Design of Artificial Intelligence-Based Biometric Authentication System using Deepfake Detection Model for Patient Data Privacy Protection and Identity Verification

Louai A. Maghrabi[1,*]

[1]Department of Software Engineering, College of Engineering, University of Business and Technology, Jeddah, Saudi Arabia

Email: l.maghrabi@ubt.edu.sa

Abstract

In biometric applications, deepfake detection is a major field of research, as it is vital to certify the authenticity and integrity of biometric data. The manipulation of biometric information, like facial and fingerprint images, presents a critical attack on patient confidentiality and healthcare security. Deepfake is one of the manipulated digital media, for instance, an image or video of an individual can be substituted with a resemblance of another being. On the other hand, the growth of deepfake technology sets major attacks on biometric security by making hyper-realistic fake individualities that can deploy authentication methods. For deepfake recognition, a vital method in biometric applications utilizes a machine learning (ML) system, mainly deep learning (DL) that might study to differentiate amongst real and fake biometric data. In this manuscript, we present a Design of an Artificial Intelligence-Based Biometric Authentication System for Deepfake Detection with Patient Data Privacy Protection and Identity Verification (AIBADD-PDPPIV) algorithm. The main intention of the AIBADD-PDPPIV model is to deliver a secure and efficient biometric authentication approach that contributes to the advancement of privacy-preserving biometric security in healthcare systems. To accomplish this, the AIBADD-PDPPIV method employs an image preprocessing stage using the adaptive median filter (AMF) to reduce noise and enhance essential biometric features. For feature extraction, the vision transformer (ViT) model can be employed to capture intricate spatial dependencies in biometric images. Moreover, the multi-head attention mechanism-based bidirectional gated recurrent unit (MA-BiGRU) model is exploited for deepfake detection and authentication processes. Eventually, the hyperparameter tuning process is accomplished through the pelican optimization algorithm (POA) to improve the detection performance of the MA-BiGRU model. To show the improved performance of AIBADD-PDPPIV model, a wide sort of simulations take place and the outcomes are inspected under numerous measures. The comparison study reported the betterment of AIBADD-PDPPIV system under various metrics.

Keywords: Biometric Authentication; Deepfake Detection; Vision Transformer; Patient Data Privacy; Artificial Intelligence; Starfish Optimization Algorithm

1. Introduction

A comparatively innovative field of Artificial intelligence (AI) method named “deep fake” has obtained fame in social networking sites, which involves stratifying one person’s face over another. The comfort of accessing innovative technology has led to the extension of deepfake videos on social networking sites [1]. Deepfake is also known as a kind of artificial media in which a false subject has been created relying on a dominant subject, usually with the media people. The deepfake involved in cybercrime is fake news, disrespectful fake content videos to blackmail celebrities, cyberbullying, inciting violence, imposter swindles, financial fraud, democratic elections, cyber extortion, etc. [2]. Deepfake has been used to threaten people and entities. Deepfakes are specifically concerned with the manipulation of sounds, images, and videos, which are created with GAN (Generative Adversarial Networks) mainly with the developments of NNs (Neural Networks) [3]. Deepfake technologies

DOI: https://doi.org/10.54216/JCIM.160119
Received: November 29, 2024 Revised: January 23, 2025 Accepted: February 25, 2025

increase the progressions in the area of cross-cultural interaction, education, and entertainment, which advances not just the educational quality, then improves life's overall quality. Therefore, deepfake recognition has been completed through biometrics to improve precision and sturdiness in identifying delicate shapes and movements [4].

Biometric-based access control methods characterize a cutting-edge pattern in the realm of safety, offering an elegant means to verify and grant access based on exclusive behavioral or physiological characteristics [5]. Classical access control approaches rely on passwords, PINs, or tokens. Biometric structures influence behavioral characteristics or inherent biological that offer user-friendly and more reliable methods. Those methods aim to enhance the precision and dependability of classifying the process of verification, which makes them specifically relevant in several areas [6]. At their roots, biometric-based access control methods operate by analyzing and capturing the unique characteristics distinctive for each person. This may include a various kind of biometric procedures comprising iris patterns, fingerprints, facial characteristics, and voice recognition [7]. Face detection is one of the types of biometric security. Face detection structures may be employed in law enforcement and security for managing cybercrime. The 3 and 2D pixels-related face imaging were altered to detect faces. They were mainly designed to differentiate faces, which were associated with the figure of cheek, bone, and distances between eyes, chin, ears, and breadth of the eye socket [8]. The key concept to identifying a deepfake is to recognize an inconsistency among the faces formed by the GAN. However, researchers still use numerous techniques for the problems [9]. Present investigators display that deepfake videos and images can extremely spread over social networking sites. The deepfake recognition has become significant [10]. Consequently, numerous Deep learning (DL) approaches were invented to recognize deepfake detection in social networking media.

In this manuscript, we present a Design of an Artificial Intelligence-Based Biometric Authentication System for Deepfake Detection with Patient Data Privacy Protection and Identity Verification (AIBADD-PDPPIV) algorithm. To accomplish this, the AIBADD-PDPPIV method employs an image pre-processing stage using the adaptive median filter (AMF) to reduce noise. For feature extraction, the vision transformer (ViT) model can be employed to capture intricate spatial dependencies in biometric images. Moreover, the multi-head attention mechanism-based bidirectional gated recurrent unit (MA-BiGRU) model is exploited for deepfake detection and authentication processes. Eventually, the hyperparameter tuning process is performed through the pelican optimization algorithm (POA) to improve the detection performance of the MA-BiGRU model. To show the improved performance of the AIBADD-PDPPIV model, extensive sort of simulations take place and the outcomes are inspected under several measures.

2. Background and Related Work

Ragab et al. [11] introduced hunter-prey optimization by DL-assisted biometric verification to cyber security (HPODL-BVCS) methods in high educational institutes. The HPODL-BVCS method uses the DL structure for accomplishing biometric verification in high educational institutes. To fulfill this, the proposed technique utilizes bilateral filtering (BF) for noise removal. Then, the proposed system uses the ShuffleNet v2.3 structure for the feature removal process. In addition to this, the HPO structure was employed for the hyperparameter alteration procedures. Next, the method employs a convolutional autoencoder (CAE) structure by root RMSProp for the process of classification. Alazwari et al. [12] presented an Artificial Rabbits Optimizer by Transfer Learning Deepfake Detection for Biometric Application (AROTL-DFDBA) method. The proposed techniques aim to perceive original and fake biometric information utilizing the DL technique. Then, an adapted DarkNet 53 model is intended for the feature removal procedure. In addition, the ARO process was used for the optimum hyperparameter tuning model. Moreover, the Weighted Regularized Extreme Learning Machine (WR-ELM) procedure was used to detect deepfakes.

In [13], the novel study endeavors to provide for these serious areas by implementing and investigating a novel methodology, using Convolutional Neural Networks (CNN) for facial classification into the biometric structure. The importance of this research lies in its ability to improve safety measures in the IoT landscape, guaranteeing efficient and reliable access control. Earlier efforts at incorporating facial detection within IoT have faced prominent difficulties, containing sub-optimal precision, scalability issues, and vulnerability to adversarial attacks. Niranjani et al. [14] offer a novel deepfake detection tactic that integrates several methods, containing Photoplethysmography (PPG). To detect and classify deepfakes, our result integrates PPG through advanced DL methods. PPG registers physiological indications, improving the analysis of sounds and images. Audio fingerprinting, LSTM systems, and CNN are employed to remove characteristics from a larger dataset, which is utilized for training the systems.

Korchenko et al. [15] are dedicated to improving modular neural network pattern that offers efficient biometric authentication for people based on facial imaging, in considering the demand list. While improving models, a method was employed where the functions of each module were determined in a manner for tasks conventionally

DOI: https://doi.org/10.54216/JCIM.160119
Received: November 29, 2024 Revised: January 23, 2025 Accepted: February 25, 2025

resolved with a distinct neural network method. Lai et al. [16] presented the well-trained vision segmentation basis method. For Forgery localization and recognition, the Segment Anything Model (SAM) is deployed. According to SAM, they introduced the Detect Any Deepfakes (DADF) structure by the Multiscale Adapter, which will catch short- as well as long-range forgery context for effective fine-tuning. Furthermore, the Reconstruction Guided Attention (RGA) model was introduced to classify fake hints and increase the method's sensibility toward fake areas. The presented structure effortlessly incorporates endwise forgery recognition and localization optimizer. Furusawa and Premachandra [17] address the safety problems modeled by Generative Adversarial Networks (GANs) in biometric authentication, which focus mainly on the usage of Hyperspectral Imaging (HSI) to neutralize the risk of deepfake biometrics produced by GANs. We want answers to the problems recognized in early research namely the incapability to manage images of people and the higher time intake needed for recognition.

3. Proposed Methods

In this manuscript, we present a Design of the AIBADD-PDPPIV algorithm. The main intention of the AIBADD-PDPPIV model is to deliver a secure and efficient biometric authentication approach that contributes to the advancement of privacy-preserving biometric security in healthcare systems. To achieve that, the proposed AIBADD-PDPPIV model contains image pre-processing, extraction of features, classification, and parameter tuning models. Fig. 1 depicts the complete working process of the AIBADD-PDPPIV method.

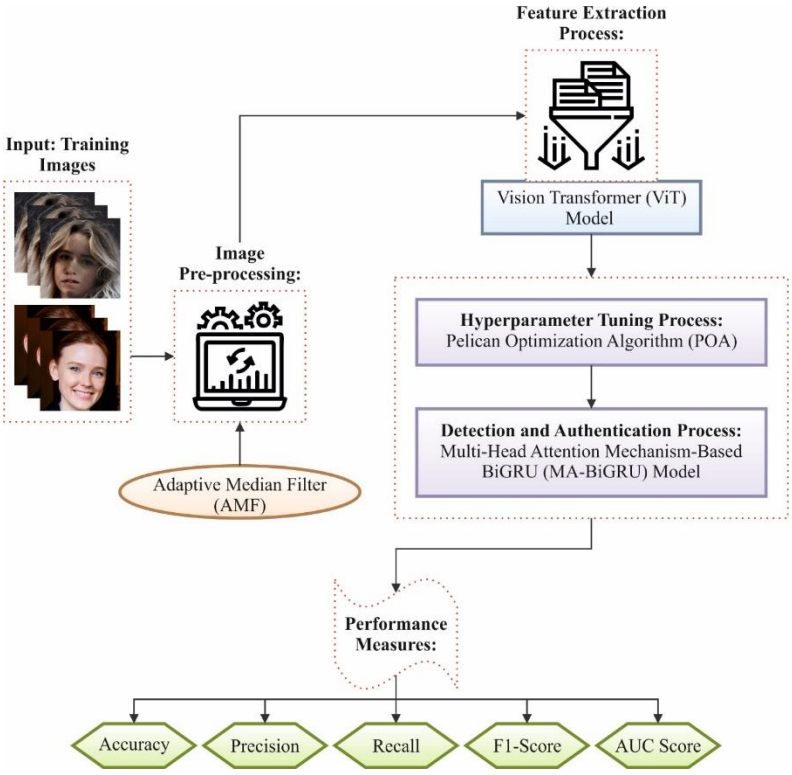

Figure 1. Overall Working Flow Process of AIBADD-PDPPIV model

A. Image Pre-processing

Initially, the pre-processing stage of an image applies AMF to reduce noise and enhance essential biometric features. AMF proposed the model for dynamical modification of either the threshold value or size of the window for every individual pixel reliant on its neighborhood [18]. Although MF employs a fixed window size that can turn result in the loss of detailed and major data, image features, important edges, and window size are made to be maintained appropriately. Consequently, while the image is in higher densities, AMF executes better than the other approaches owing to its capability to decrease sound without losing substantial aspects. Once an image has been corrupted by sound, diverse parts of an image have dissimilar noisy levels of intensity. Thus, areas with lower levels of noise are filtered with a smaller sliding window, whereas regions with greater noise levels necessitate a larger size of filter. Hence, if filtering is executed, then the filter size must be fine-tuned based on the level of noise. This kind of filtering is known as AMF. Nevertheless, filters generally begin with a window size of 3x3

DOI: https://doi.org/10.54216/JCIM.160119
Received: November 29, 2024 Revised: January 23, 2025 Accepted: February 25, 2025

pixels. The dimension of the window maximizes based on the procedure and ends up rising equivalently to a specific condition.

B. ViT-based Feature Extraction Model

Then, the ViT model can be employed to capture intricate spatial dependencies in biometric images for feature extraction. Primarily, transformers were examined for natural language processing (NLP) and subsequently explored in time series forecasting, speech processing, computer vision (CV), generative architecture, classification and much more owing to their exceptional capability to acquire contextual data and longer dependency [19]. Moreover, it surpasses prominent LSTM and RNN in various applications. Additionally, the structure of the transformer resists the vanishing gradient problem, which hampers the training since the beginning. In this regard, ViTs formed a model change to CV by displaying the excellent performance of CNN with the stimulus to self-attention. ViTs can learn multi-dimensional intricate aspects over self-attention mechanisms. Likewise, ViTs handle inductive bias more, effectually which enhances either reliability or scalability. Explicitly, ViTs concentrate more on global aspects than local characteristics, In the structure point, ViTs only focus on the encoder with embedded patches, while the transformer contains positional encoding, input embedding, decoder, and encoder.

A novel analysis is implementing a transformer framework for difficult wireless concerns to specify the possible direction for challenging subjects. The authors examine transformer for time series prediction, particularly for management and interference prediction, here the transformer model surpasses auto-regressive integrated moving average (ARIMA) and LSTM by a substantial margin. ViTs are implemented in a broad array of applications. The authors introduce mobile positioning for 6G employing ViTs, while the model examines the angle-delay channel power matrix (ADCPM) through various BSs. Besides, the authors underline the proficiency of ViTs's attention mechanism for learning the multi-dimensional and sparse features. A multi-model vehicle-to-everything (V2X) structure is projected in employing ViTs to forecast the future blocking ages in LoS, enhancing antenna position optimization and beam direction. Likewise, the authors present a blockage prediction technique for vehicular networks employing ViTs and CNN. In addition, an automated modulation classification utilizing ViTs is projected in the attention mechanism employed to concentrate on the respective field of the input sequence and improve the classification precision. For spectrum monitoring, a structure for spectrum prediction utilizing flow-processing models with ViTs is projected, here the visual representation of the spectrogram is inspected. Fig. 2 represents the ViT model.

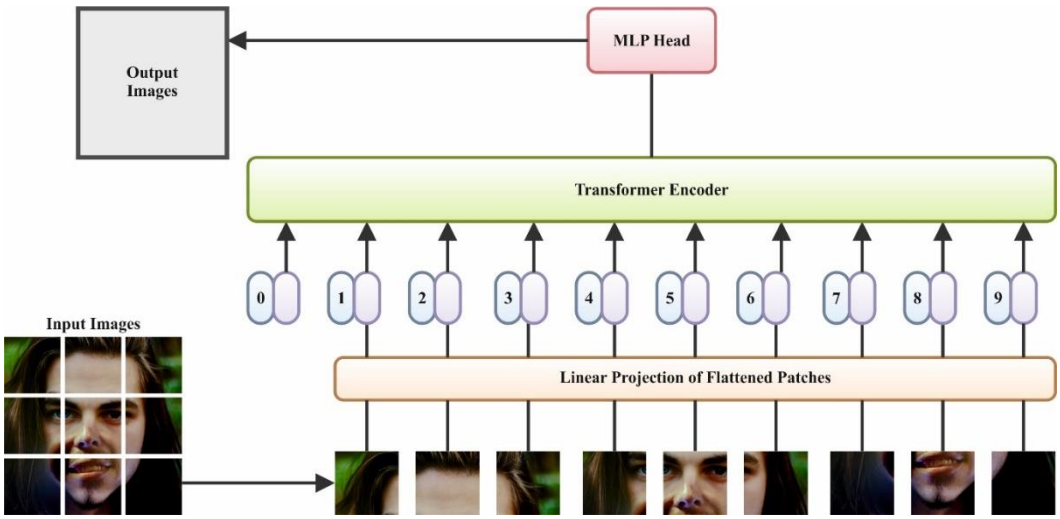

Figure 2. Structure of ViT model

C. Classification Process using MA-BiGRU Technique

Furthermore, the MA-BiGRU model is developed for deepfake detection and authentication procedures. The MA-Bi-GRU technique is made from a multi-head attention mechanism and Bi-GRU is intended to enhance stability and accuracy [20]. It integrates the assets of GRU and bi-directional recurrent neural networks (Bi-RNN). The hybrid approach improves the capability to acquire longer-term dependency and dynamical modifications in time series data, so upgrading feature learning over training.

DOI: https://doi.org/10.54216/JCIM.160119
Received: November 29, 2024 Revised: January 23, 2025 Accepted: February 25, 2025

$$\vec{h}_t = GRU\left(x_t, \overrightarrow{h_{t-1}}\right) \quad (1)$$

$$\overleftarrow{h}_t = GRU\left(x_t, \overleftarrow{h_{t-1}}\right) \quad (2)$$

$$h_t = f\left(W_{\vec{h}_t}\vec{h}_t + W_{\overleftarrow{h}_t}\overleftarrow{h}_t + b_t\right) \quad (3)$$

Here x_t represent the vector of input at moment t, $\overleftarrow{h}_t$ and $\vec{h}_t$ backward and forward states of the hidden layer (HL) at moment t, correspondingly, $W_{\overleftarrow{h}_t}$ and $W_{\vec{h}_t}$ are the weight of reverse and forward states of HL at moment t, correspondingly, and b_t is the bias of HL at moment t. h_t represents the HL state at moment t. As the NN technique increases in difficulty and number of parameters, they risk data overload, despite amplified expressive power. The attention mechanism reduces this by allocating weighted parameters, permitting the methodology to concentrate on key data and minimize prominence on lesser relevant information. This decreases data redundancy and increases the efficacy of the model. A single attention mechanism can be struggling with intricate semantical relations. The multi-head attention mechanism tackles this by utilizing multiple self-attentive sub-layers, acquiring data from diverse levels and perspectives, thus improving the perception of a model of global data. In the model of MA-Bi-GRU, the output of the Bi-GRU layer functions as the input for key (K), value (V), and query (Q) matrices in every self-attention mechanism.

$$head_i = Attention\left(QW_i^Q, KW_i^K, VW_i^V\right) \quad (4)$$

$$MultiHead(Q,K,V) = concat(head_1, \ldots, head_h \quad (5)$$

Here W^Q, W^K, W^V are the weighted matrix and h represents the number of heads.

D. POA-based Parameter Tuning Method

At last, the hyperparameter tuning process is made through POA to progress the detection performance of the MA-BiGRU model. The POA is a group-based model that contains pelicans as members of its bird population [21]. Among group-based models, every individual in the group signifies a possible solution. Each individual in the group proposes values for the variables of optimization concern depending on their position in the searching area. The following steps are expressed for implementing POA:

1. The population individuals are initialized arbitrarily in the particular upper and lower bounds of the problem described in the succeeding equation,

$$x_{i,j} = l. + rand.\left(u_j - l_j\right), i = 1,2,\ldots,N,\ j = 1,2,\ldots,m \quad (6)$$

The value of jth variable described by the ith solution of a candidate is depicted by $x_{i,j}$. N relates to the population member counts, m specifies the problem variable counts, $rand$ represents an arbitrary number with a range of 0 to 1, l_j is the lower bound of jth variable, and u_j denotes the upper limit of jth variable in the problem. The matrix named the population matrix is expressed by Eq. (7), which establishes the population members of pelicans in the POA.

$$X = \begin{bmatrix} X_1 \\ \vdots \\ X_i \\ \vdots \\ X_N \end{bmatrix}_{N\times m} = \begin{bmatrix} x_{1,1} & \cdots & x_{1,j} & \cdots & x_{1,m} \\ & & \vdots & & \\ x_{i,1} & \cdots & x_{i,j} & \cdots & x_{i,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{N,1} & \cdots & x_{N,j} & \cdots & x_{N,m} \end{bmatrix}_{N\times m} \quad (7)$$

The pelican's population matrix is represented as X, whereas X_i is the ith pelican.

2. In the POA, each individual in the population depicted a pelican and functions as a possible solution to the respective problem. A vector called the objective vector function is described:

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} F(x_1) \\ \vdots \\ F(x_i) \\ \vdots \\ F(x_N) \end{bmatrix}_{N\times 1} \quad (8)$$

The objective vector function indicated as F, depicts the huge amount of objective function values for every solution of a candidate, here F_i is the objective function value of ith solution of a candidate.

3. The POA mimics the strategies and actions of pelicans in their pursuit and acquiring prey to enhance possible solutions. The search model can be emulated in dual stages:

DOI: https://doi.org/10.54216/JCIM.160119
Received: November 29, 2024 Revised: January 23, 2025 Accepted: February 25, 2025

a) Moving towards prey (exploration phase)

During this stage, the pelicans determine the location of their prey and then proceed to the specified site. The POA arbitrarily generates the position of prey in the searching area, improving its exploratory ability in accurately hunting the domain of problem-solving. It upgrades the exploratory ability of POA in accurately exploring the domain of problem-solving.

$$x_{i,j}^{P_1} = \begin{cases} x_{i,j} + rand.\left(p_j - I.x_{i,j}\right), & F_p < F_i; \\ x_{i,j} + rand.\left(x_{i,j} - p_j\right), & else, \end{cases} \quad (9)$$

Now, $x_{i,j}^{P_1}$ is the existing status of ith pelican in ith dimension through stage 1. The value of I specifies a random number which can be both one and two. p_j is the position of prey in ith dimension, here F_p denotes a value of an objective function. Allocate a numerical value arbitrarily to both 1 and 2 for the parameter I. Therefore, the parameter I directly impacts the ability of POA to precisely and effectively study the searching area.

The POA assumes the novel position for a pelican if it outcomes in the value of an objective function.

$$x_i = \begin{cases} x_i^{P_1}, F_p < F_i^{P_1} < F_i; \\ x_i, else, \end{cases} \quad (10)$$

The upgraded state of ith pelican is depicted by $x_i^{P_1}$, whereas its value of objective function originating from 1st stage is specified by $F_i^{P_1}$.

b) Winging on the water surface (exploitation phase).

In this stage, pelicans utilize their wings to transfer fish upward on the water's surface, gathering prey in their pouch of the throat, thus acquiring more fish in the assaulted region. The procedure of pretending this behavior of pelicans outcomes in the point of attraction (PoA) converging to a more optimum position with the searching space. This model improves the local searching ability and exploitation possibility of POA. The foraging behavior of pelicans is quantitatively recreated.

$$x_{i,j}^{P_2} = x_{i,j} + R.\left(1 - \frac{t}{T}\right).(2.rand - 1).x_{i,j}. \quad (11)$$

Here $x_{i,j}^{P_2}$, is the upgraded status of ith pelican in the ith dimension through the 2nd stage. The constant R is equal to 0.2 and. $\left(1 - \frac{t}{T}\right)$, is the adjacent radius of $x_{i,j}$. Now, T specifies the iteration counter and denotes the maximal iteration counts. The co-efficient $R.\left(1 - \frac{t}{T}\right)$, shows the radius of a member of the population which is hunted locally around every member to converge a more optimum solution. The coefficient $R.\left(1 - \frac{t}{T}\right)$ declines to the reduction of neighborhoods for every member which allows us to investigate the neighboring region of every individual in the population employing lesser and more accurate increments. Consequently, the POA can converge to solutions which is closer to the global optimum solution, and an ideal reliant on the concept of employment that is global accurately.

$$x_i = \begin{cases} x_i^{P_2}, F_p < F_i^{P_2} < F_i; \\ x_{i'}\ else, \end{cases} \quad (12)$$

The variable $x_i^{P_2}$ is the upgraded status of ith pelican, here $F_i^{P_2}$ denote its value of an objective function in 2nd stage.

4. This model upgrades the finest solution of the candidate depending on the existing status of a population and the values of objective function when each individual in the population are upgraded based on the subsequent and initial phases. Until the overall execution is accomplished, the model proceeds to the subsequent iteration and repeats the numerous stages of POA described by Eqs. (9 to 12).

The POA method develops a fitness function (FF) for attaining a performance of classification. It describes a positive digit to mean the better outcome of the candidate solution. The classifier error rate minimization is dignified as FF, which is formulated in Eq. (13).

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{no.of\ misclassified\ samples}{Total\ no.of\ samples} * 100 \quad (13)$$

DOI: https://doi.org/10.54216/JCIM.160119
Received: November 29, 2024 Revised: January 23, 2025 Accepted: February 25, 2025

4. Experimental Result and Analysis

This section examines the performance analysis of the AIBADD-PDPPIV model under the Real and Fake Face detection dataset [22]. This dataset contains 2041 no. of face images under two faces such as fake and real. The complete details of this dataset are shown in Table 1. The sample images are shown in Fig. 3.

Table 1: Details of dataset

Faces	Face Images
Fake	960
Real	1081
Total	2041

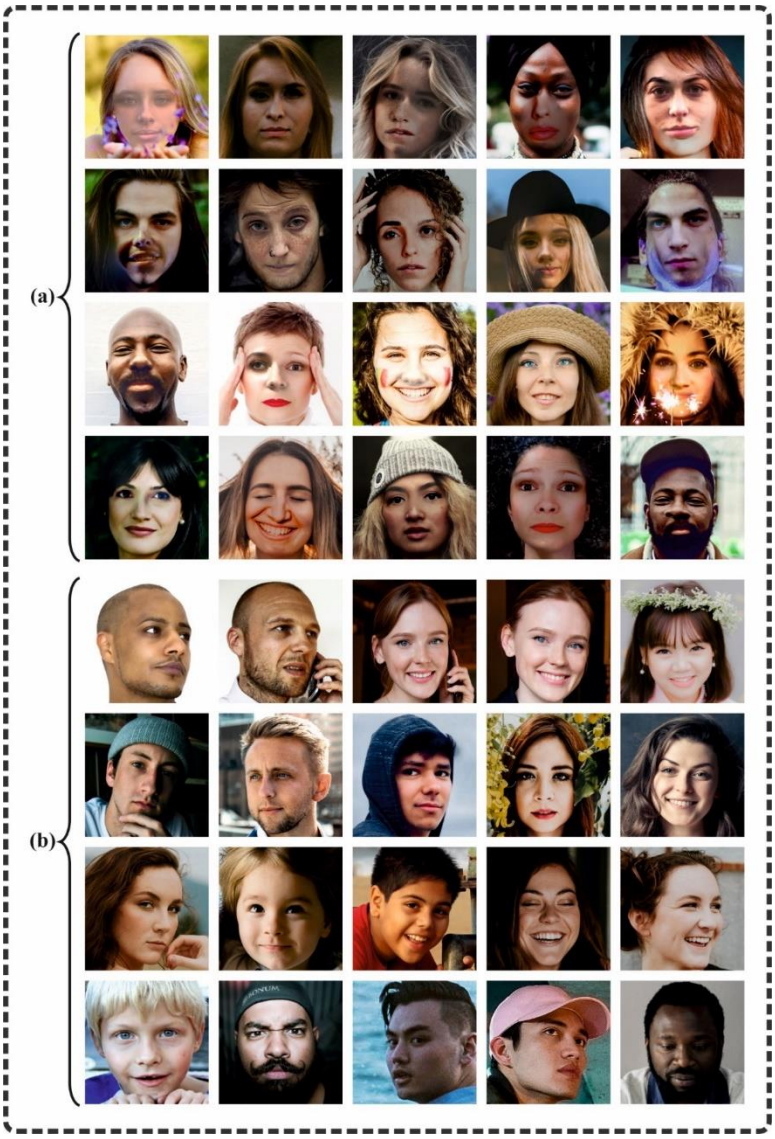

Figure 3. Sample Images

DOI: https://doi.org/10.54216/JCIM.160119
Received: November 29, 2024 Revised: January 23, 2025 Accepted: February 25, 2025

The deepfake detection outcome of AIBADD-PDPPIV system under 70%TRPHA and 30%TSPHA is shown in Table 2. The table values indicate that the AIBADD-PDPPIV technique has properly identified the samples. With 70%TRPHA, the AIBADD-PDPPIV technique offers an average $accu_y$, $prec_n$, $reca_l$, $F1_{score}$, and AUC_{score} of 99.17%, 99.14%, 99.17%, 99.16%, and 99.17%, correspondingly. Furthermore, based on 30% TSPHA, the AIBADD-PDPPIV algorithm provides average $accu_y$, $prec_n$, $reca_l$, $F1_{score}$, and AUC_{score} of 99.21%, 99.16%, 99.21%, 99.18%, and 99.21%, respectively.

Table 2: Deepfake detection outcome of AIBADD-PDPPIV system under 70%TRPHA and 30%TSPHA

Class Labels	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{score}$	AUC_{score}
TRPHA (70%)					
Fake	99.41	98.82	99.41	99.11	99.17
Real	98.94	99.47	98.94	99.20	99.17
Average	99.17	99.14	99.17	99.16	99.17
TSPHA (30%)					
Fake	99.65	98.62	99.65	99.13	99.21
Real	98.77	99.69	98.77	99.23	99.21
Average	99.21	99.16	99.21	99.18	99.21

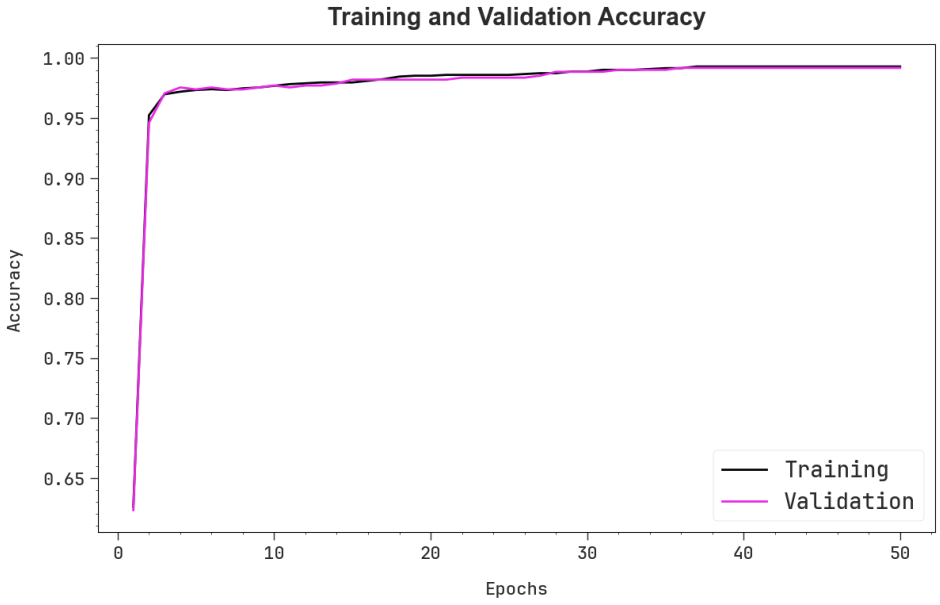

Figure 4. $Accu_y$ Analysis of AIBADD-PDPPIV model

DOI: https://doi.org/10.54216/JCIM.160119
Received: November 29, 2024 Revised: January 23, 2025 Accepted: February 25, 2025

In Fig. 4, the training (TRA) $accu_y$ and validation (VAL) $accu_y$ outcomes of the AIBADD-PDPPIV technique is exemplified. The values of $accu_y$ are computed for 0-50 epochs. The figure highlights that both $accu_y$ analysis shows a rising tendency that notified the ability of the AIBADD-PDPPIV methodology with higher performance across several iterations. Additionally, the both $accu_y$remains closer across the epochs, which indicates lesser overfitting and exhibits enhanced performance of the AIBADD-PDPPIV model.

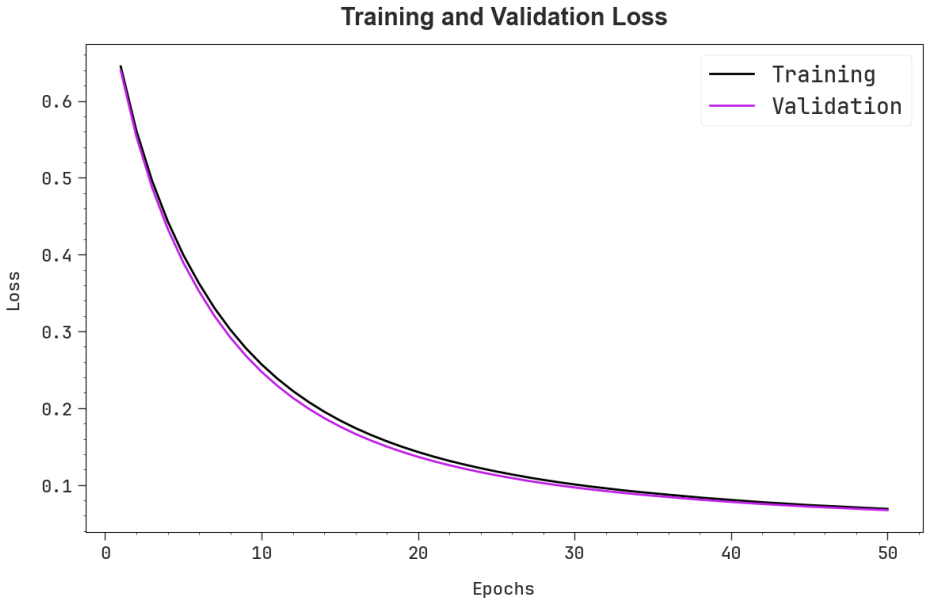

Figure 5. Loss graph of AIBADD-PDPPIV algorithm

In Fig. 5, the TRA loss (TRALOS) and VAL loss (VALLOS) graph of the AIBADD-PDPPIV technique is exhibited. The loss values are calculated within the range of 0-50 epochs. It is signified that both values illustrate a reducing tendency, informing the capability of the AIBADD-PDPPIV model in balancing a trade-off amongst data fitting and generalization. The constant decrease in loss values likewise guarantees the optimal performance of the AIBADD-PDPPIV algorithm and tunes the prediction outcomes over time.

The comparative outcomes of the AIBADD-PDPPIV approach with existing systems are illustrated in Table 3 and Fig. 6 [23, 24]. Based on $accu_y$, the AIBADD-PDPPIV technique has better $accu_y$ of 99.21% while the CED-DCGAN, GAN-based generators, 3D CNN, HASSO, VGG16, ResNET-50, and HDL-GRDFF system have obtained lesser $accu_y$ of 95.26%, 96.22%, 98.84%, 93.38%, 93.28%, 94.97%, and 95.98%, respectively. Besides, depend upon $Prec_n$ of 99.16% where the CED-DCGAN, GAN-based generators, 3D CNN, HASSO, VGG16, ResNET-50, and HDL-GRDFF approach have accomplished lower $Prec_n$ of 93.74%, 98.89%, 92.83%, 96.57%, 93.19%, 90.96%, and 92.71%, correspondingly. Moreover, with respect to $Reca_l$ of 99.21% whereas the CED-DCGAN, GAN-based generators, 3D CNN, HASSO, VGG16, ResNET-50, and HDL-GRDFF methodology have achieved minimal $Reca_l$ of 95.26%, 96.17%, 91.19%, 93.83%, 96.28%, 91.98%, 92.11%, and 95.34%, respectively. Also, based on $F1_{score}$ of 99.18% while the CED-DCGAN, GAN-based generators, 3D CNN, HASSO, VGG16, ResNET-50, and HDL-GRDFF technique have gained inferior $F1_{score}$ of 95.63%, 92.63%, 90.53%, 98.71%, 92.30%, 96.84%, and 96.97%, correspondingly.

Table 3: Comparative results of AIBADD-PDPPIV approach with existing classifiers

Technique	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{score}$
CED-DCGAN	95.26	93.74	96.17	95.63
GAN-based generators	96.22	98.89	91.19	92.63

DOI: https://doi.org/10.54216/JCIM.160119
Received: November 29, 2024 Revised: January 23, 2025 Accepted: February 25, 2025

3D CNN	98.84	92.83	93.83	90.53
HASSO	93.38	96.57	96.28	98.71
VGG16 Method	93.28	93.19	91.98	92.30
ResNET-50	94.97	90.96	92.11	96.84
HDL-GRDFF	95.98	92.71	95.34	96.97
AIBADD-PDPPIV	99.21	99.16	99.21	99.18

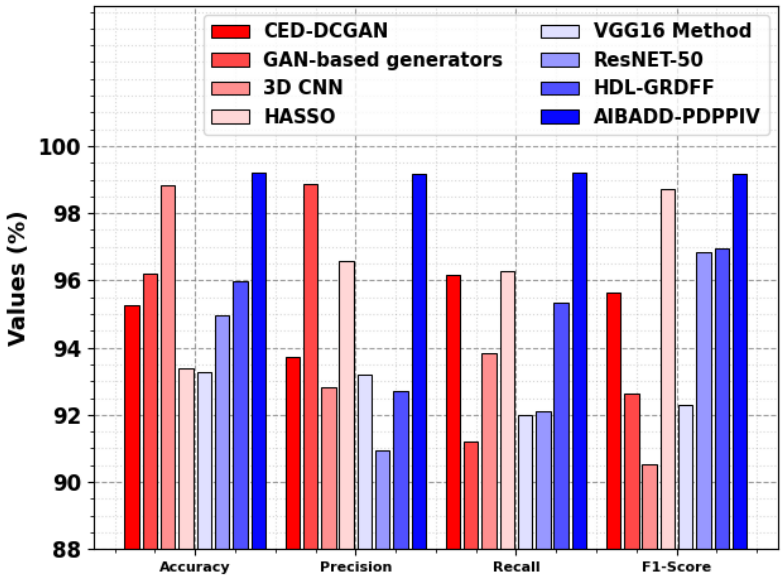

Figure 6. Comparative analysis of AIBADD-PDPPIV model with existing classifiers

Table 4 and Fig. 7 depict the processing time (PT) result of the AIBADD-PDPPIV method with existing algorithms are established. Based on PT, the AIBADD-PDPPIV approach offers lower PT of 6.02sec whereas the CED-DCGAN, GAN-based generators, 3D CNN, HASSO, VGG16, ResNET-50, and HDL-GRDFF system attain greater PT of 27.05sec, 26.01sec, 23.33sec, 21.69sec, 10.40sec, 24.24sec, and 7.53sec, correspondingly.

Table 4: PT outcome of AIBADD-PDPPIV method with existing models

Technique	Processing Time (sec)
CED-DCGAN	27.05
GAN-based generators	26.01

DOI: https://doi.org/10.54216/JCIM.160119
Received: November 29, 2024 Revised: January 23, 2025 Accepted: February 25, 2025

3D CNN	23.33
HASSO	21.69
VGG16 Method	10.40
ResNET-50	24.24
HDL-GRDFF	7.53
AIBADD-PDPPIV	6.02

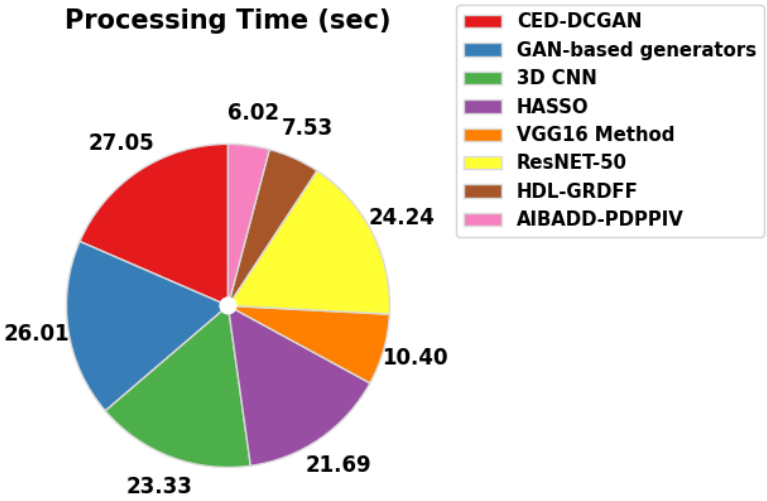

Figure 7. PT outcome of AIBADD-PDPPIV method with existing models

5. Conclusion

In this manuscript, we present a Design of the AIBADD-PDPPIV algorithm. The primary goal of the AIBADD-PDPPIV model is to provide a secure and efficient biometric authentication approach that contributes to the advancement of privacy-preserving biometric security in healthcare systems. To accomplish this, the AIBADD-PDPPIV method employs an image pre-processing stage using the AMF to reduce noise and enhance essential biometric features. For feature extraction, the ViT model can be employed to capture intricate spatial dependencies in biometric images. Moreover, the MA-BiGRU model is exploited for deepfake detection and authentication processes. Eventually, the hyperparameter tuning process is performed through POA to improve the detection performance of the MA-BiGRU model. To demonstrate the improved performance of the AIBADD-PDPPIV model, a wide sort of simulations take place and the outcomes are inspected under several measures. The comparison study reported the betterment of the AIBADD-PDPPIV system under various metrics.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

DOI: https://doi.org/10.54216/JCIM.160119
Received: November 29, 2024 Revised: January 23, 2025 Accepted: February 25, 2025

References

[1] S. Alazwari et al., "Artificial rabbits optimization with transfer learning-based deepfake detection model for biometric applications," *Ain Shams Engineering Journal*, vol. 15, no. 12, p. 103057, 2024.

[2] S. T. Suganthi et al., "Deep learning model for deep fake face recognition and detection," *PeerJ Computer Science*, vol. 8, p. e881, 2022.

[3] S. Agarwal, H. Farid, T. El-Gaaly, and S. N. Lim, "Detecting deep-fake videos from appearance and behavior," in *2020 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2020, pp. 1–6.

[4] T. L. Do, M. K. Tran, H. H. Nguyen, and M. T. Tran, "Potential Attacks of DeepFake on eKYC Systems and Remedy for eKYC with DeepFake Detection Using Two-Stream Network of Facial Appearance and Motion Features," *SN Computer Science*, vol. 3, no. 6, p. 464, 2022.

[5] S. Ramachandran, A. V. Nadimpalli, and A. Rattani, "An experimental evaluation on deepfake detection using deep face recognition," in *2021 International Carnahan Conference on Security Technology (ICCST)*, 2021, pp. 1–6.

[6] A. Mitra, S. P. Mohanty, P. Corcoran, and E. Kougianos, "iFace: a deepfake resilient digital identification framework for smart cities," in *2021 IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 361–366.

[7] A. Malik, M. Kuribayashi, S. M. Abdullahi, and A. N. Khan, "DeepFake detection for human face images and videos: A survey," *IEEE Access*, vol. 10, pp. 18757–18775, 2022.

[8] R. Salariya and D. Malhotra, "ADFB: Anti-deepfake Framework for Facial Biometric Authentication Systems," in *The International Conference on Recent Innovations in Computing*, Singapore: Springer Nature Singapore, 2023, pp. 233–255.

[9] C. Z. Yang, J. Ma, S. Wang, and A. W. C. Liew, "Preventing deepfake attacks on speaker authentication by dynamic lip movement analysis," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1841–1854, 2020.

[10] G. Guarnera, B. Giudice, and S. Battiato, "Deepfake detection by analyzing convolutional traces," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, 2020, pp. 666–667.

[11] M. Ragab et al., "Enhancing cybersecurity in higher education institutions using optimal deep learning-based biometric verification," *Alexandria Engineering Journal*, vol. 117, pp. 340–351, 2025.

[12] A. V. Srinivas et al., "Deepfake Detection Based on Temporal Analysis of Facial Dynamics Using LSTM and ResNeXt Architectures," *Journal of Image Processing and Intelligent Remote Sensing*, vol. 4, no. 03, pp. 47–54, 2024.

[13] B. S. Babu et al., "Biometric-Based Access Control Systems with Robust Facial Recognition in IoT Environments," in *2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, 2024, pp. 1–6.

[14] V. Niranjani, S. Aishwarya, T. Devamitra, and B. Jagapreetha, "Deep Fake Detection: Unmasking the illusion using CNN and LSTM," in *2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, 2023, pp. 861–865.

[15] O. Korchenko et al., "Modular Neural Network Model for Biometric Authentication of Personnel in Critical Infrastructure Facilities Based on Facial Images," *Applied Sciences*, vol. 15, no. 5, p. 2553, 2025.

[16] Y. Lai, Z. Luo, and Z. Yu, "Detect any deepfakes: Segment anything meets face forgery detection and localization," in *Chinese Conference on Biometric Recognition*, Singapore: Springer Nature Singapore, 2023, pp. 180–190.

[17] S. Furusawa and C. Premachandra, "High-Performance Face Identification using Hyperspectral Imaging to Counteract Deep Fake Biometrics," in *2024 Eighth IEEE International Conference on Robotic Computing (IRC)*, 2024, pp. 186–189.

DOI: https://doi.org/10.54216/JCIM.160119
Received: November 29, 2024 Revised: January 23, 2025 Accepted: February 25, 2025

[18] F. Ullah, K. Kumar, T. Rahim, J. Khan, and Y. Jung, "A new hybrid image denoising algorithm using adaptive and modified decision-based filters for enhanced image quality," *Scientific Reports*, vol. 15, no. 1, p. 8971, 2025.

[19] T. Sivalingam et al., "Novel Learning-Based Multi-User Detection Algorithms for Spatially Correlated MTC," *IEEE Internet of Things Journal*, 2025.

[20] Q. Pan et al., "Interpretable machine learning for thermospheric mass density modeling using GRACE/GRACE-FO satellite data," *Space Weather*, vol. 23, no. 3, p. e2024SW004259, 2025.

[21] S. W. Mahmood, G. T. Basheer, and Z. Y. Algamal, "Improving kernel ridge regression for medical data classification based on meta-heuristic algorithms," *Kuwait Journal of Science*, p. 100408, 2025.

[22] "Real and Fake Face Detection Dataset," [Online]. Available: https://www.kaggle.com/datasets/ciplab/real-and-fake-face-detection?select=real_and_fake_face.

[23] S. K. Sharma, A. AlEnizi, M. Kumar, O. Alfarraj, and M. Alowaidi, "Detection of real-time deep fakes and face forgery in video conferencing employing generative adversarial networks," *Heliyon*, vol. 10, no. 17, 2024.

[24] S. Safwat, A. Mahmoud, I. E. Fattoh, and F. Ali, "Hybrid Deep Learning Model Based on GAN and RESNET for Detecting Fake Faces," *IEEE Access*, 2024.

DOI: https://doi.org/10.54216/JCIM.160119
Received: November 29, 2024 Revised: January 23, 2025 Accepted: February 25, 2025