10.12785/ijcds/150153

Deep Learning Based Person Authentication System using Fingerprint and Brain Wave

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*

Received 20 Nov. 2022, Revised 27 Dec. 2023, Accepted 27 Jan. 2024, Published 1 Feb. 2024

Abstract: Person authentication is the automated process of identifying individuals using computational techniques based on information stored in computer systems. This procedure encompasses critical aspects such as security, robustness, privacy, and prevention of forgery. Traditional biometric systems rely on a single mode of identification, which can fall short in providing high-security levels and are susceptible to noise and exploitation. To address these limitations, we introduce an optimization-enabled, deep learning-based multimodal person authentication system. In this innovative system, we leverage a combination of brainwave signals and fingerprint images to enhance security. To carry out person authentication on both modalities, we employ a Deep Maxout Network (DMN). The output from this network is fused using cosine similarity to yield the final authentication result. An important component of this system is the unique African vultures-Aquila Optimization (AVAO) algorithm, designed to update the weights of the DMN. The AVAO algorithm is constructed by enhancing the African Vulture Optimization Algorithm (AVOA) with the extended exploration capabilities of the Aquila Optimizer (AO). This fusion results in an algorithm that effectively fine-tunes the DMN for optimal performance. Our presented multimodal person authentication system demonstrates outstanding performance, achieving an accuracy of 0.926, sensitivity of 0.940, specificity of 0.928, and an F1-score of 0.921, underscoring its exceptional capabilities. An experimental study also showcases the superior performance of AVAO compared to existing techniques such as Multi-task EEG-based Authentication, Multi-model-based fusion, multi-biometric systems, and Visual secret sharing and super-resolution models, using a variety of metrics.
Keywords: Person authentication, multimodal, fingerprint, brain signal, Deep Max out Network.

1. INTRODUCTION

Daily technological advancements, security measures are evolving to keep pace with these innovations. Biometric recognition systems, a subject of active research, encompass various biological and behavioural features for user authentication. Biometrics, as a technology, involves measuring and analysing physical aspects of the human body to establish identity. In contexts demanding high-level security, traditional authentication methods like passwords, PINs, tokens, and smart cards have become outdated. Instead, biometric systems are gaining prominence by leveraging unique human physical or behavioural traits, which are challenging to replicate, steal, or counterfeit [1]. Behavioural biometrics, rooted in distinct human behaviours like signatures, keystrokes, and voice, coexist with physiological biometrics, which focus on identifying physical traits like the iris, face, or fingerprint. Both of these biometric types offer memorability, non-transferability, distinctiveness, and resilience to tampering or theft. However, uni-biometrics face certain challenges related to manufacturing and susceptibility to fake identities, posing significant security risks [2].

The need for novel authentication techniques that resist falsification is therefore evident [3]. Enhancing the security and robustness of authentication approaches can be achieved by adopting multimodal biometrics. Multimodal techniques combine two or more biometric traits to create a robust system that overcomes the limitations faced by unimodal systems, such as high error rates, vulnerability to spoof attacks, lack of universality, inflexibility, susceptibility to noise, and distinctions within the same class [4]. Fusion of biometric data enhances system flexibility and safeguards against the detrimental effects of noisy information, thereby enhancing security due to multiple authentication levels [5].

Hand-based authentication methods, known for their effectiveness in identifying veins, hand geometry, palm prints, and fingerprints, have been widely adopted for their reliability, simplicity, acceptance, and stability [6]. Fingerprint authentication, in particular, has gained widespread

E-mail address: rasika_deshmukh@yahoo.com, plyannawar.csit@bamu.ac.in

usage due to its high accuracy, affordability, and portability of fingerprint scanners, leading to numerous applications [7].

Recently, non-physical signals that are difficult to forge, such as brainwaves, have been explored for person authentication [3] Electroencephalograms (EEG) are used to record brainwave signals, where electrodes placed on the scalp measure voltage fluctuations. EEG authentication benefits from the uniqueness and resistance to spoofing attacks inherent in individual brainwave patterns [8]. The major advantages of utilizing EEG for authentication are that the brain signals or the electrical activity of each individual is varied, very difficult to manipulate or forge, and highly resistant to spoofing attacks [9]. Given the complexity of EEG signals and the growing reliance on data with high complexity, deep learning techniques have proven highly effective in various health-related fields, including public health, medical informatics, medical imaging, and bioinformatics [10]. Deep learning is especially advantageous in applications involving complex EEG signals, such as Brain-Computer Interfaces (BCI), emotion recognition, sleep studies, seizure detection, and insomnia diagnosis [11]. The varied influence of mental states, stress, and mood on EEG signals makes them extremely challenging to obtain through coercion or force [12]. Despite the advantages of fingerprint-based schemes, they remain vulnerable to presentation attacks (PAs) [13]. Authentication systems relying solely on EEG signals may suffer from instability and reduced accuracy. Additionally, EEG signals collected from the scalp often exhibit a weak Signal-to-Noise Ratio (SNR) and low resolution [14].

In this study, a multimodal authentication method is developed by combining brainwave and fingerprint signals, chosen for their reliability and widespread acceptance. After preprocessing both modalities, distinct features from brainwave signals and minutiae details from processed fingerprints are identified. The resulting data is simultaneously input into a Deep Maxout Network (DMN), fine-tuned using the developed AVAO algorithm. The outcomes are then combined using Cosine similarity. This paper makes significant contributions in the following areas:

1) The creation of a multimodal authentication system using two distinct modalities, namely brain waves and fingerprint images.
2) The development of an innovative AVAO algorithm designed to enhance person authentication by adjusting the weights of hidden neurons within the DMN.
3) To optimize classifier performance, the AVAO algorithm is crafted through a modification of the AVOA algorithm with the addition of AO.

This paper is structured in five sections following Section 1, The rest are as follows: Section 2 provides a comprehensive review of the existing literature on various multimodal authentication systems, while Section 3 presents an in-depth exploration of the newly introduced person authentication system. Section 4 offers a detailed analysis and discussion of the experimental results, and in Section 5, the paper concludes and provides some insights for the future.

2. LITERATURE REVIEW

Numerous research endeavors have explored the development of authentication systems utilizing multiple modalities. Within this research, we examine eight prominent studies, providing detailed insights into their methodologies. Wu Q et al. [15] introduced a multi-task EEG-based person authentication system, integrating eye blinking and EEG signals to form a multimodal approach. This system employed Rapid Serial Visual Presentation (RSVP) to acquire distinctive EEG signals. The method included morphological and Event-Related Potential (ERP) feature extraction, followed by score estimation using backpropagation neural networks and Convolutional Neural Networks (CNN). Although highly accurate and privacy-focused, it failed to address factors like noisy environments, heart rate, mood, and fatigue. To address the aforementioned limitations, Aleem S et al. [16] proposed a multi-modal system that leveraged a fusion strategy, combining facial and fingerprint modalities for person authentication. The technique utilized an alignment-based elastic algorithm for fingerprint matching and Extended Local Binary Patterns (ELBP) for facial feature extraction. Local non-negative matrix factorization was employed to reduce the ELBP feature space before fusion. While effective in reducing redundant information, it didn't enhance real-time application accuracy. In [17], Chanukya PS and Thivakaran TK introduced a highly accurate biometric image classification method utilizing fingerprint and ear modalities for person authentication. The method involved Modified Region Growing (MRG) algorithm for shape feature extraction from ear and fingerprint images, and Local Gabor Xor pattern (LGXP) for texture feature calculation. An optimal neural network, trained with the Firefly algorithm, was used for authentication, achieving high accuracy but lacking sensitivity enhancement. Addressing sensitivity concerns, Jijomon CM and Vinod AP presented an EEG-based biometric identification method in [18], incorporating auditory evoked potentials (AEPs). This method utilized frontal electrodes for AEP extraction, followed by feature extraction. Gated Recurrent Unit (GRU), Long Short-Term Memory (LSTM), and one-dimensional (1D)-CNN were employed for authentication, offering rapid data acquisition but struggling with the use of consumer-grade data collection devices. A cost-effective multi-biometric system by Khodadoust J et al. [19] integrated finger-knuckle-print, finger-vein, and fingerprint modalities using three different cameras for contactless capture. 2D images were transformed into 3D, matched with stored information, and underwent score-level fusion for user detection. This method achieved high accuracy and robustness but lacked performance optimization. In [20] introduced a more optimized approach as Chakladar D et al. developed a multimodal Siamese Neural Network (mSNN) to enhance user verification. Spatial and temporal features

of signatures and EEG signals were fused to create a feature space, processed by a Siamese network for user verification. The method was efficient in reducing forgery success but still wrestled with computational complexity. In [21], Muhammad A et al. introduced a secure fingerprint authentication technique employing fingerprint template protection through super-resolution (SR) and visual secret sharing (VSS). The technique encrypts fingerprint images during enrollment into multiple shares, stored separately. During authentication, a multiple-image super-resolution technique was utilized to reconstruct the secret fingerprint image from these shares, providing superior security and privacy but falling short in contrast enhancement of the reconstructed image. To circumvent fingerprint-related drawbacks, Bidgoly AJ et al. [22] introduced an EEG-based authentication scheme. Deep learning approaches were used to capture the EEG signal's fingerprint, preserving user privacy with a fingerprint function. The technique excelled in accuracy and privacy protection but missed out on exploiting deep learning techniques for performance enhancement.

2.1. CHALLENGES

The key challenges faced by current authentication techniques utilizing brain signals and fingerprints can be summarized as follows: In the case of the fusion-based multi-modal system introduced in [16], while it achieves higher recognition accuracy, there is a pressing need to make this approach more suitable for real-time applications. On the other hand, the multi-task EEG-based person authentication system presented in [15] addresses real-time applicability, enhancing system robustness and accuracy. However, a significant challenge lies in ensuring the practicality of this system through the use of commercially available EEG acquisition equipment. While the EEG-based authentication scheme in [22] attains high accuracy, it falls short in enhancing privacy and universality, posing a notable challenge for its broader adoption. The fingerprint template protection and authentication scheme in [21] successfully enhances privacy. However, a significant challenge remains in exploring improved data-hiding techniques to embed more information in the shares effectively. Automated authentication systems relying on fingerprints encounter security concerns due to the storage of data in databases, along with the inherent risk of forgery. In contrast, EEG-based authentication systems face issues of instability and low Signal-to-Noise Ratio (SNR), emphasizing the importance of developing a stable and swift response system.

3. PROPOSED DEEP LEARNING BASED PERSON AUTHENTICATION TECHNIQUE - AVAO

As discussed, this paper leverages two biometric modalities, namely brainwave signals and fingerprint images, to enhance the efficiency, privacy, and security of the authentication system. Figure 1 provides a visual representation of the introduced person authentication technique. The entire process involves the utilization of these two modalities: fingerprint images and brain signals. In the fingerprint authentication module, the process begins with data acquisition, followed by ridge enhancement during pre-processing. Subsequently, minutiae are detected using the Hit or Miss transform (HMT), and finally, person authentication is performed with the assistance of the DMN. Similarly, in the brain signal authentication module, brain signals are initially acquired from the dataset. These signals undergo pre-processing with a Gaussian filter, followed by feature extraction. After feature extraction, person authentication is carried out using the DMN. To fine-tune the DMN's performance, the devised AVAO algorithm is employed to adjust the weight factors. The authenticated results derived from both modules are fused together using cosine similarity to yield the final output. These processes are detailed in the following subsections.

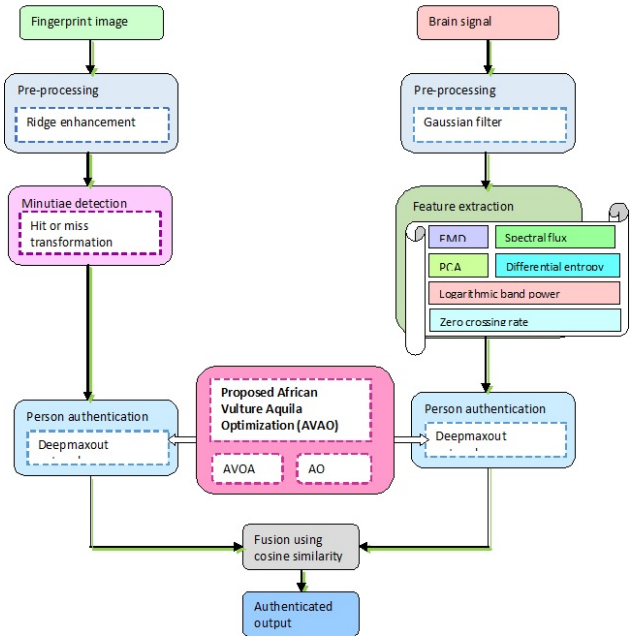

Figure 1. Schematic representation of the Proposed deep learning based person authentication technique-AVAO

3.1. Module for Fingerprint Authentication

The procedure for 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 to prepare the fingerprint image for authentication are listed below, along with the authentication process.

3.1.1. Acquiring Fingerprint images

Consider the following dataset that is represented as

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

where, fp_idenotes 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_iacquired 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, several 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. The 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 obtainedRid_i is then passed to the minutiae detection phase**.**

3.1.3. Minutiae Detection Phase

The ridge-enhanced image 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, to make it suitable for gray-scale images. Moreover, the GHMT is modified using the template matching idea., whose expression can be represented by,

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

Here, $R_i$specifies the gray-scale image, $l_f$denotes the foreground structuring element, and $l_b$is the background in whichl_f is present. The terms$\min^2$ $\max^2$denote the second minimum as well as the maximum values of the gray-level substitution of binary erosion and dilation operation. The terms $a_1$anda_2 pixels in the foreground 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 endpoint. The endpoints are identified by considering the inverted images, which are obtained by the following expression,

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

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

By utilizing 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,

$$B^j_{org} = Rid_i \otimes \left(l^{\theta_j}_f, l^{\theta_j}_b\right) \quad where \quad j \in \{1, 2, ..., 16\} \tag{5}$$

$$B^j_{inv} = Ridinv_i \otimes \left(l^{\theta_j}_f, l^{\theta_j}_b\right) \quad where \quad j \in \{1, 2, ..., 16\} \tag{6}$$

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^jsignifies 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 is above the threshold is chosen as the minutiae, which can be expressed as,

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

Here, $B^j_{ori/inv}(x, y)$gives the pixel intensity $(x, y)$of thej^{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 max-out layers connected consecutively, each of which contains hidden units that are divided into groups. Each layer employs the max-out 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,

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

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

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

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

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

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 $b_s$denotes the output of the max-out 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 the selection of the best vulture, estimation of the 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 program 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 behavior 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 algorithms. Following are the steps in the proposed AVAO algorithm.

i) Initialization

Let us assume there are avnumber of vultures. The first step is to initialize the population of vultures in the problem space which 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 the mean square error given by the following equation.

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

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.

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

Here, $K_1$and $K_2$are factors that have to be calculated ahead of the search operation and have 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 termJ_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 long distances in search of food when they are full and as a result, they have high energy. But in case they are hungry, they feel a shortage of energy from exploring long distances and they become aggressive and seek 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,

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

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

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, $\beta$is a parameter, whose value is fixed before the searching process, and the probability of exploration enhances with the value ofβ. The vultures hunt for food in varied spaces and the algorithm is in the 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 for food is highly challenging and the vultures have to perform scrutiny of their surroundings for a long period over vast distances. Random areas are examined by the usage of two approaches. An arbitrary parameterI_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.

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

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

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

Here, $R(i+1)$denotes the vulture position vector, Zrepresents the coefficient vector. rd_I, $rd_2$and $rd_3$are random variables

in the range [0,1]. The terms*upb lwb*denote 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, $T = 1$

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

Consider,

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

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

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

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),

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

$$\begin{aligned} &R(i+1) + R(i+1) \times SR \\ &= W(i)\left[1 + Z \times SR + \left(1 - \tfrac{n}{N} - rnd\right) \times SR\right] \end{aligned} \tag{33}$$

$$\begin{aligned} &R(i+1)[1 + SR] \\ &= W(i)\left[1 + \left(Z + \left(1 - \tfrac{n}{N}\right) - rnd\right) \times SR\right] \end{aligned} \tag{34}$$

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

Here, Ndenotes the number of samples and $rnd$is a arbitrary number.

v) Exploitation: phase 1

Exploitation is performed in two phases depending on the valueSR. If the value$|SR|$ lies between 0.5 and 1, then phase 1 is executed. The first phase comprises two techniques, such as rotating flight as well as siege-fight. A parameter $I_2$is utilized 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 a rotating flight approach is implemented, else a siege fight 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 modeling the spiral movement, and a spiral motion is formed among the best two vultures and the other vultures and this can be modeled as,

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

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

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

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, a 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,

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

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

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

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

(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 modeled as,

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

Here, $E(t)$specifies the distance between a vulture and any one 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 the 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 high-efficiency in-person authentication owing to their significant features, like the impossibility of retrieving signals by force or coercion and high resistance to spoofing attacks. The raw brain signals have to be processed before they can be utilized for authentication. These processes along with the authentication are detailed in the ensuing subsections.

3.2.1. Brain Signal Acquisition

Consider a dataset Brcontaining a total ofn_b brainwave signals, which is given by the following expression,

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

where, br_jrepresents thej^{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,

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

Here, μ, σsignifies the mean and standard deviation of the distribution, and $z$represents the signal. Consider the output obtained to be denotedg_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 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 analyzed efficiently by using the time-frequency domain. Therefore, 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 patterns named Intrinsic Mode Function (IMF) present in the time series data. EMD is utilized 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 the application of the Hilbert-Huang Transform (HHT) for obtaining the initial sequence of the instantaneous frequency spectrum. The EMD thus obtained is denoted asf_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].

$$Y[p] = FFT[g_i[q]] \quad p = 1, 2, ..P \quad q = 1, 2, .., P \quad (47)$$

$$\hat{Y}[p] = \frac{Y[p]}{\arg\max[Y[p]]} \quad (48)$$

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

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 the zero crossing rate. The zero crossing rate can be given by the following expression,

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

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

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

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

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

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 the majority of the variability is contained in the first components. These components are uncorrelated mutually to each other and are extracted as a 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,

$$f_4 = \varphi^T g_i \tag{53}$$

where, φ^T denotes the orthogonal transformation.

v) Differential entropy

Differential entropy (DE) [34] is a feature that is used to evaluate the complex nature of discrete random variables. 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 and extracting the important information in the raw brain signal, and is expressed as,

$$f_5 = \frac{1}{2} \log 2\pi\varepsilon{\sigma_1}^2 \tag{54}$$

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 contain 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 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 concerning the fingerprint image in training and α_1 refers to the target concerning the fingerprint image dataset. ${L^t}_{br}$ Denote the output of DMN concerning the brain signal in training and α_2 refers to the target concerning 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 similar-

ity 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 a detailed analysis of the proposed method.

4.1. Experimental set up

The innovative AVAO-enabled Deep learning approach for the efficient authentication of individuals utilizing fingerprint and brainwave signals is implemented in the 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 employed in this study were sourced from the CASIA Fingerprint Image Database Version 5.0 [36], which contains images obtained from 500 individuals. A total of 40 images were captured from each individual, encompassing all eight fingers. Consequently, the database contains 20,000 fingerprint images stored as 8-bit Gray-level BMP files. These images were captured using URU4000 fingerprint sensors, with a resolution of 328 x 356 pixels. The brainwave dataset used in this research was obtained from the Vision and Intelligent System Laboratory of the Department of Computer Science and Information Technology at Dr. Babasaheb Ambedkar Marathwada University, Aurangabad [37]. This dataset comprises EEG signal recordings from 10 subjects, including 7 males and 3 females, all falling within the age group of 20-25. The total database size amounts to 12 (recordings) x 10 (subjects) x 10 (samples) for a total of 1200 samples.

4.3. Performance measures

The effectiveness of the proposed AVAO-enabled Deep Learning approach is assessed through several efficiency metrics, including accuracy, sensitivity, specificity, F1 score, and ROC (Receiver Operating Characteristic). Subsequent subsections will delve deeper into the details of these 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 tpindicate the number of genuine users who are authenticated correctly, tnspecify the number of illegal users classified as such, fprepresent the number of non-authorized users who are detected as authorized, and fnsignify the count of authorized 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 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 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

$$F1Score = 2 * (Recall * Precision)/(Recall + Precision) \tag{65}$$

4.3.5 ROC

A 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. A 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.

4.5. Comparative methodologies

This section involves the assessment of the performance of the proposed AVAO-enabled deep learning-based person authentication system. It is evaluated by means of a comparative analysis with existing techniques, including Multi-task EEG-based Authentication [15], Multi-model-based fusion [16], Multi-biometric systems [19], and Visual secret sharing and super-resolution models [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.

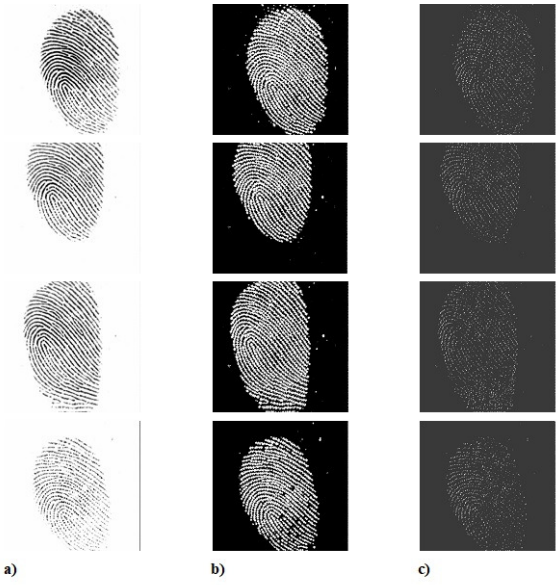

Figure 2. a) depicts the input fingerprint images, 2 b) shows the pre-processed images, figure 2c) illustrates the minutiae detection

a) Analysis based on Fingerprint Image

Figure 3 presents an evaluation based on fingerprint images for various proportions of training data. In Figure 3a, the assessment focuses on accuracy. The proposed person authentication system using fingerprints achieved an accuracy of 0.896, while existing technologies, including multi-task EEG-based authentication, multi-biometric systems, visual secret sharing, and super-resolution models, and multi-model-based fusion, attained accuracy values of 0.718, 0.758, 0.819, and 0.868, respectively, when trained on 60% of the data. This indicates that the proposed multimodal authentication system outperforms the existing methods by 19.86%, 15.37%, 8.60%, and 3.13%. In Figure 3b, the evaluation focuses on specificity. The specificity values for the existing multi-task EEG-based authentication, multi-biometric systems, visual secret sharing and super-resolution models, and multi-model-based fusion, as well as the proposed AVAO-optimized multimodal person authentication scheme, are 0.720, 0.760, 0.817, 0.878, and 0.896, respectively, when trained on 70% of the data. This demonstrates that the proposed AVAO-optimized multimodal person authentication scheme exhibits performance improvements of 19.70%, 15.25%, 8.81%, and 2.11% compared to the prevailing methods. Figure 3c displays the analysis of the techniques concerning sensitivity. The existing methods, such as multi-task EEG-based authentication, multi-biometric systems, visual secret sharing and super-resolution models, and multi-model-based fusion, achieved sensitivity values of 0.813, 0.829, 0.875, and 0.885, while the proposed AVAO-optimized multimodal person authentication scheme attained a sensitivity value of 0.925 when trained on 80% of the data. Consequently, the devised technique demonstrates an enhancement in performance of 12.15%, 10.45%, 5.43%, and 4.32%. In Figure 3d, the evaluation centers on the F1-score. The F1-score values for the existing multi-task EEG-based authentication, multi-biometric systems, visual secret sharing and super-resolution models, and multi-model-based fusion, as well as the proposed AVAO-optimized multimodal person authentication scheme, are 0.815, 0.836, 0.853, 0.877, and 0.901, respectively, when trained on 70% of the data. This reveals that the proposed AVAO-optimized multimodal person authentication scheme demonstrates performance improvements of 10.5%, 7.75%, 5.62%, and 2.73% over the prevailing methods. Finally, in Figure 3e, the analysis of the techniques focuses on the Receiver Operating Characteristic (ROC).

b) Analysis based on brain signal

In this section, we assess person authentication schemes utilizing brain signals across various levels of training data, as depicted in Figure 4. The assessment encompasses accuracy, specificity, sensitivity, and F1-score, each showcased in Figure 4a, Figure 4b, Figure 4c, and Figure 4d, respectively. Additionally, the evaluation of the ROC curve for these techniques is presented in Figure 4e. For the proposed AVAO-optimized multimodal person authentication scheme, when 80% of the training data is considered, an accuracy of 0.918 is achieved. In contrast, existing techniques such as multi-task EEG-based authentication, multi-biometric systems, visual secret sharing and super-resolution models, and multi-model-based fusion yield accuracy values of 0.772, 0.801, 0.872, and 0.894, respectively. This demonstrates a superiority of 15.89%, 12.71%, 4.91%, and 2.53% for the proposed approach. At a 70% training data level, the prevailing methods, including multi-task EEG-based authentication, multi-biometric systems, visual secret sharing and super-resolution models, and multi-model-based fusion, produce specificity values of 0.730, 0.775, 0.858, and 0.887, while the proposed AVAO-optimized multimodal person authentication scheme achieves a specificity of 0.910, outperforming the existing techniques by 19.79%, 14.88%, 5.72%, and 2.57%.

For 60% of the training data, the devised AVAO-optimized multimodal person authentication scheme attains a sensitivity value of 0.915. In comparison, existing techniques reach sensitivity values of 0.804 for multi-task EEG-based authentication, 0.808 for the multi-biometric system, 0.851 for visual secret sharing and super-resolution models, and 0.879 for multi-model-based fusion. This highlights performance enhancements of 12.13%, 11.72%, 7.04%, and 3.93% for the proposed method over the existing authentication techniques. Finally, with a training data percentage of 70, prevailing methods return F1-score values of 0.818, 0.836, 0.865, and 0.871, while the proposed AVAO-optimized multimodal person authentication scheme achieves an F1-score of 0.901. This signifies a superiority

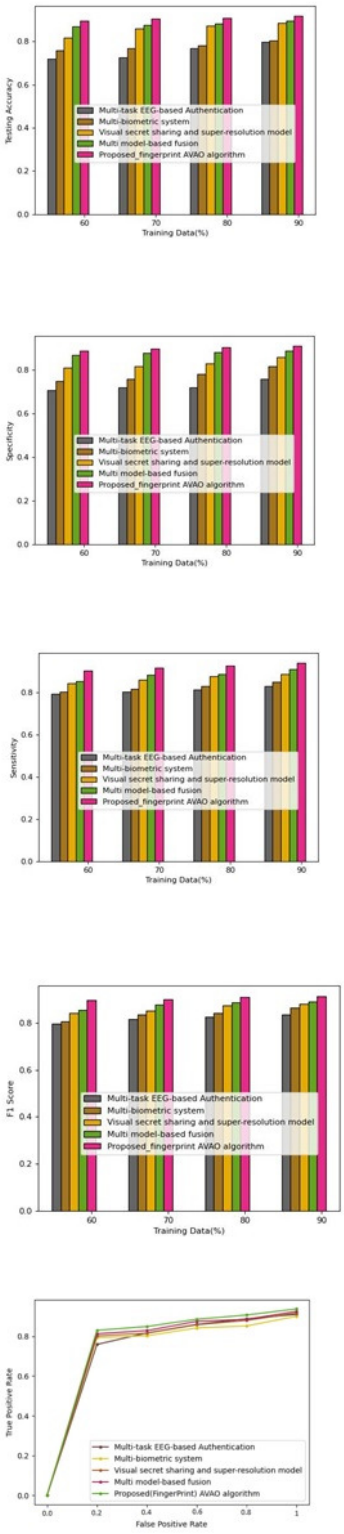

Figure 3. Assessment of the techniques using a) accuracy b) sensitivity c) specificity for varying training data d) F1-score e) roc

of 10.14%, 7.75%, 4.16%, and 3.44% for the proposed approach over the existing techniques.

c) Analysis based on Multimodalities

Figure 5 illustrates the evaluation of multimodal authentication schemes with variations in the percentages of training data. The assessment of these approaches in terms of accuracy is presented in Figure 5a. The devised AVAO-optimized person authentication scheme achieves an accuracy of 0.904, whereas existing authentication techniques, including multi-task EEG-based authentication, multi-biometric systems, visual secret sharing and super-resolution models, and multi-model-based fusion, attain accuracy values of 0.723, 0.758, 0.851, and 0.868, respectively, with 60% of training data. Consequently, the proposed technique demonstrates a performance improvement of 20.09%, 16.18%, 5.90%, and 4.05% over the existing methods.

In Figure 5b, the evaluation based on specificity is depicted. With 70% of training data considered, existing authentication techniques, such as multi-task EEG-based authentication, multi-biometric systems, visual secret sharing and super-resolution models, and multi-model-based fusion, produce specificity values of 0.720, 0.775, 0.817, and 0.857, while the proposed AVAO-optimized person authentication scheme achieves a specificity of 0.896. This highlights an improved performance of 19.70%, 13.59%, 8.81%, and 4.45% for the proposed scheme over the prevailing ones.

Figure 5c presents an analysis focusing on sensitivity. The introduced AVAO-optimized person authentication technique computes a sensitivity of 0.929, while the prevailing approaches measure sensitivity values at 0.828 for multi-task EEG-based authentication, 0.879 for the multi-biometric system, 0.883 for visual secret sharing and super-resolution models, and 0.885 for multi-model-based fusion when 80% training data is employed. This indicates an enhanced performance of 10.88%, 5.40%, 4.92%, and 4.68% for the proposed technique over the existing methods.

In Figure 5d, the analysis based on the F1-score is displayed. The introduced AVAO-optimized person authentication technique computes an F1-score of 0.919, while the prevailing approaches measure F1-score values at 0.883 for multi-task EEG-based authentication, 0.893 for the multi-biometric system, 0.901 for visual secret sharing and super-resolution models, and 0.902 for multi-model-based fusion when 90% training data is used. This showcases an improved performance of 4.07%, 2.9%, 1.9%, and 1.8% for the proposed technique over the prevailing ones.

4.7. Comparative Algorithms

The performance of the developed AVAO algorithm is evaluated in comparison to various existing algorithms, including the Sine Cosine Algorithm (SCA) + DMN [37], Sail Fish Optimization (SFO) + DMN [38], AO + DMN [27], and AVOA + DMN [26].

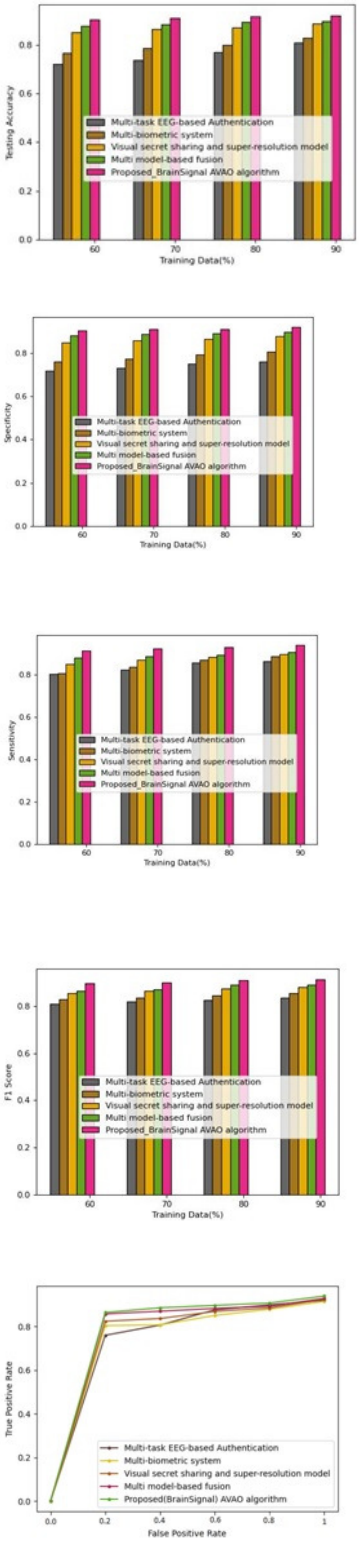

Figure 4. Assessment of the techniques using a) accuracy b) sensitivity c) specificity for varying training data d) F1-score e) ROC curve

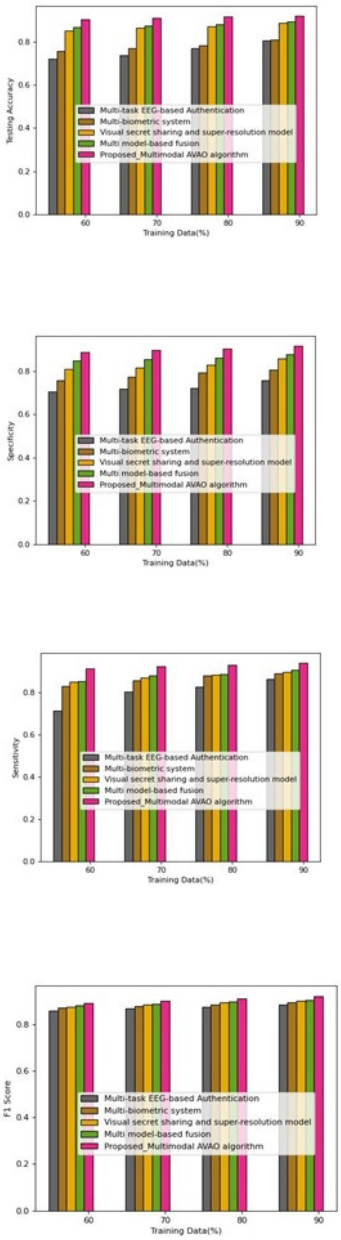

Figure 5. Assessment of the techniques using a) accuracy, b) sensitivity, c) specificity for varying training data, d) F1-score

4.8. Algorithmic Analysis

The performance of the proposed AVAO algorithm is assessed using fingerprint images, brain signals, and multimodalities across various population sizes, focusing on metrics such as accuracy, specificity, sensitivity, and F1 score. Figure 6 provides an analysis of the different algorithms utilizing fingerprint images. In Figure 6a, the algorithms are evaluated for accuracy with varying population sizes. The existing algorithms, namely SCA+DMN, SFO+DMN, AO+DMN, and AVOA+DMN, achieve accuracies of 0.887, 0.892, 0.895, and 0.900, while the proposed AVAO+DMN algorithm attains an accuracy of 0.902 with a population size of 5. This results in a performance improvement of 1.67%, 1.09%, 0.70%, and 0.23% by the proposed algorithm.

In Figure 6b, the evaluation based on specificity is presented. With a population size of 10, the developed AVAO+DMN algorithm yields a specificity of 0.918, whereas the prevailing SCA+DMN, SFO+DMN, AO+DMN, and AVOA+DMN algorithms achieve specificity values of 0.898, 0.900, 0.900, and 0.905. This indicates a performance enhancement of 2.13%, 1.94%, 1.91%, and 1.34% with the proposed algorithm.

Figure 6c illustrates the analysis based on sensitivity. The values of sensitivity obtained by the existing algorithms, SCA+DMN, SFO+DMN, AO+DMN, and AVOA+DMN, along with the proposed AVAO+DMN algorithm, are 0.906, 0.908, 0.912, 0.919, and 0.927, respectively, for a population size of 15. This shows that the proposed algorithm achieves a higher sensitivity value compared to the existing methods by 2.22%, 1.95%, 1.52%, and 0.83%. In Figure 6d, the evaluation based on the F1-score is depicted. With a population size of 20, the developed AVAO+DMN algorithm computes an F1-score of 0.912, while the prevailing SCA+DMN, SFO+DMN, AO+DMN, and AVOA+DMN algorithms achieve F1-score values of 0.893, 0.898, 0.904, and 0.907, respectively. This demonstrates a performance improvement of 2.12%, 1.6%, 0.8%, and 0.5% for the proposed algorithm over the existing ones.

Figure 7 presents the assessment of the algorithms using brainwave signals for different population sizes. In Figure 7a, the accuracy assessment is displayed. The developed AVAO+DMN algorithm achieves an accuracy of 0.908, while the existing SCA+DMN, SFO+DMN, AO+DMN, and AVOA+DMN algorithms attain accuracies of 0.899, 0.902, 0.901, and 0.907 when the population size is 10. This indicates that the AVAO+DMN algorithm outperforms the conventional algorithms with an improved accuracy of 1.06%, 0.75%, 0.77%, and 0.10%.

Figure 7b presents the evaluation based on specificity. The proposed AVAO+DMN algorithm demonstrates superior performance, achieving a specificity value of 0.918. In contrast, the prevailing algorithms, SCA+DMN, SFO+DMN, AO+DMN, and AVOA+DMN, achieve lower specificity values of 0.906, 0.908, 0.913, and 0.916 when the population size is 15. The AVAO+DMN algorithm surpasses the existing ones with a performance improvement of 1.27%, 1%, 0.51%, and 0.19%.

In Figure 7c, the sensitivity-based evaluation of the algorithms is depicted. When the population size is 5, sensitivity values are calculated for various algorithms, including SCA+DMN, SFO+DMN, AO+DMN, AVOA+DMN, and the AVAO+DMN algorithm, resulting in values of 0.901, 0.901, 0.903, 0.910, and 0.911. The AVAO+DMN algorithm achieves higher sensitivity compared to the prevailing algorithms, with an improvement of 1.10%, 1.02%, 0.83%, and 0.08%.

Figure 7d presents the evaluation based on the F1-score. For a population size of 15, F1-score values are calculated for various algorithms, including SCA+DMN, SFO+DMN, AO+DMN, AVOA+DMN, and the AVAO+DMN algorithm, resulting in values of 0.891, 0.901, 0.904, 0.907, and 0.916, respectively. The AVAO+DMN algorithm outperforms the conventional algorithms with an improved F1-score of 2.8%, 1.6%, 1.3%, and 0.99%.

Figure 8 illustrates the evaluation of algorithms based on different population sizes and modalities. In Figure 8a, the assessment of accuracy is shown. The existing SCA+DMN, SFO+DMN, AO+DMN, and AVOA+DMN algorithms achieve accuracy values of 0.906, 0.909, 0.910, and 0.914 when the population size is 15. In contrast, the proposed AVAO+DMN algorithm attains a higher accuracy of 0.921, resulting in an enhanced performance of 1.65%, 1.34%, 1.15%, and 0.80%.

Figure 8b presents the analysis of specificity. When the population size is 5, the proposed AVAO algorithm achieves a specificity of 0.913, surpassing 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 specificity values of only 0.882, 0.890, 0.900, and 0.906.

In Figure 8c, the analysis of sensitivity is depicted. For a population size of 10, the existing algorithms, including SCA+DMN, SFO+DMN, AO+DMN, and AVOA+DMN, achieve sensitivity values of 0.903, 0.906, 0.907, and 0.913, while the introduced AVAO+DMN algorithm calculates a sensitivity of 0.928. This demonstrates an enhanced performance of 2.67%, 2.35%, 2.17%, and 1.60% by the proposed algorithm.

Figure 8d shows the analysis of the F1-score. For a population size of 20, the existing algorithms, including SCA+DMN, SFO+DMN, AO+DMN, and AVOA+DMN, achieve F1-score values of 0.902, 0.909, 0.915, and 0.918. In comparison, the introduced AVAO+DMN algorithm calculates an F1-score of 0.921, demonstrating an enhanced

performance of 2.1%, 1.3%, 0.65%, and 0.32% by the proposed algorithm.

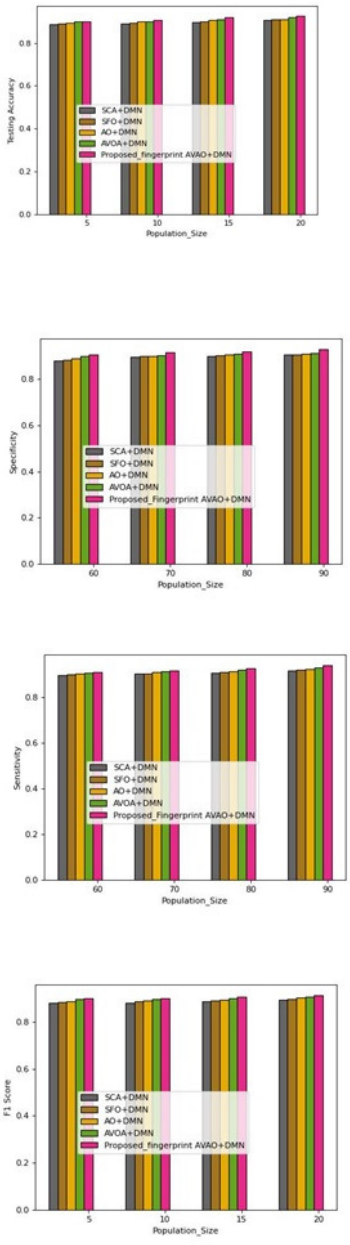

Figure 6. Algorithmic evaluation using fingerprint image based on a) accuracy b) sensitivity c)specificity and d) F1-score.

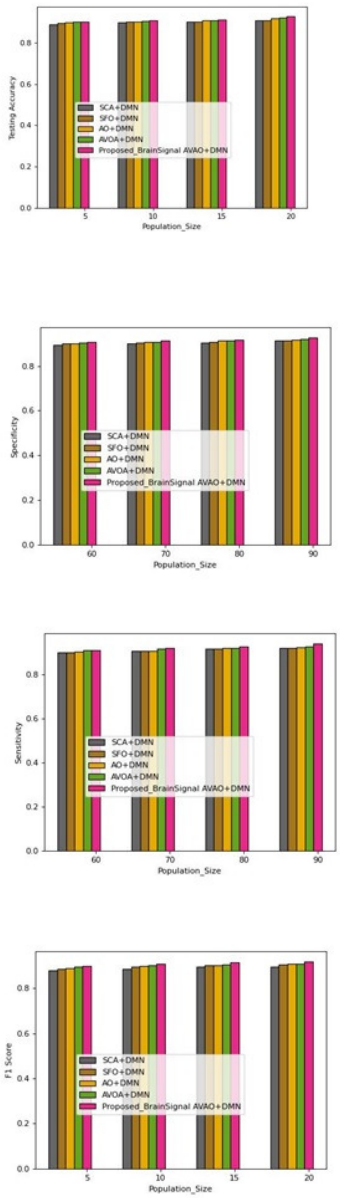

Figure 7. Algorithmic evaluation using brain signals based on a specificity for varying training data.

4.9. Comparative Discussion

In this section, we compare the AVAO-optimized multimodal person authentication scheme developed in this study with existing techniques using various metrics. Table 1 provides a comprehensive list of these metrics, along with the corresponding values obtained by both existing and introduced authentication methods, which incorporate fingerprint images, brain signals, and multimodalities. These values are derived from an evaluation involving 90% of the training data.

From the table, it is evident that the AVAO-optimized multimodal person authentication scheme, particularly for brain signal modality, achieves exceptional performance, with maximum values of accuracy (0.920), specificity (0.920), sensitivity (0.940), and F1-score (0.912). The use of two distinct biometric modalities within the authentication process contributes to the high accuracy. Furthermore, the

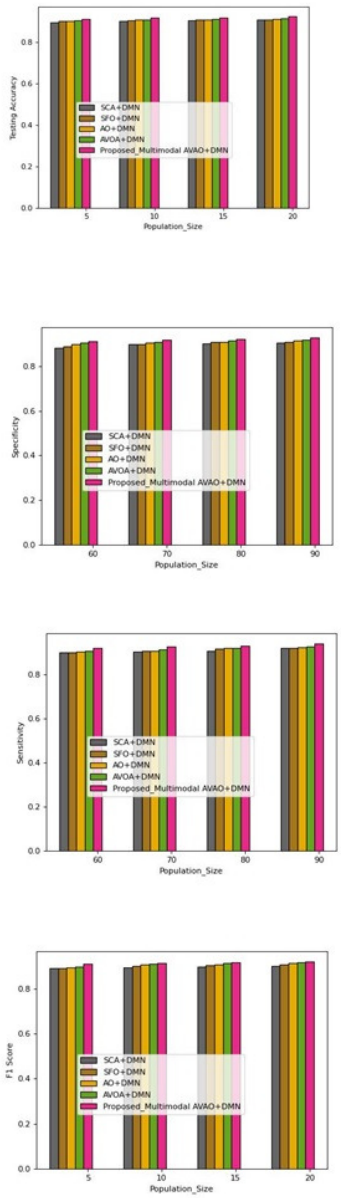

Figure 8. Algorithmic evaluation using multimodalities based on a sensitivity.

utilization of the Deep Multimodal Network (DMN) for classification enhances specificity and the incorporation of the proposed AVAO algorithm for optimization results in heightened sensitivity.

Table II presents a comparative analysis of algorithms. In this evaluation, the devised AVAO+DMN algorithm is assessed in terms of accuracy, specificity, and sensitivity, and it is compared to the existing SCA+DMN, SFO+DMN, AO+DMN, and AVOA+DMN algorithms. The metric values in this table are associated with a population size of 80.

TABLE I. COMPARATIVE ASSESSMENTS OF THE VARIOUS PERSON AUTHENTICATION SCHEMES

Modalities	Metrics	Multi-task EEG-based authentication	Multi-biometric system	Visual secret sharing and super-resolution model	Multi model-based fusion	Proposed-AVAO 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

From the table, it is evident that the devised AVAO+DMN algorithm has achieved the highest values for accuracy (0.929), sensitivity (0.930), specificity (0.940), and F1-score (0.921).

TABLE II. 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

This paper introduces a robust multimodal person authentication method that leverages the security of brain signals and the simplicity of fingerprint images. It utilizes a Deep Multimodal Network (DMN) to identify users, preceded by preprocessing for both brain signals and fingerprint images. User authentication is performed by combining the extracted features from both modalities and the identified minutiae points from DMNs. An innovative AVAO algorithm, inspired by the African vulture (AVOA) and the Aquila (AO), is developed to optimize the DMN weight factor. The final authentication output is achieved through cosine similarity-based fusion of DMN outputs, resulting in impressive performance metrics with an accuracy of 0.926, specificity of 0.928, sensitivity of 0.940, and an F1-score of 0.921. Future work may include exploring other deep learning networks and more efficient optimization algorithms to enhance the authentication scheme's performance.

ACKNOWLEDGEMENT

Authors would like to thank authorities of Department of Computer Science and Information Technology, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad for their infrastructure and facility support to carryout presented research work.

REFERENCES

[1] M. M. Ali, P. L. Yannawar, and A. Gaikwad, "Multi-algorithm of palmprint recognition system based on fusion of local binary pattern and two-dimensional locality preserving projection," *Procedia computer science*, vol. 115, pp. 482–492, 2017.

[2] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, "Continuous and transparent multimodal authentication: reviewing the state of the art," *Cluster Computing*, vol. 19, pp. 455–474, 2016.

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

[4] Z. A. S. A. Momin *et al.*, "Security of multimodal biometric systems against spoof attacks," 2012.

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

[6] A. S. Tarawneh, A. B. Hassanat, E. Alkafaween, B. Sarayrah, S. Mnasri, G. A. Altarawneh, M. Alrashidi, M. Alghamdi, and A. Almuhaimeed, "Deepknuckle: Deep learning for finger knuckle print recognition," *Electronics*, vol. 11, no. 4, p. 513, 2022.

[7] R. M. Jomaa, M. S. Islam, H. Mathkour, and S. Al-Ahmadi, "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*, vol. 34, no. 8, pp. 5132–5143, 2022.

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

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

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

[11] T. Wilaiprasitporn, A. Ditthapron, K. Matchaparn, T. Tongbuasirilai, N. Banluesombatkul, and E. Chuangsuwanich, "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] Q. Gui, Z. Jin, and W. Xu, "Exploring eeg-based biometrics for user identification and authentication," in *2014 IEEE Signal Processing in Medicine and Biology Symposium (SPMB)*. IEEE, 2014, pp. 1–6.

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

[14] A. Rahman, M. E. Chowdhury, A. Khandakar, S. Kiranyaz, K. S. Zaman, M. B. I. Reaz, M. T. Islam, M. Ezeddin, and M. A. Kadir, "Multimodal eeg and keystroke dynamics based biometric system using machine learning algorithms," *IEEE Access*, vol. 9, pp. 94 625–94 643, 2021.

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

[16] S. Aleem, P. Yang, S. Masood, P. Li, and B. Sheng, "An accurate multi-modal biometric identification system for person identification via fusion of face and finger print," *World Wide Web*, vol. 23, pp. 1299–1317, 2020.

[17] P. S. Chanukya and T. Thivakaran, "Multimodal biometric cryptosystem for human authentication using fingerprint and ear," *Multimedia Tools and Applications*, vol. 79, pp. 659–673, 2020.

[18] C. Jijomon and A. P. Vinod, "Person-identification using familiar-name auditory evoked potentials from frontal eeg electrodes," *Biomedical Signal Processing and Control*, vol. 68, p. 102739, 2021.

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

[20] D. D. Chakladar, P. Kumar, P. P. Roy, D. P. Dogra, E. Scheme, and V. Chang, "A multimodal-siamese neural network (msnn) for person verification using signatures and eeg," *Information Fusion*, vol. 71, pp. 17–27, 2021.

[21] A. Muhammed, N. C. Mhala, and A. R. Pais, "A novel fingerprint template protection and fingerprint authentication scheme using visual secret sharing and super-resolution," *Multimedia Tools and Applications*, vol. 80, pp. 10 255–10 284, 2021.

[22] A. J. Bidgoly, H. J. Bidgoly, and Z. Arezoumand, "Towards a universal and privacy preserving eeg-based authentication system," *Scientific Reports*, vol. 12, no. 1, p. 2531, 2022.

[23] P. Görgel and A. Ekşi, "Minutiae-based fingerprint identification

using gabor wavelets and cnn architecture," *Electrica*, vol. 21, no. 3, pp. 480–490, 2021.

[24] D. Das, "A minutia detection approach from direct gray-scale fingerprint image using hit-or-miss transformation," in *Computational Intelligence in Pattern Recognition: Proceedings of CIPR 2019*. Springer, 2020, pp. 195–206.

[25] W. Sun, F. Su, and L. Wang, "Improving deep neural networks with multi-layer maxout networks and a novel initialization method," *Neurocomputing*, vol. 278, pp. 34–40, 2018.

[26] B. Abdollahzadeh, F. S. Gharehchopogh, and S. Mirjalili, "African vultures optimization algorithm: A new nature-inspired metaheuristic algorithm for global optimization problems," *Computers & Industrial Engineering*, vol. 158, p. 107408, 2021.

[27] L. Abualigah, D. Yousri, M. Abd Elaziz, A. A. Ewees, M. A. Al-Qaness, and A. H. Gandomi, "Aquila optimizer: a novel meta-heuristic optimization algorithm," *Computers & Industrial Engineering*, vol. 157, p. 107250, 2021.

[28] P. L. Yannawar *et al.*, "p1: An optimization enabled deep learning based multimodal person authentication system," *International Journal of Digital Technologies*, vol. 1, no. 1, 2022.

[29] A. Kumar and S. S. Sodhi, "Comparative analysis of gaussian filter, median filter and denoise autoenocoder," in *2020 7th International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2020, pp. 45–51.

[30] A. R. Mane, S. Biradar, and R. Shastri, "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] S. Lee, J. Kim, and I. Lee, "Speech/audio signal classification using spectral flux pattern recognition," in *2012 ieee workshop on signal processing systems*. IEEE, 2012, pp. 232–236.

[32] D. Shete, S. Patil, and S. Patil, "Zero crossing rate and energy of the speech signal of devanagari script," *IOSR-JVSP*, vol. 4, no. 1, pp. 1–5, 2014.

[33] F. Castells, P. Laguna, L. Sörnmo, A. Bollmann, and J. M. Roig, "Principal component analysis in ecg signal processing," *EURASIP Journal on Advances in Signal Processing*, vol. 2007, pp. 1–21, 2007.

[34] J. Li, Z. Zhang, and H. He, "Hierarchical convolutional neural networks for eeg-based emotion recognition," *Cognitive Computation*, vol. 10, pp. 368–380, 2018.

[35] M. Aljalal, R. Djemal, K. AlSharabi, and S. Ibrahim, "Feature extraction of eeg based motor imagery using csp based on logarithmic band power, entropy and energy," in *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*. IEEE, 2018, pp. 1–6.

[36] "Casia fingerprint image database."

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

[38] S. Shadravan, H. R. Naji, and V. K. Bardsiri, "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.

Rasika Deshmukh was born in 1979. She received her B.Sc Computer Science from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad in June 1999 , and M.Sc. Computer Science from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad in June 2001.She has published and presented one paper in the 3rd Biennial International Conference on Recent Trends in Image Processing and Pattern Recognition. Recently she is working as Assistant Professor in the department of computer science at Fergusson College (Autonomous), Pune.

Pravin Yannawar born in 1979, holds an impressive academic background. He earned his B.Sc. in Computer Science from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, in June 1999. Following that, he completed his M.Sc. in Computer Science from the same institution in June 2001. In March 2011, he attained his Ph.D. in Computer Science, also from the Department of Computer Science and Information Technology at Dr. Babasaheb Ambedkar Marathwada University, Aurangabad. Dr. Yannawar is a respected figure in academia, actively contributing to the scholarly community. He serves as a reviewer and editor for various international journals, highlighting his commitment to academic excellence. His body of work includes numerous publications available in Elsevier and Springer Conference Proceedings as book chapters, as well as over 30+ peer-reviewed journal articles. Furthermore, he has authored more than six books, showcasing his expertise in the field. Currently, Dr. Pravin Yannawar holds the position of Associate Professor within the Vision and Intelligent System Lab at the Department of Computer Science and Information Technology, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad. His substantial contributions to the field of Computer Science and Information Technology continue to influence and advance the academic community.