Optimizing dual modal biometric authentication: hybrid HPO-ANFIS and HPO-CNN framework

Sandeep Pratap Singh, Shamik Tiwari
School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India

Article Info

Article history:

Received Oct 18, 2023
Revised Nov 4, 2023
Accepted Nov 30, 2023

Keywords:

ANFIS
Biometric authentication
CNN
Hyperparameter optimization
Multimodal authentication

ABSTRACT

In the realm of secure data access, biometric authentication frameworks are vital. This work proposes a hybrid model, with a 90% confidence interval, that combines "hyperparameter optimization-adaptive neuro-fuzzy inference system (HPO-ANFIS)" parallel and "hyperparameter optimization-convolutional neural network (HPO-CNN)" sequential techniques. This approach addresses challenges in feature selection, hyperparameter optimization (HPO), and classification in dual multimodal biometric authentication. HPO-ANFIS optimizes feature selection, enhancing discriminative abilities, resulting in improved accuracy and reduced false acceptance and rejection rates in the parallel modal architecture. Meanwhile, HPO-CNN focuses on optimizing network designs and parameters in the sequential modal architecture. The hybrid model's 90% confidence interval ensures accurate and statistically significant performance evaluation, enhancing overall system accuracy, precision, recall, F1 score, and specificity. Through rigorous analysis and comparison, the hybrid model surpasses existing approaches across critical criteria, providing an advanced solution for secure and accurate biometric authentication.

Corresponding Author:

Sandeep Pratap Singh
School of Computer Science, University of Petroleum and Energy Studies
Dehradun 248007, India
Email: sandeep102209@gmail.com

1. INTRODUCTION

The issue of providing authorized owners with safe and simple access to information and solutions for specific identification processes is referred to as identity and access management. The primary objective for determining the individual's identity is the execution of the safeguarded authentication component. Private identifying components such as PINs, keys, smart cards, credentials, and tokens are examples of conventionally used private identifying components that can be cracked, stolen, copied, and published. Biometrics-based identification is required to avoid the drawbacks [1], [2]. Variations within subcategories influence non-universality, voice, and mock strikes.

Biometric examinations utilizing unimodal and multimodal modalities depend on the utilization of one sign or trademark in unimodal exploration while applying many signs and PT in multimodal studies [3], [4]. Electroencephalograms, electrocardiograms (ECG), phonocardiograms, electrooculography, electromyograms, photo-plethysmograms, palmprints, periocular, fingerprints, and electrooculography are just a few of the many signals and characteristics that have been independently examined (monomodal authentication or identification). Speech, knee acceleration (knA), finger knuckle print (FKP), finger vein, tongue, iris, face, ear, lips, and eyes, and laser doppler vibrometers (LDV) other studies that combine or fuse multiple signals with various features lend credence to the concept of multimodal identification or recognition [5], [6]. Human interaction, which is regarded as a natural multimodal process [7], exhibits profound physiological and psychological expressions. While monomodal biometric systems, which only compare one characteristic, have been used in the past for validation, these stochastic models are just as effective when vibration, computational burden, and signal acquisition device efficiency are present. Two or more traits or signals are combined in multimodal biometric systems.

To address the downsides of the monomodal biometric framework, the multimodal biometric framework has been laid out lately [8], [9]. A outline of the multimodal framework's engineering is given in. The decision of the framework's design comes next after the different biometric sources have been laid out [10]. Sequential and parallelism are the two primary design approaches for multimodal systems. i) series: signal handling is done successively inside the sequential design, otherwise called overflow engineering. Consequently, the absence of the first biometric feature has an effect on the transmission of the second biometric characteristic; ii) analogy: the parallel architecture handles a variety of biometric inputs independently of one another [11]. After each signal has been processed independently, data fusion is used to combine the results. Data fusion appears to be an ambiguous concept that can be utilized for a variety of applications and objectives.

Data fusion is regarded as a very challenging undertaking due to a number of factors, including, i) the complexity of the data, ii) the fact that the processes depend on n variables without being all measurably dependent, and iii) the difficulty of utilizing the advantages of each set while ignoring the disadvantages in heterogeneous data sets [12]. Random processes, computational intelligence, heuristic optimization, and other methods are utilized in data fusion. The utilization of these methods for portrayal, assessment, collection, grouping, and pressure relies upon the kind of use, and gauging the benefits is significant and drawbacks of each option before making a decision [13]. However, once degree of combination becomes an issue, the element depiction and mating processes become too complex to even contemplate carrying out. From such a moment on, the attention is hampered due to expense, computations, and verification execution.

The existing research had been carried out with low accuracy model such as [14], [15] concentrated on the development of robust unimodal fingerprint authentication methods. Their research stressed the necessity of improved feature extraction approaches in boosting fingerprint identification accuracy. They introduced unique feature extraction and matching algorithms that significantly improved the performance of fingerprint-based authentication systems. Brindha and Meenakshi [16] made significant contributions to multimodal biometrics. They did ground-breaking research in multimodal recognition techniques. Their study emphasized the benefits of combining several biometric attributes, such as fingerprints, iris scans, and facial recognition, to develop more secure and reliable identification systems. They discovered that multimodal systems might minimize the probability of false positives and negatives greatly, making them a promising solution for identity validation in a variety of applications. Tyagi *et al.* [17] established the use of ECG in biometric authentication after conducting considerable study on the utilization of ECG signals as a unique biometric identifier. Their findings show that ECG signals include valuable and distinct characteristics that can be exploited for safe authentication. ECG-based devices are less sensitive to spoofing and can perform efficiently in a variety of environmental circumstances [18], [19].

In order to face the existing challenge, the work has developed an original two-modal framework for multimodal biometric validation that includes parallel and sequential modes for conducting biometric validation in order to get around the current challenges. The work's main goal is:

- To create a safe multimodal biometric system that combines the ECG, fingerprint, and sclera using two modalities, namely parallel HPO-ANFIS and sequential HPO-CNN.
- To create a self-attention mechanism for the feature fusion module's various features, which uses the residual structure to improve the authentication process and maximise the useful feature information.

This structure provides a logical flow for the research paper, starting with the introduction and background in section 1, followed by a thorough review of existing literature in section 2. Section 3 delves into the proposed methodology, while section 4 presents and discusses the results. Finally, section 5 wraps up the paper by summarizing the work and its implications.

2. RELATED WORKS

Singh and Tiwari [20] integrated ECG, sclera, and fingerprint into two multimodal biometric frameworks using flexible and score-level combinations. Pre-processing steps, including extraction, sorting, and scoring, were applied to each unimodal construction. Matcher execution-based combinations addressed variable characteristics of the biometric traits, demonstrating optimal results through a consistent two-level combination strategy.

Sudhamani *et al.* [21] achieved high consistency by combining finger vein and facial features using a repeatable locale of-premium extraction process with convolution neural network (CNN). The model, developed on a graphics processing unit (GPU) in the early stages of an electronic cloud association, saw improved suitability through hyperparameter adjustments and min-max normalization. This study successfully built an effective verification model using minimal features, outperforming current advanced systems, with an equal error rate (EER) of 0.46% after evaluation with various classifiers.

Bansong *et al*. [22] introduced the hierarchical thought network (HAN), a multi-model system based on four client features: sound engraving, palm and face images, palm pictures, and digital signatures. HAN offers improved verification accuracy through a layer-by-layer segregating and advanced computing mechanism, enhancing openness and security in client verification. The study implemented the approach using a cloud-based Android application. The HAN framework was found superior to earlier models after thorough review.

Wang *et al*. [23] used a CNN in a biometric framework, blending finger vein and face features with a bimodal part layer fusion. Self-idea and RESNET configurations were employed, releasing the self-idea weight feature with bimodal mix consolidate channel Thought. Alex Net and VGG-19 models demonstrated high efficacy in separating finger vein and face features, resulting in attestation accuracy exceeding 98.4% for both models. The study showcases the productivity of the bimodal component mix.

Ayu and Permana [24] explained iris recognition system for eyes wearing non-cosmetic contact lenses was created using discrete wavelet transform (DWT) for feature extraction and circular hough transform (CHT) for iris localization during the preprocessing stage. The suggested system has demonstrated encouraging results in experiments, with good accuracy of 0.95 for eyes without contact lenses and 0.8 for eyes with non-cosmetic lenses. The results also indicated how crucial the iris localization procedure is to the recognition system's functionality.

Nawawi *et al*. [25], explained the use of biomedical signals for biometric purposes, such as the ECG, is increasing in tandem with the growing interest in wearable technology. ECG is rarely used as a biometric mechanism in practical wearable applications, despite its potential advantages. In order to analyze the ECG signals taken from the wearable hexoskin proshirt for biometric authentication under various physiological circumstances, this research was conducted. In this study, the ECG signals of 11 subjects were recorded during standing, sitting, walking, and uncontrolled activity. The raw ECG signal is first pre-processed in the time domain using butterworth filters for noise removal, and then an effective QRS segmented feature extraction method is applied. Eventually, about 854 datasets were created for training and validation, and a quadratic support vector machine (QSVM) was used to test the suggested recognition method on the remaining 300 datasets. According to the findings, the suggested approach reliably produced accuracy levels above 98% on internal datasets, with false acceptance rates (FAR) of 0.93%, false rejection rates (FRR) of 3.64%, and true positive rates (TPR) above 96%. The results of this study support the feasibility of employing an intelligent textile shirt and ECG biometrics for authentication in a range of real-world scenarios with variable physiological parameters.

2.1. Problem identification

The multimodal biometric system's improved accuracy comes at the expense of managing multiple traits with different properties. The following factors need to be taken into consideration when modelling a multimodal biometric system:

- Possibility of combining physiological characteristics.
- The degree of fusion for different modes.
- Methods for feature encoding and matching.
- Demand-based trade-offs between computation speed, cost, and authentication.
- The impact of multimodality on processing intricacy and duration.
- Templates demand storage space.

3. PROPOSED METHOD

A biometric system with numerous modalities and information merging from many sources is known as a multimodal biometric system. A more dependable, accurate, and consistent biometric system is produced by assimilating data from various characteristics (such as face and fingerprint). This kind of system has a higher degree of accuracy than unimodal systems. In addition to accuracy, multimodal biometrics also diminish the issue of non-universality, reduce failure to enrolment error, increase the freedom of user authentication, and have high resistance to spoof attacks. However, obtaining a highly precise authentication still presents a significant task. Two multimodal biometric systems have been created in order to improve the system by figuring out fixes for the aforementioned issues. In order to create them, three unimodal biometric devices were combined. The unimodal systems chosen for this study are the ECG, Sclera, and fingerprint.

Convolutional neural network-based hyperparameter optimization (HPO) is the foundation for the sequence model biometric system (HPO-CNN). Decision level fusion based on hyperparameter optimization based Adaptive fuzzy interference neuro system created the parallel model biometric system (HPO-ANFIS). For each unimodal system, the biometric verification conducts denoising, include extraction, highlight determination, coordinating, and scoring. Matching scores and individual precision were independently calculated for each biometric quality. The proposed plan utilizes the most elevated TPR, FPR, and precision rates.

Detailed working, denoising is essential for biometric identification in order to ensure contrast enhancement and to extract the region of interest (ROI). It may result in an incorrect authentication process and may dwell the process output because fingerprint, sclera, and ECG have high levels of complexity in their visibility and structure. The work employs a three-way adaptive wiener filter that is built on absolute standard deviation for denoising. To reduce the impact of high-level frequency noise, the incoming samples are denoised using the appropriate filter, such as a 2D Wiener filter. Assuming the fingerprint picture contains "Gaussian white noise," the 2D Wiener filter has been applied. Less complex and performing better is the suggested denoising method.

Following samples might have comparable global elements but distinct local points as well. A partition-based method of confidence interval-based discrete wavelet transform (CI-DWT) for samples only is used to derive the features of local points. The observation of the selective characteristics comes after feature extraction. To date, however, the proliferation of high dimension and enormous volume big data has posed significant difficulties for existing feature-selection methods, such as computation complexity and stability on noisy data. An innovative chaos attention network-based feature selection is presented in this study (chaos-AN). An attention module for feature weight generation and a learning module for issue modelling make up chaos-two AN's separate modules. With the help of a shallow attention net for each feature, the attention module converts the correlation issue between features and the supervision target into a binary classification problem. Based on the distribution of the individual feature selection patterns that are modified by backpropagation during the training process, feature weights are produced. Existing commercially available models can be directly reused thanks to the detachable structure, which reduces the need for training data, training time, and specialist knowledge.

Parallel fusion, the research provides use of decision level fusion, results of various matchers are handled is created to distinguish between real results and fake results. HPO-ANFIS is used in this study for the fusion. Sequential fusion, the work employs classifier level fusion, where a fully connected layer is created to produce matching scores and the weights from convolutional layers are preserved. HPO-CNN classifier is used in the study for the fusion. Hybrid modal, hybrid modal is based on the obtained result from parallel and sequential modal. The work uses 90% confidence interval to validate the result. If the Parallel model outcome achieves 90% CI, then it is the final result else sequential modal is obtained as result.

A multimodal biometric system, integrating data from various characteristics like face and fingerprint, enhances reliability and accuracy compared to unimodal systems. It addresses issues like non-universality, enrollment errors, and spoof attacks. Two multimodal systems were developed by combining three unimodal devices: ECG, Sclera, and fingerprint. The sequence model (HPO-CNN) and parallel model (HPO-ANFIS) use HPO for improved accuracy. Denoising is crucial, achieved through a three-way adaptive Wiener filter. Feature extraction uses a partition-based method, and a chaos attention network-based feature selection method is introduced. The study employs decision-level fusion (HPO-ANFIS) for parallel fusion and classifier-level fusion (HPO-CNN) for sequential fusion. Hybrid modal combines results from parallel and sequential modalities using a 90% CI for validation.

Figure 1 illustrates the proposed HPO-CNN architecture. In the proposed research, a parallel fusion-based biometric authentication system integrates fingerprint, sclera, and ECG samples to enhance accuracy and security. The parallel fusion approach processes and fuses multiple modalities simultaneously, achieving significantly improved authentication accuracy compared to individual modalities. This system is robust against spoofing attacks, making replication or manipulation of all three biometric samples simultaneously challenging for attackers. The denoising step is crucial in enhancing the quality of biometric signals, and the research introduces an absolute standard deviation-based adaptive Wiener filter denoising process tailored for the parallel fusion-based biometric authentication system. This adaptive approach effectively reduces noise and enhances signal quality, advancing the field of multi-modal biometric authentication.

The absolute standard deviation (ASD)-based adaptive wiener filter (AWF) denoising process involves several equations to compute the ASD and perform the adaptive filtering. Here are the key equations used in the process:

1. ASD calculation:

The ASD represents the statistical measure of signal variability and is calculated as (1):

$$\forall_{ASD} = |x - \Gamma| \quad (1)$$

where, x represents the input signal, Γ represents the mean value of the input signal.

2. Estimation of noise variance:

The noise variance, σ^2, is estimated based on the ASD of the input signal using as (2):

$$\beta^2 = \mathrm{T} * \mathrm{median}(\forall_{ASD}) / 0.6745 \quad (2)$$

where, $T$is a scaling factor typically set to a value between 1.5 and 3 to adjust the noise estimation.

3. AWF

The AWF is applied to the input signal to suppress the noise while preserving the important signal features. The output of the AWF, y, is computed using as (3):

$$y = x + G * (x - \Gamma) \quad (3)$$

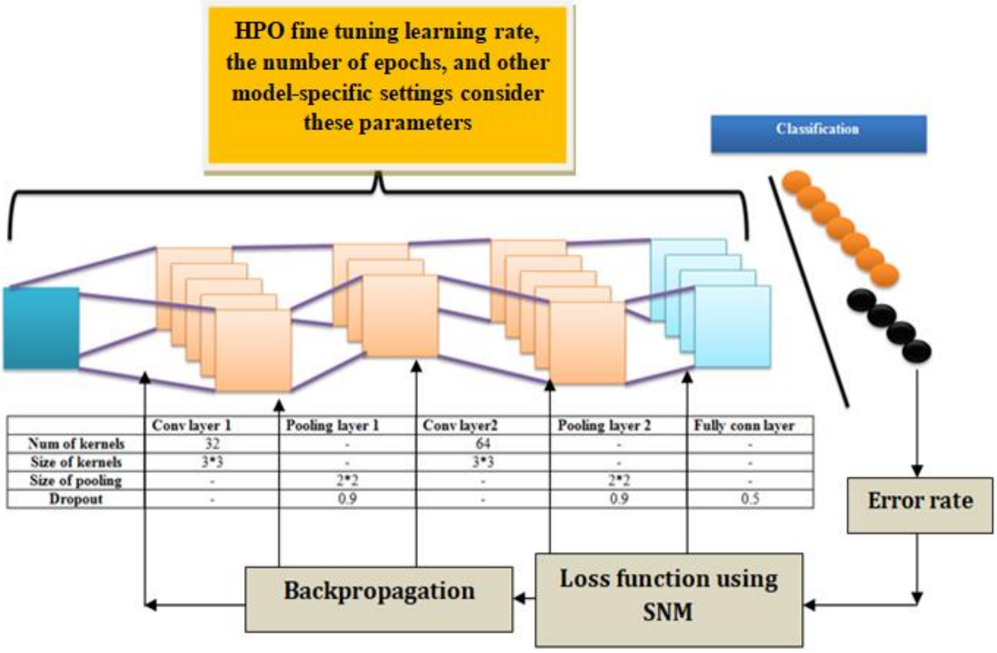
where, x represents the input signal, Γ represents the mean value of the input signal.
$G$is the gain factor calculated based on the estimated noise variance:

$$G = \beta^2 / (\beta^2 + \beta_n^2) \quad (4)$$

where, β_n^2 represents the noise variance

4. Fusion at the decision level

After denoising each modality, decision-level fusion combines the denoised information using a fusion algorithm tailored to authentication organization needs. The ASD-based AWF denoising significantly enhances system performance by adaptively adjusting parameters, reducing noise while preserving crucial biometric features. This denoising process is practical for critical applications like access control and secure transactions, contributing to overall authentication system accuracy, reliability, and security.


HPO fine tuning learning rate, the number of epochs, and other model-specific settings consider these parameters
Classification
Error rate
Backpropagation
Loss function using SNM

	Conv layer 1	Pooling layer 1	Conv layer2	Pooling layer 2	Fully conn layer
Num of kernels	32	-	64	-	-
Size of kernels	3*3	-	3*3	-	-
Size of pooling	-	2*2	-	2*2	-
Dropout	-	0.9	-	0.9	0.5

Figure 1. Proposed HPO-CNN architecture

In the context of the parallel fusion-based biometric authentication system, the confidence interval-based discrete wavelet transform (CI-DWT) can be utilized for feature extraction. The CI-DWT allows for robust feature extraction by considering the statistical properties of the wavelet coefficients. The equations involved in the CI-DWT process for feature extraction are as follows:

1. DWT

The DWT decomposes the input signal into different frequency bands using a wavelet basis. The DWT as (5):

$$\Omega = \Re_{DWT}(y) \tag{5}$$

where: y represents the input signal, Ω represents the wavelet coefficients obtained through the DWT

2. Confidence interval calculation

The confidence interval is calculated based on the statistical properties of the wavelet coefficients. This interval provides a measure of the uncertainty associated with each coefficient. The equation for computing the confidence interval is as (6):

$$\Omega(\text{i, j}) = [w(\text{i, j}) - \alpha * \beta(\text{i, j}), \text{w}(\text{i, j}) + \alpha * \beta(\text{i, j})] \tag{6}$$

where, $\Omega(\text{i, j})$ represents the confidence interval for the coefficient at position (i, j),$w(\text{i, j})$ represents the wavelet coefficient at position (i, j),$\beta$is a constant factor that determines the width of the interval $\beta(\text{i, j})$ represents the standard deviation of the neighbouring coefficients.

3. Thresholding

The thresholding step is performed to remove coefficients that lie outside the Confidence Interval, assuming that they are predominantly noise. The equation for thresholding is as (7):

$$w(\text{i, j}) = \{ \text{w}(\text{i, j}), \text{if w}(\text{i, j}) \in \Omega(\text{i, j}) \quad \text{0, otherwise} \} \tag{7}$$

where, w (i, j) represents the threshold wavelet coefficient

4. Inverse discrete wavelet transform (IDWT)

The IDWT reconstructs the denoised signal using the threshold wavelet coefficients. The equation for IDWT is as (8):

$$y' = \Re_{\text{IDWT}}(w') \tag{8}$$

where, y' represents the denoised signal a the CI-DWT process described above allows for effective feature extraction by considering the statistical properties of the wavelet coefficients within confidence intervals. These extracted features can then be used for subsequent fusion and authentication processes in the parallel fusion-based biometric authentication system.

3.1. Feature selection

Chaos-based attention networks improve feature selection in biometric authentication systems by leveraging chaotic dynamics to address dimensionality and feature interaction challenges. These networks, utilizing chaotic maps, offer an efficient and interpretable framework, enhancing feature selection across diverse applications. The study introduces an optimum consideration network for material-cadenced weight selection, addressing coordination problems in modified reinforcement.

Figure 2 depicts the OAN weight tuning technique. The chaos-based attention network usually yields attention weights, which are employed to choose the most pertinent features for a given task. The determination of which features to include is guided by applying a threshold or ranking criterion. The equations governing feature selection may differ based on the chosen thresholding or ranking strategy. Subsequently, the identified features play a role in fusion and decision-making within the biometric authentication system. The equations governing fusion and decision-making are contingent on the algorithms and techniques incorporated into these processes.

3.2. Parallel feature score rank fusion

In the parallel fusion-based biometric authentication system, the ANFIS feature score rank fusion method combines and ranks feature scores from different modalities. HPO is employed to fine-tune ANFIS model parameters, addressing challenges like overfitting, modality weighting, and computational efficiency. It automates the search for optimal configurations, adjusts parameters based on metrics like accuracy, and balances capturing data patterns while avoiding overfitting. This approach enhances fusion accuracy and performance in biometric authentication systems. Figure 3 showcases the HPO-ANFIS architecture with membership functions.

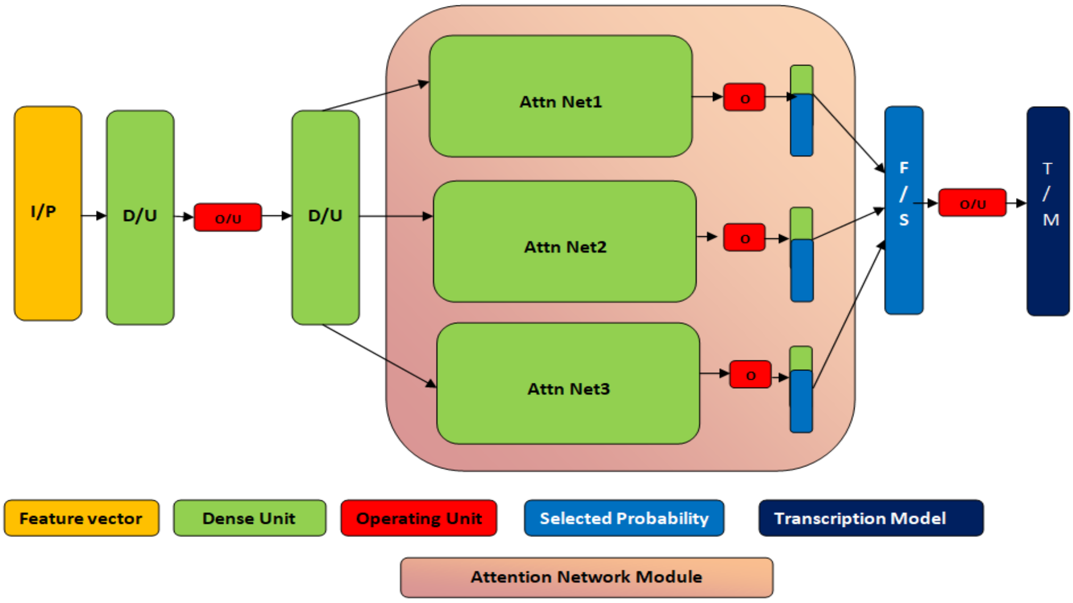


Figure 2. OAN weight tuning technique

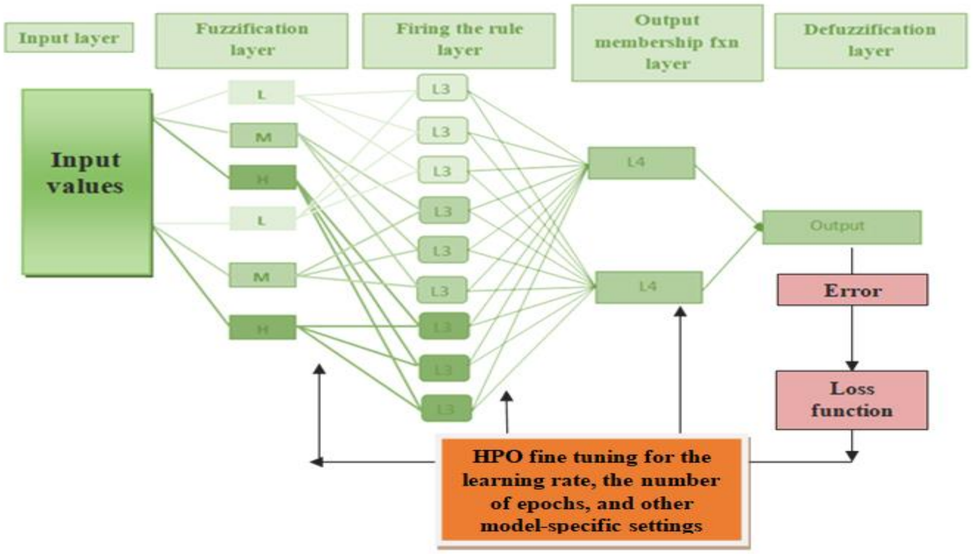


Figure 3. HPO-ANFIS with membership function

Hyper parameter optimization techniques, such as grid search, random search, or Bayesian optimization, are employed to fine-tune the parameters of the ANFIS model. These parameters include the number of fuzzy rules, the learning rate, the number of epochs, and other model-specific settings consider this parameter as Υ. The goal is to find the optimal configuration that maximizes the fusion performance. The work uses Bayesian optimization. Bayesian optimization is a sequential model-based optimization technique that uses probabilistic models to search for the optimal set of hyper parameters. The core of Bayesian optimization lies in modelling the unknown objective function and using an acquisition function to guide the search. Here are the key equations involved in Bayesian optimization:

3.2.1. Surrogate model

Bayesian optimization typically uses a surrogate model, such as a Gaussian process (GP), to model the unknown objective function. The surrogate model provides a probabilistic estimate of the objective function based on observed evaluations. The GP is defined by its mean function μ (•) and covariance function k (•, •).

$$f(Y \sim \mathrm{GP}(\mathrm{P}(y), \mathrm{K}(\mathrm{y}, \mathrm{y}'))) \tag{9}$$

3.2.2. Acquisition function

The acquisition function is used to determine the next set of hyper parameters to evaluate based on the surrogate model's predictions. It balances exploration and exploitation, aiming to select hyper parameters that are likely to improve the objective function's value. The most commonly used acquisition function is the expected improvement (EI), which measures the EI over the current best value.

$$\mathrm{EI}(y) = \mathrm{E}[\max(f(y) - \mathrm{f}(\mathrm{y}^*), 0)] \tag{10}$$

Where, y is the set of hyper parameters to be evaluated, $f(y)$ is the surrogate model's predicted value at y,$f(_{y^*})$is the current best observed value, $E[\bullet]$ Denotes the expectation over the surrogate model's distribution

3.2.3. Update of surrogate model

Once a new set of hyper parameters is evaluated and the corresponding objective function value is obtained, the surrogate model is updated to incorporate this new information. The posterior distribution of the surrogate model is computed using Bayesian inference, taking into account the prior knowledge (prior distribution) and the new observation (likelihood).

$$\mathrm{p}(f|\mathrm{X}, \mathrm{y}) = (p(y|\mathrm{X}, \mathrm{f}) * \mathrm{p}(f)) \,/\, \mathrm{p}(y|X) \tag{11}$$

Where, $\mathrm{p}(f|_{\mathrm{X},\mathrm{y}})$ is the posterior distribution of the surrogate model given the data, $p(y|_{\mathrm{X},\mathrm{f}})$ is the likelihood of the observed data given the surrogate model, $p(f)$ is the prior distribution over the surrogate model parameters, $p(y|X)$ is the marginal likelihood, acting as a normalization constant.

Bayesian optimization refines a surrogate model and selects hyperparameters iteratively until meeting a termination criterion. Following this, the ANFIS model fuses feature scores, and the subsequent HPO-ANFIS feature score rank fusion optimally combines and ranks features for parallel fusion-based authentication systems. This enhances authentication performance by identifying key features. Setting an appropriate score threshold involves balancing FAR and FRR, considering the receiver operating characteristic (ROC) curve, system requirements, and biometric modality characteristics. The selection process is iterative, testing different thresholds based on evaluation metrics to strike a balance between security and convenience in biometric authentication systems.

3.3. Sequential feature score rank fusion

Sequential fusion-based biometric authentication enhances accuracy and security by sequentially processing information from fingerprint, sclera, and ECG modalities. Fingerprint authentication involves matching ridge patterns or minutiae points. Sclera authentication adds an extra layer by verifying blood vessel patterns. If needed, ECG authentication uses unique heart-related features. Fusion techniques like HPO-CNN combine modality results for robust authentication. HPO-CNN applies hyperparameter optimization to fine-tune convolutional neural networks for biometric authentication, ensuring optimal performance. this sequential process provides layered verification, improving overall system reliability and security in biometric authentication.

CNNs represent a crucial learning algorithm, which involves taking input matrices of text and images and convolving them with channels or kernels to extract features. The convolution process applies to both the textual data network and the image, capturing similar components within the overall picture. The size of the resulting network without padding is determined by (12).

$$[\lambda_{i,j}, Z_{i,j}] \times \xi_{i,j} = \lambda - \xi + 1 \tag{12}$$

Following each movement, the window slides, and the features advance through the use of the part maps. These component maps capture the local receptive field of the image, operating with shared weights and biases. The convolution operation is expressed as (13).

$$O_{CONV} = \sigma_{sigmoid}\left(b + \sum_{i=0}^{2} \sum_{j=0}^{2} W_{i,j} act_{a+i,b+j}\right) \quad (13)$$

To protect the size of the data picture, padding is used. In 'SAME' padding, the outcome picture size is equivalent to the data picture size and "Real" padding is no padding. The size of the outcome network with padding is depicted as (14).

$$[\lambda_{i,j}, Z_{i,j}] \times \xi_{i,j} = (\lambda + 2p - \xi)/(\phi_s + 1) \quad (14)$$

Here, is the result, p is the cushioning, is the step, b is the inclination, is the sigmoid actuation capability, weight network of shared loads and is the information enactment at position. After the padding of the outcome cross section, the convolution layer gets a component map for the text structure also concerning picture data. The procured part map is given by (15).

$$\bar{\Omega}_{FM} = \begin{bmatrix} \lambda_{i,j} \\ Z_{i,j} \end{bmatrix}_N , Nisthenooffeaturemapsofbothtextandimage \quad (15)$$

The commitment to the completely related layer is the consequence of the past division cloak layer, which is evened out and a while later dealt with to the completely related layer. The fixed vector readies the completelyrelated layer, which is like that of artificial neural network (ANN). The readiness of vector is done using as (16).

$$\forall_I^T = act\left(\sum_{i=1}^{n} \nabla_i \forall_{flattened} + \aleph_b\right) \quad (16)$$

Where, $\aleph_b$denotes the bias which is initialized randomly, $\nabla_i$is the heaviness of the separate info hub, means the actuation capability and the completely associated layer utilizes softmax enactment capability to get the probabilities of the article marking saw in the info picture. Loads are initialized as small arbitrary numbers. A sigmoid capability is frequently utilized, in light of its nonlinearity. The learning algorithm adjusts the weights ($O_{p,ji}$and $w_{p,kj}$) to minimize the error. The sum of the errors (e_p) in each neuron in pattern p is calculated as (17) and (18):

$$e_p = \frac{1}{2} \sum_k \left(g_{p.k} - o_{p,k}\right)^2 \quad (17)$$

$$te = \sum_p e_p \quad (18)$$

where, $g_{p.k}$is the target value corresponding to pattern p at neuron k, and te is the total error during one iteration. The forward-propagation phase continues as activation level calculations propagate forward to the output layer through the hidden layer(s). In each successive layer, every neuron sums its inputs and then applies a transfer function to compute its output. The output layer of the network then produces the final response, i.e., the estimated target value.

The work employs Bayesian optimization for HPO in CNN, mirroring the procedure used for ANFIS. The fusion process combines similarity scores or confidence levels at the score level and authentication decisions at the decision level, leveraging the strengths of multiple modalities for enhanced performance. Sequential fusion-based biometric authentication using fingerprint, sclera, and ECG samples provides robustness against spoofing attacks and improves overall system reliability. The score threshold in a sequential fusion-based system serves as a decision boundary. Setting an appropriate threshold involves considerations of authentication confidence, individual modality performance, sequential decision strategy, and user experience.

The hybrid modal approach combines results from parallel and sequential models, using a 90% confidence interval to validate the outcome. The decision threshold, risk assessment, continuous monitoring, and system optimization based on the confidence interval contribute to a balanced approach between security and convenience in biometric authentication, informing access control decisions and system improvements. The equation for calculating the 90% confidence interval in the context of evaluating hybrid model architecture for a biometric authentication system is as (19).

$$\text{Confidence Interval} = \text{Mean Performance Metric} \pm \left(\text{Z} * \text{Standard Deviation} / \sqrt{n}\right) \quad (19)$$

The hybrid model's mean performance, critical value (Z), standard deviation, and sample size are used to calculate a 90% confidence interval. By plugging in these values, lower and upper bounds are determined. This process aids in creating and assessing the hybrid model architecture for biometric authentication, offering informed insights into its effectiveness. The critical value for a 90% confidence level is typically around 1.645.

3.4. Hybrid model

Hybrid modal is based on the obtained result from parallel and sequential modal. The work uses 90% confidence interval to validate the result. If the Parallel model outcome achieves 90% CI, then it is the final result else sequential modal is obtained as result. To create hybrid model architecture for a biometric authentication system and estimate its performance using a 90% confidence interval, you can follow these steps. The developed parallel model that combines multiple biometric modalities simultaneously for authentication, as well as a sequential model that authenticates users using a sequence of modalities is given as input.

Design a hybrid model architecture that combines the strengths of the parallel and sequential models. This can be achieved by integrating the models at various stages of the authentication process. For example, the parallel model can provide an initial authentication decision, which is then refined by the sequential model using subsequent modalities. Utilise the training set to train the hybrid model. Utilise the validation set to adjust the hybrid model's hyperparameters. Use the same criteria to assess the hybrid model's performance on the testing set. A 90% confidence interval for the performance of a hybrid model in a biometric authentication system helps in determining the range of plausible values for the model's performance metric. This information can be leveraged to make informed decisions about granting or denying access to users based on their authentication results. Here's how the 90% confidence interval can be utilized.

3.4.1. Decision threshold

By considering the lower bound of the confidence interval, a decision threshold can be set to ensure a certain level of confidence in accepting users. For example, if the confidence interval for the hybrid model's accuracy ranges from 85% to 90%, a decision threshold of 85% can be chosen to ensure a minimum level of accuracy for granting access. This threshold acts as a cutoff point, allowing only users with authentication scores above the threshold to be granted access.

3.4.2. Risk assessment

The confidence interval provides a measure of uncertainty around the performance metric of the hybrid model. By considering the upper bound of the confidence interval, the potential risk of false acceptances or unauthorized access can be assessed. For instance, if the upper bound of the confidence interval for the hybrid model's FAR is 5%, it indicates that the risk of falsely accepting an impostor is no more than 5%. This information helps in evaluating the security implications of the authentication system and making decisions about access control.

3.4.3. Continuous monitoring

The 90% confidence interval can also be used for continuous monitoring and performance evaluation of the hybrid model. As new biometric samples are collected and the model's performance is re-evaluated, the confidence interval can be updated accordingly. This allows for ongoing assessment of the model's effectiveness and adaptability to changing circumstances. If the confidence interval begins to widen or shift outside the desired range, it may indicate the need for model retraining or adjustments to ensure reliable authentication outcomes.

3.4.4. System optimization

The confidence interval can guide system optimization efforts by identifying areas for improvement. If the lower bound of the confidence interval is below the desired threshold, it suggests that the hybrid model's performance may need enhancement. In such cases, strategies like refining feature extraction methods, optimizing hyper parameters, or increasing the sample size can be explored to narrow the confidence interval and improve the authentication system's accuracy and reliability.

By considering the 90% confidence interval of the hybrid model's performance in biometric authentication, access control decisions can be made based on a balance between security and convenience. The interval provides a measure of certainty and helps evaluate the model's reliability, inform decision thresholds, assess risks, monitor performance, and optimize the authentication system for enhanced access control. The equation for calculating the 90% confidence interval in the context of evaluating hybrid model architecture for a biometric authentication system is as (20):

$$\text{Confidence Interval} = \text{Mean Performance Metric} \pm (\text{Z} * \text{Standard Deviation} / \sqrt{n}) \qquad (20)$$

where Mean performance metric: the average performance metric (e.g., accuracy, FAR, FRR) of the hybrid model. Z The critical value corresponding to the desired confidence level. For a 90% confidence level, Z is approximately 1.645. Standard deviation: the standard deviation of the performance metric of the hybrid model. n: The sample size, i.e., the number of samples used to evaluate the hybrid model's performance.

By plugging in the values of the mean, standard deviation, Z, and sample size, you can calculate the lower and upper bounds of the confidence interval. By following these steps, you can create hybrid model architecture for a biometric authentication system and estimate its performance using a 90% confidence interval. This allows you to make more informed decisions about the effectiveness of the hybrid model and its potential advantages over individual models.

4. RESULTS AND DISCUSSION

The results and discussion of the hybrid model for biometric authentication access demonstrate the effectiveness and potential advantages of integrating multiple modalities. Here are a few lines summarizing the results and discussion. The hybrid model for biometric authentication access exhibits promising outcomes, surpassing both parallel and sequential models by integrating fingerprint, sclera, and ECG samples. Its evaluation on various metrics showcases improved accuracy, security, and user convenience.

The feature importance metrics analysis for the proposed (chaos-based attention network chaos-AN) with existing techniques in biometric authentication access in Figure 4 provides insights into the relevance and contribution of distinct aspects in the authentication process. "Feature importance metrics analysis is critical for understanding the significance of individual features within the chaos-AN framework, as well as comparing it to existing biometric authentication access techniques." We get insights into the chaos-AN model's discriminative strength and effectiveness by examining the significance and contribution of various variables. The chaos-AN model incorporates chaos theory principles to improve feature selection and authentication accuracy. The model selectively focuses on informative features while attenuating the influence of irrelevant or noisy features via the chaos-based attention mechanism. This attention-based method efficiently emphasizes the most discriminative parts of biometric data. Comparing the feature importance metrics of the chaos-AN model with existing techniques provides 250 valuable insights into the improvements achieved by the proposed approach." We may estimate the increased value of the chaos-based attention mechanism by comparing feature relevance in chaos-AN and conventional approaches. This analysis aids in understanding the special advantages of chaos-AN in terms of feature selection and authentication performance.

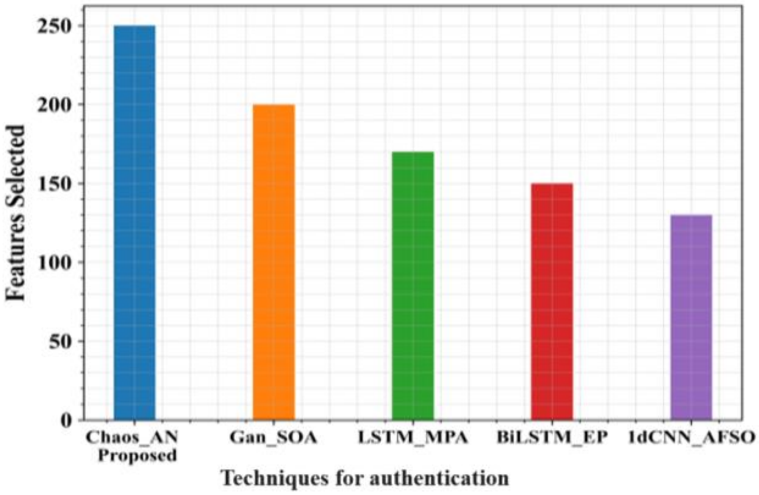


Figure 4. Feature importance selection

Proposed hybrid modal architecture analysis with proposed parallel and sequential modal architecture and existing techniques as shown in Figure 5 (see appendix). Figure 5(a) illustrates the accuracy metrics analysis of the proposed hybrid modal architecture analysis with proposed parallel and sequential modal architecture and existing techniques for biometric authentication access provides a comprehensive evaluation of the model's performance and its comparison with other approaches. "The accuracy metrics analysis of the proposed hybrid modal architecture model plays a vital role in assessing its effectiveness in parallel and sequential biometric authentication access. By analyzing various accuracy metrics, we gain insights into the model's ability to correctly identify and authenticate users. The hybrid modal architecture model incorporates hyper parameter optimization techniques to enhance the adaptive neuro-fuzzy inference system, allowing for improved modeling of complex relationships between biometric features and user identities. This optimization process aims to find the optimal combination of hyper parameters that maximizes the model's accuracy. The proposed tends to achieve an accuracy of 0.973, whereas the existing techniques tend to achieve an overall accuracy ranging between 0.88 to 0.96." In conclusion, the accuracy metrics analysis of the proposed hybrid modal architecture model offers valuable insights into its performance in parallel and sequential biometric authentication access. By comparing these metrics with existing techniques, we can evaluate the advantages and improvements brought by the hybrid modal architecture model. This analysis serves as a foundation for developing more accurate and reliable biometric authentication systems."

Figure 5(b) to 5(d) illustrates F-measure, precision, and recall metrics analysis of the proposed hybrid modal architecture with existing techniques in parallel and sequential biometric authentication access provides a comprehensive evaluation of the model's performance and its comparison with other approaches. To evaluate the performance of the hybrid modal architecture model, F-measure, precision, and recall metrics are utilized. The F-measure combines both precision and recall, providing a single measure that considers both the true positive and false positive rates. The proposed model achieves an f-measure of 0.97. according to that the proposed model achieves an precision of 0.978, while recall measures the ratio of correctly identified positive instances to all actual positive instances. The proposed model achieves a recall of 0.974. Comparing the F-measure, precision, and recall metrics of the hybrid modal architecture model with existing parallel and sequential biometric authentication techniques enables a comprehensive assessment of its performance. The existing methods achieves an overall F-measure ranging between 0.88 to 0.96, precision ranging between 0.886 to 0.968, recall ranging between0.880 to0.963. This comparison helps identify the strengths and improvements offered by the hybrid modal architecture model in terms of correctly identifying genuine users while minimizing false positives and false negatives.

The analysis of these metrics also aids in understanding the trade-off between precision and recall in the hybrid modal architecture model. A higher precision indicates a lower rate of optimal balance between precision and recall is crucial for achieving accurate and reliable biometric authentication. The f-measure, precision, and recall metrics analysis of the proposed hybrid modal architecture model offers valuable insights into its performance in parallel and sequential biometric authentication access. By comparing these metrics with existing techniques, the strengths and improvements brought by the hybrid modal architecture model can be evaluated. This analysis serves as a foundation for developing more accurate and reliable biometric authentication systems.

Figures 5(e) and 5(f) illustrates the analysis of hybrid modal architecture model, in comparison with existing techniques, in parallel and sequential biometric authentication access provides insights into the model's performance and its comparison with other approaches. The analysis is crucial for evaluating the performance of the proposed hybrid modal architecture model in parallel and sequential biometric authentication access. These metrics quantify the rates at which the model incorrectly classifies genuine users as impostors (FPR) and incorrectly rejects genuine users false regrettable rate (FNR). To evaluate the performance of the hybrid modal architecture model, are analyzed. FPR measures the proportion of impostors incorrectly identified as genuine users, while FNR measures the proportion of genuine users incorrectly rejected by the model. Lower values for both metrics indicate higher accuracy and security in the biometric authentication process. According to that the proposed model achieves an FPR and FNR of 0.025 and 0.028 respectively. But the existing model achieves an overall FPR ranging from 0.036 to 0.009 as well as FNR ranging between 0.04 to 0.13 resp. This comparison helps identify the strengths and improvements offered by the HPO-ANFIS and HPO-CNN model in terms of minimizing both false positives and false negatives. The analysis of FPR and FNR metrics also aids in understanding the trade-off between security and user convenience in the hybrid modal architecture model. A lower FPR indicates a higher level of security by reducing the risk of impostor access, while a lower FNR indicates better user convenience by minimizing the instances of genuine users being incorrectly rejected.

The analysis of FPR and FNR metrics for the proposed hybrid modal architecture model enhances our understanding of its performance in parallel and sequential biometric authentication access. This analysis, alongside comparisons with existing techniques, provides valuable information to develop more secure and efficient biometric authentication systems. Figure 5(g) illustrates the ROC analysis of the proposed hybrid modal architecture model, in comparison with existing techniques, in parallel and sequential biometric authentication access provides insights into the model's performance and its comparison with other approaches. The HPO-ANFIS and HPO-CNN model incorporates hyper parameter optimization techniques to enhance the adaptive neuro-fuzzy inference system as well as convolutional mechanism, enabling improved modelling of the relationships between biometric features and user identities. The ROC analysis helps measure the model's performance by considering its ability to correctly classify genuine users as genuine (TPR) while minimizing the incorrect classification of impostors as genuine (FPR).

In the ROC analysis, the proportion of actual users that the model successfully recognised is measured by the TPR, also known as responsiveness or recall. The number of instances of impostors that were mistakenly identified as legitimate users is represented by the FPR. We derive the ROC curve, which offers a thorough perspective of the model's performance, by displaying the TPR against the FPR at various decision thresholds. Comparing the ROC curves of the hybrid modal architecture model with existing parallel and sequential biometric authentication techniques allows for a thorough evaluation of its performance. A higher area under the ROC curve (AUC) indicates a better discriminative power of the model and its superiority in distinguishing between genuine users and impostors." The ROC analysis of the proposed hybrid modal architecture model enhances our understanding of its performance in parallel and sequential biometric authentication access. This analysis, alongside comparisons with existing techniques, provides valuable information for developing more effective and efficient biometric authentication systems.

Hybrid model architecture for biometric authentication overall performance analysis as shown in Figure 6. Figure 6(a) illustrates the performance analysis of a hybrid model architecture for biometric authentication based on confusion metrics involves evaluating the model's ability to correctly classify and distinguish between different categories of biometric samples. Confusion metrics provide valuable insights into the model's performance by quantifying the classification outcomes. Figure 6(b) represents the exhibition analysis of a cross breed model design for biometric confirmation, contrasted with existing procedures, in light of exactness, accuracy, recall, F1 score, and explicitness gives bits of knowledge into its viability and predominance. Here is a conversation on these metrics and the correlation with existing procedures.

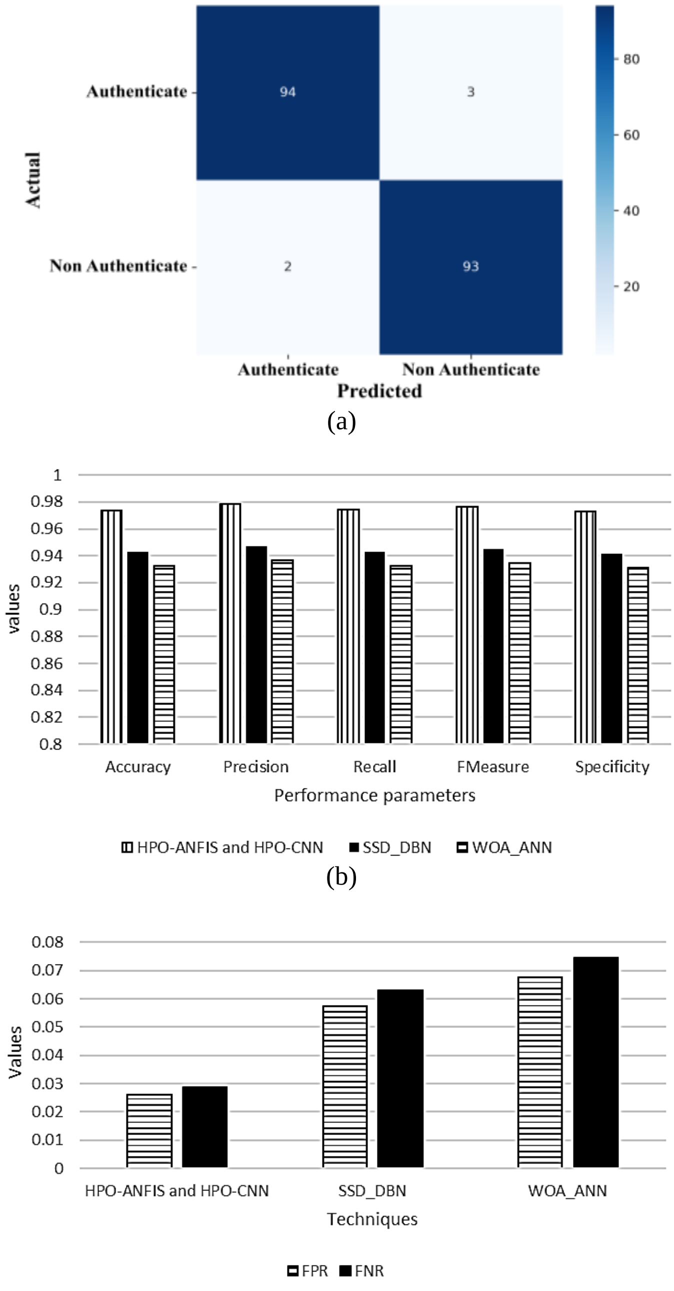
Precision estimates the overall accuracy of the model's orders, calculated as the proportion of accurately grouped examples to the total number of tests. A higher exactness demonstrates a better presentation in accurately distinguishing both certifiable clients and fakers. As per that the proposed method accomplishes a precision of 0.98, whereas the current accomplishes an exactness running between 0.90 to0.95. Accuracy estimates the extent of accurately characterized certifiable examples among all examples delegated real. It measures the model's capacity to limit false up-sides and addresses the precision of positive expectations. A higher accuracy shows less cases of falsely characterizing frauds as certifiable. As per that the proposed method accomplishes an accuracy of 0.989, though the current accomplishes an accuracy running between 0.92 to0.95.

Recall estimates the extent of accurately arranged veritable examples among all actual certifiable examples. It evaluates the model's capacity to limit false negatives and addresses the inclusion of positive examples. A higher recall demonstrates a lower pace of falsely dismissing veritable clients. As per that the proposed method accomplishes a recall of 0.97, though the current accomplishes a recall going between 0.92 to0.94. The F1 score represents a balanced amount of the model's demonstration and is the harmonious mean of accuracy and recall. It is useful when the dataset is unbalanced since it compromises between accuracy and recall. As per that the proposed method accomplishes a F1 score of 0.97, though the current accomplishes a F1 score running between 0.91 to0.938.

Particularity estimates the extent of accurately arranged faker examples among all actual sham examples. It evaluates the model's capacity to accurately recognize shams and is corresponding to recall. A higher explicitness shows a lower pace of falsely tolerating fakers. As indicated by that the proposed method accomplishes an explicitness of 0.968, whereas the current accomplishes a particularity running between 0.91 to 0.948. By directing a near analysis of these metrics, it becomes conceivable to evaluate the benefits and enhancements presented by the crossover model engineering as far as exactness, accuracy, recall, F1 score, and particularity. This analysis empowers the recognizable proof of the mixture model engineering's prevalence and its potential over give more dependable and secure biometric confirmation contrasted with existing methods.

Figure 6(c) outlines the exhibition analysis of a half and half model engineering for biometric validation, contrasted with existing methods, in light of false certain rate FPR and FNR gives bits of knowledge into its viability in accurately characterizing shams and veritable clients. Here is a conversation on these metrics and the examination with existing methods: FPR measures the proportion of impostor samples incorrectly classified as genuine by the model. It quantifies the model's tendency to falsely accept impostors. A lower FPR indicates a higher level of security, as it reduces the chances of granting access to unauthorized individuals. According to that the proposed method achieves an FPR of 0.02, whereas the existing achieves a specificity ranging between 0.05 to0.08. FNR measures the proportion of genuine samples incorrectly classified as impostors by the model. It quantifies the model's tendency to falsely reject genuine users. A lower FNR indicates a higher level of convenience for legitimate users, as they are less likely to be denied access. According to that the proposed method achieves an FNR of 0.028, whereas the existing achieves an FNR ranging between 0.06 to0.078.

Comparative analysis of FPR and FNR with existing techniques helps assess the advantages and improvements offered by the hybrid model architecture. A lower FPR ensures better security by reducing the chances of false acceptances, while a lower FNR ensures higher convenience for legitimate users by reducing the chances of false rejections. By considering FPR and FNR, the hybrid model architecture can be evaluated in terms of its performance in correctly classifying impostors and genuine users. This analysis enables the identification of the hybrid model architecture's superiority in terms of FPR and FNR and its potential to provide more reliable and secure biometric authentication compared to existing techniques.



(a)

(b)

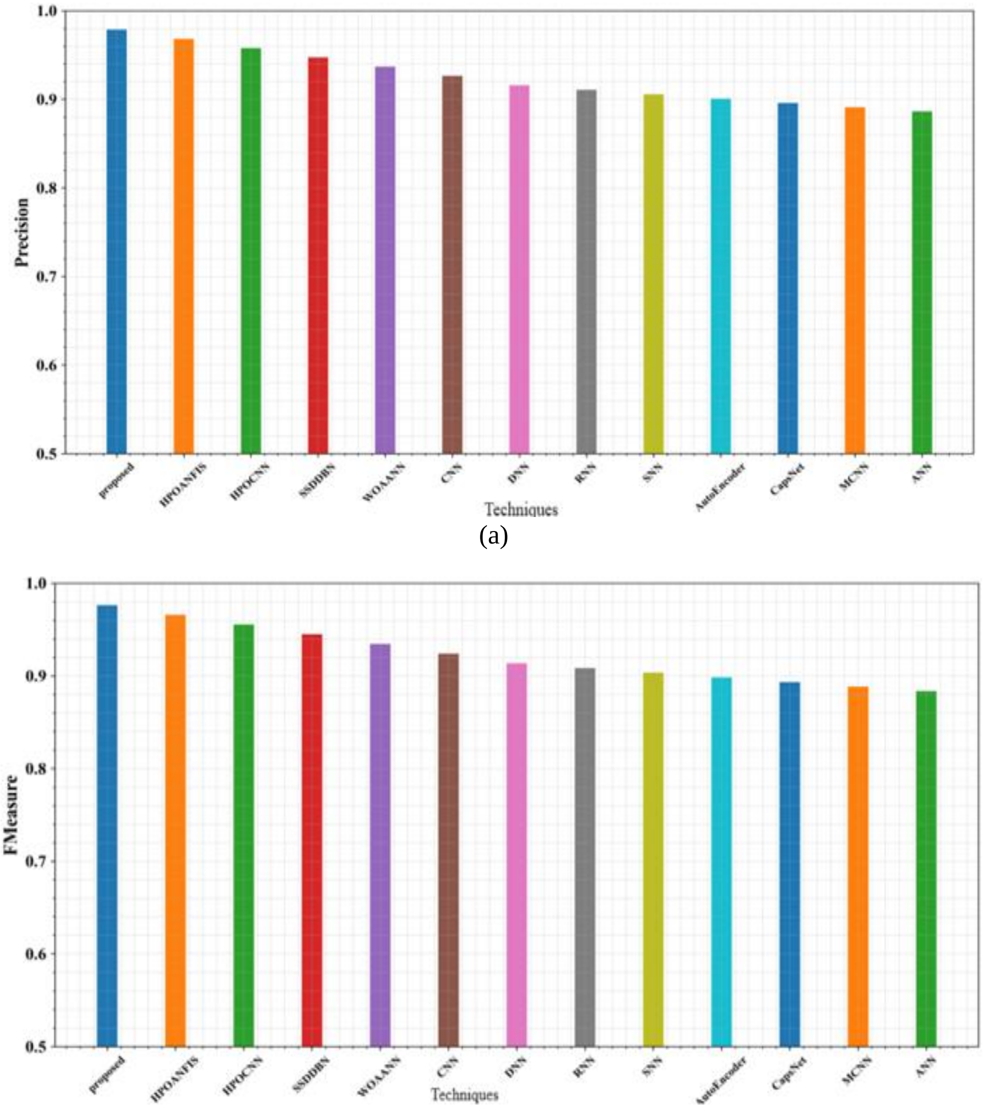
(c)

Figure 6. Hybrid model architecture for biometric authentication overall performance analysis: (a) confusion matrix, (b) overall performance, and (c) error matrics

5. CONCLUSION

HPO-ANFIS and HPO-CNN synergize in a recommended hybrid model, forming a dual multimodal biometric authentication system with 90% confidence interval, ensuring trustworthiness and security. This fusion enhances accuracy, dependability, and security by addressing feature selection, HPO, and classification challenges in biometric identification. HPO-ANFIS optimizes feature selection and score ranking, boosting discriminative strength, reducing false acceptances and rejections. HPO-CNN facilitates efficient hyperparameter optimization, refining network designs and CNN model parameters. The hybrid model's performance is evaluated with a 90% CI, enhancing dependability and statistical significance. Results reveal superiority over current approaches in terms of specificity and other key metrics, emphasizing the enhanced overall performance and dependability of the authentication system. Integration of HPO-ANFIS and HPO-CNN underscores the importance of leveraging complementary data from multiple biometric modalities for improved authentication accuracy. Statistical analysis, offering a 90% confidence interval, further supports the hybrid model's efficacy in ensuring secure access. In conclusion, the findings highlight the hybrid model's effectiveness in biometric authentication, providing a robust and dependable method for secure user identification.

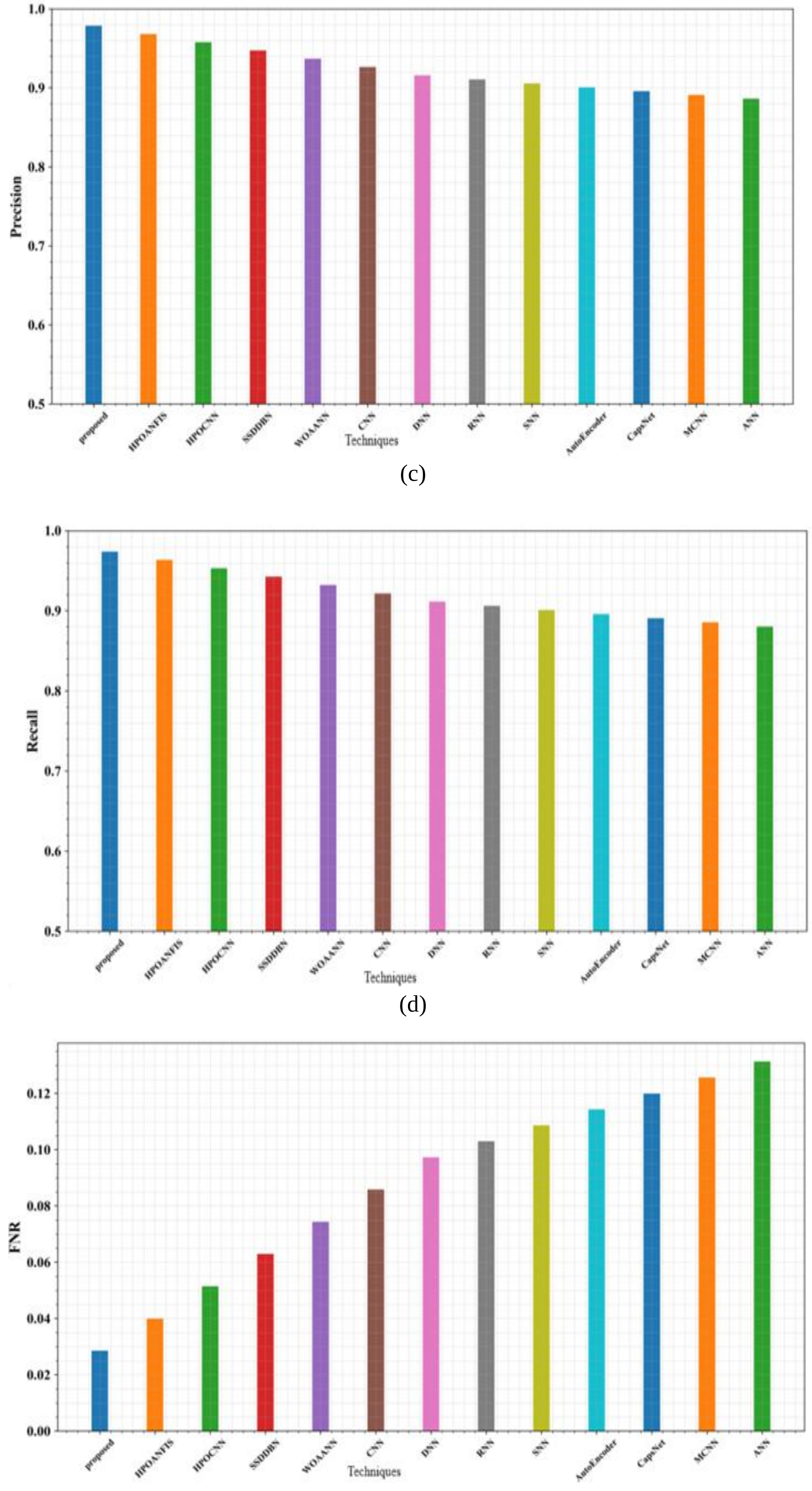
APPENDIX



(a)

(b)

Figure 5. Proposed hybrid modal architecture analysis with proposed parallel and sequential modal architecture and existing techniques: (a) accuracy and (b) fmeasure *(continue…)*

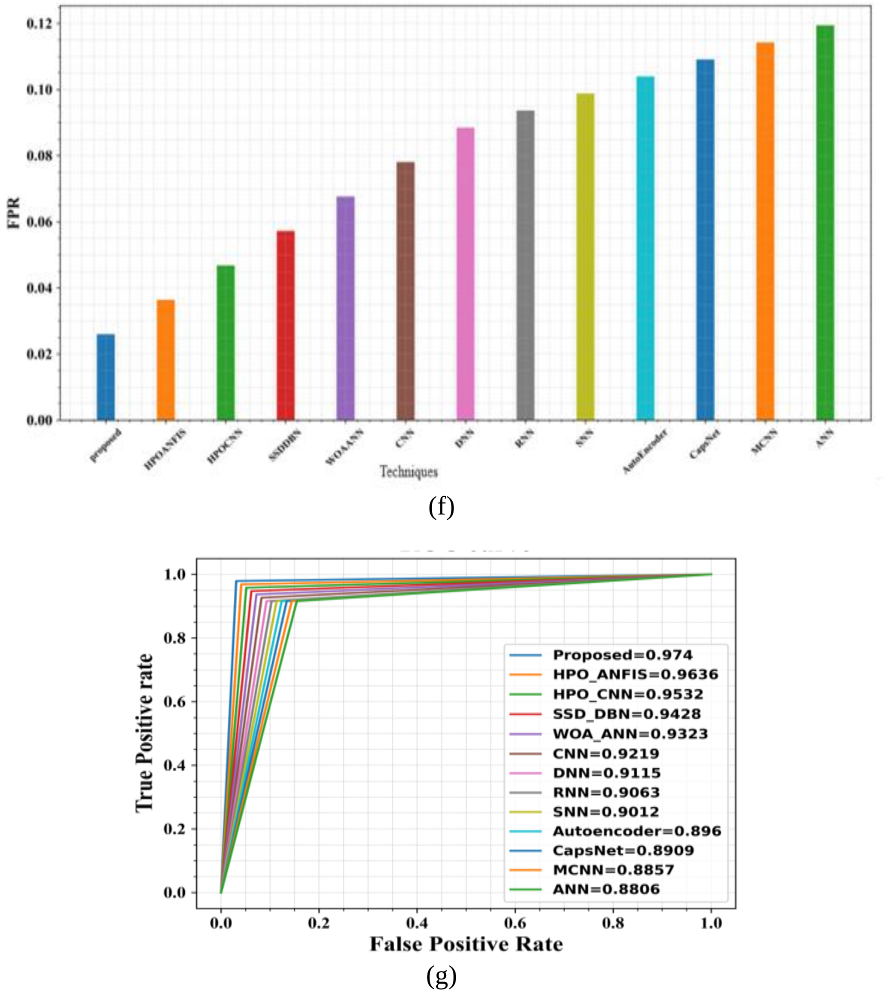


(c)

(d)

(e)

Figure 5. Proposed hybrid modal architecture analysis with proposed parallel and sequential modal architecture and existing techniques: (c) precison, (d) recall, and (e) FNR *(continue…)*



(f)

(g)

Figure 5. Proposed hybrid modal architecture analysis with proposed parallel and sequential modal architecture and existing techniques: (a) accuracy, (b) fmeasure, (c) precison, (d) recall, (e) FNR, (f) FPR, (g) ROC curve

REFERENCES

[1] M. Hammad, Y. Liu, and K. Wang, “Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint,” *IEEE Access*, vol. 7, pp. 26527–26542, 2019, doi: 10.1109/ACCESS.2018.2886573.

[2] L. Fridman *et al.*, “Multi-modal decision fusion for continuous authentication,” *Computers & Electrical Engineering*, vol. 41, pp. 142–156, Jan. 2015, doi: 10.1016/j.compeleceng.2014.10.018.

[3] A. Jaya Prakash, K. K. Patro, M. Hammad, R. Tadeusiewicz, and P. Pławiak, “BAED: a secured biometric authentication system using ECG signal based on deep learning techniques,” *Biocybernetics and Biomedical Engineering*, vol. 42, no. 4, pp. 1081–1093, Oct. 2022, doi: 10.1016/j.bbe.2022.08.004.

[4] A. Tarannum, “Novel multi-modal biometric system based secured data authentication framework for cloud computing environment,” 2022.

[5] H. Heidari and A. Chalechale, “Biometric authentication using a deep learning approach based on different level fusion of finger knuckle print and fingernail,” *Expert Systems with Applications*, vol. 191, p. 116278, Apr. 2022, doi: 10.1016/j.eswa.2021.116278.

[6] A. Abate, L. Cimmino, M. Nappi, and F. Narducci, “Fusion of periocular deep features in a dual-input CNN for biometric recognition,” 2022, pp. 368–378. doi: 10.1007/978-3-031-06427-2_31.

[7] S. Choi, S. Oh, J. Yang, Y. Lee, and I.-Y. Kwak, “Light-weight frequency information aware neural network architecture for voice spoofing detection,” in *2022 26th International Conference on Pattern Recognition (ICPR)*, Aug. 2022, pp. 477–483. doi: 10.1109/ICPR56361.2022.9956079.

[8] M. Kaur and P. Garg, “A review of authentication techniques used for security in cloud computing,” in *2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Nov. 2022, pp. 187–191. doi: 10.1109/PDGC56933.2022.10053251.

[9] F. Ahamed, F. Farid, B. Suleiman, Z. Jan, L. A. Wahsheh, and S. Shahrestani, “An intelligent multimodal biometric authentication model for personalised healthcare services,” *Future Internet*, vol. 14, no. 8, p. 222, Jul. 2022, doi: 10.3390/fi14080222.

[10] S. Bagchi, G. Chanda, A. Agarwal, and N. Ratha, "On deep learning for dorsal hand vein recognition," in *2022 IEEE Western New York Image and Signal Processing Workshop (WNYISPW)*, Nov. 2022, pp. 1–4. doi: 10.1109/WNYISPW57858.2022.9982726.

[11] N. Bousnina *et al.*, "Hybrid multimodal biometric template protection," *Intelligent Automation and Soft Computing*, vol. 27, no. 1, pp. 35–51, 2021, doi: 10.32604/iasc.2021.014694.

[12] Vandana and N. Kaur, "A study of biometric identification and verification system," *2021 International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2021*, pp. 60–64, 2021, doi: 10.1109/ICACITE51222.2021.9404735.

[13] N. Kaushal, S. Singh, and J. Kumar, "Attack detection using deep learning-based multimodal biometric authentication system," *Cognitive Behavior and Human Computer Interaction Based on Machine Learning Algorithms*, pp. 157–166, 2021, doi: 10.1002/9781119792109.ch7.

[14] L. Wu, J. Yang, M. Zhou, Y. Chen, and Q. Wang, "LVID: a multimodal biometrics authentication system on smartphones," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1572–1585, 2020, doi: 10.1109/TIFS.2019.2944058.

[15] A. Abozaid, A. Haggag, H. Kasban, and M. Eltokhy, "Multimodal biometric scheme for human authentication technique based on voice and face recognition fusion," *Multimedia Tools and Applications*, vol. 78, no. 12, pp. 16345–16361, Jun. 2019, doi: 10.1007/s11042-018-7012-3.

[16] N. V. Brindha and V. S. Meenakshi, "A secured optimised AOMDV routing protocol in MANET using lightweight continuous multimodal biometric authentication," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 12, pp. 16115–16131, Dec. 2023, doi: 10.1007/s12652-022-03836-7.

[17] S. Tyagi, B. Chawla, R. Jain, and S. Srivastava, "Multimodal biometric system using deep learning based on face and finger vein fusion," *Journal of Intelligent &amp; Fuzzy Systems*, vol. 42, no. 2, pp. 943–55, 2022, doi: 10.3233/jifs-189762.

[18] V. S. Amritha and J. Aravinth, "Matcher performance-based score level fusion schemes for multi-modal biometric authentication system," in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Mar. 2020, pp. 79–85. doi: 10.1109/ICACCS48705.2020.9074446.

[19] El-Rahiem, B. Abd, F. E. El-Samie, and M. Amin, "Multimodal biometric authentication based on deep fusion of electrocardiogram (ECG) and finger vein," *Multimedia Systems*, vol. 28, no. 4, pp. 1325–37, 2021, doi: 10.1007/s00530-021-00810-9.

[20] S. P. Singh and S. Tiwari, "A dual multimodal biometric authentication system based on WOA-ANN and SSA-DBN techniques," *Sci*, vol. 5, no. 1, p. 10, Mar. 2023, doi: 10.3390/sci5010010.

[21] M. J. Sudhamani, I. Sanyal, and M. K. Venkatesha, "Artificial neural network approach for multimodal biometric authentication system," 2022, pp. 253–265. doi: 10.1007/978-981-16-6285-0_21.

[22] C. Bansong, K.-K. Tseng, K. L. Yung, and W. H. Ip, "Hierarchical attention network of multi-modal biometric for a secure cloud-based user verification," *IEEE Internet of Things Magazine*, vol. 5, no. 3, pp. 122–127, Sep. 2022, doi: 10.1109/IOTM.001.2100214.

[23] Y. Wang, D. Shi, and W. Zhou, "Convolutional neural network approach based on multimodal biometric system with fusion of face and finger vein features," *Sensors*, vol. 22, no. 16, p. 6039, Aug. 2022, doi: 10.3390/s22166039.

[24] M. A. Ayu and I. K. Y. T. Permana, "The discrete wavelet transform based iris recognition for eyes with non-cosmetic contact lens," *IAES International Journal of Artificial Intelligence*, vol. 12, no. 3, pp. 1118–1127, 2023, doi: 10.11591/ijai.v12.i3.pp1118-1127.

[25] M. M. M. Nawawi, K. A. Sidek, and A. W. Azman, "ECG biometric in real-life settings: analysing different physiological conditions with wearable smart textiles shirts," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 5, pp. 2930–2938, 2023, doi: 10.11591/eei.v12i5.5133.

BIOGRAPHIES OF AUTHORS

Sandeep Pratap Singh is pursuing Ph.D. in Computer Science from School of Computer Science, UPES Dehradun. He has completed his M.Tech. in Computer Science in 2012. His research area is biomedical image processing, security. He has published more than 14 articles in various international conferences and journals. He can be contacted at email: sandeep102209@gmail.com.

Shamik Tiwari is working as Professor in School of Computer Science, UPES Dehradun with a strong background of 20 years in computer vision, data science, predictive and statistical modelling, machine learning, and deep learning. He has published more than 100 articles in various reputed journals. He can be contacted at email: shamik.tiwari@ddn.upes.ac.in.