Journal of Discrete Mathematics and Its Applications 11 (1) (2026) 13–32

Journal of Discrete Mathematics and Its Applications

Available Online at: http://jdma.sru.ac.ir

Shahid Rajaee Teacher Training University

Research Paper

Enhancing ECG-based authentication systems using VGG16 model and transfer learning

Narges Eshaghi[1], **Mohammad Habibi**[1,*], **Nasour Bagheri**[2], **Ali Khatibi**[3]

[1] Department of Mathematics, Tafresh University, Tafresh 39518-79611, Iran

[2] Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran 16788-15811, Iran

[3] Department of Mechanical Engineering, Tafresh University, Tafresh 39518-79611, Iran

Academic Editor: Nader Jafari-Rad

Abstract. This study explores a novel authentication algorithm leveraging ECG signals and deep learning models, specifically VGG16, enhanced with transfer learning. Authentication systems were evaluated based on preparation time, response time, and accuracy, with biometric data utilized to increase security. Traditional deep learning models face challenges in retraining time when data changes, prompting the proposed algorithm to incorporate new users or modify access efficiently using transfer learning. Key findings included training the VGG16 model on ECG data from 48 individuals (MITDB dataset) with a 99.45% accuracy and 120 seconds average training time. The transfer learning approach enabled adding or removing user data by adjusting a modified (1:1 matching) SoftMax coefficients, reducing training time significantly to about 12 seconds per user with accuracy exceeding 99%. Removing a user followed a similar process with comparable results. Overall, the algorithm reduced retraining time by 72.89% while maintaining over 99.16% accuracy. Additionally, the system's response time for a new user was 37 milliseconds, demonstrating practicality for real-time applications. The study highlights the proposed algorithm's efficiency in managing user data changes while ensuring high accuracy and reduced retraining time, making it a robust solution for modern authentication systems.

Keywords. graph, eccentricity, diameter.

[*] Corresponding author (Email address: mhabibi@tafreshu.ac.ir).

Received 28 September 2025; Revised 08 October 2025; Accepted 14 October 2025
First Publish Date: 01 March 2026

Mathematics Subject Classification (2020): 05C07, 05C09.

1 Introduction

Biometric authentication has emerged as a reliable method for verifying individual identities by utilizing unique physiological and behavioral traits. This technology has evolved from traditional password systems to more secure biometric modalities, enhancing user experience and security across various applications, including healthcare, finance, and law enforcement [23]. On the other hand, deep learning (DL) has significantly transformed authentication methods, particularly in biometric systems, enhancing security and efficiency. By leveraging advanced algorithms, DL can analyze complex biometric data, leading to more reliable identification processes. DL models, particularly Convolutional Neural Networks (CNNs), have been employed to enhance fingerprint authentication, achieving accuracy rates of up to 99.8% [31]. DL models can generate cryptographic keys from facial images, eliminating the need for traditional key storage and enhancing security measures [11]. Also, DL techniques, such as the AlexNet model, have been applied for personal recognition, achieving an accuracy of 98% in real-time applications [1]. Different DL algorithms have been used in biometric authentication systems, one of which is the VGGNet model.

VGGNet, originally designed for image classification, is a convolutional neural network (CNN) characterized by its deep architecture and small receptive fields. Its structure typically consists of multiple convolutional layers followed by fully connected layers, utilizing ReLU activation functions and max pooling for down-sampling. The architecture's depth allows it to capture intricate features, making it suitable for various applications, including medical imaging and traffic sign recognition. The application of VGGNet in biometric authentication has shown significant advancements across various modalities, including face [6], fingerprint [12], and iris [19] recognition. VGGNet's deep architecture enables the extraction of hierarchical features, enhancing the accuracy and robustness of biometric systems. VGGNet employs a series of convolutional layers (3×3 filters) followed by max pooling layers, culminating in fully connected layers. Common variants include VGG-16 and VGG-19, differing in the number of layers, which enhances feature extraction capabilities. VGGNet employs 2 to 4 convolution operations per layer, significantly increasing the depth compared to earlier models like AlexNet, which used larger kernels (7×7) and fewer layers. Most parameters are concentrated in the fully connected layers, which can lead to a high number of total parameters, making the model computationally intensive [24]. The VGG16 model structure is shown in Figure 1.

The VGGNet has emerged as a significant architecture in biometric applications, particularly in face recognition, liveness detection, and fingerprint-based encryption. Its deep learning capabilities allow for effective feature extraction and classification, enhancing the accuracy and reliability of biometric systems. VGG19 has been integrated into hybrid models to improve face recognition accuracy, leveraging its depth for hierarchical feature learning. Studies demonstrate that VGG architectures outperform traditional CNNs in various face recognition tasks, achieving high accuracy rates on standard datasets [6]. VGG16 and VGG19 have

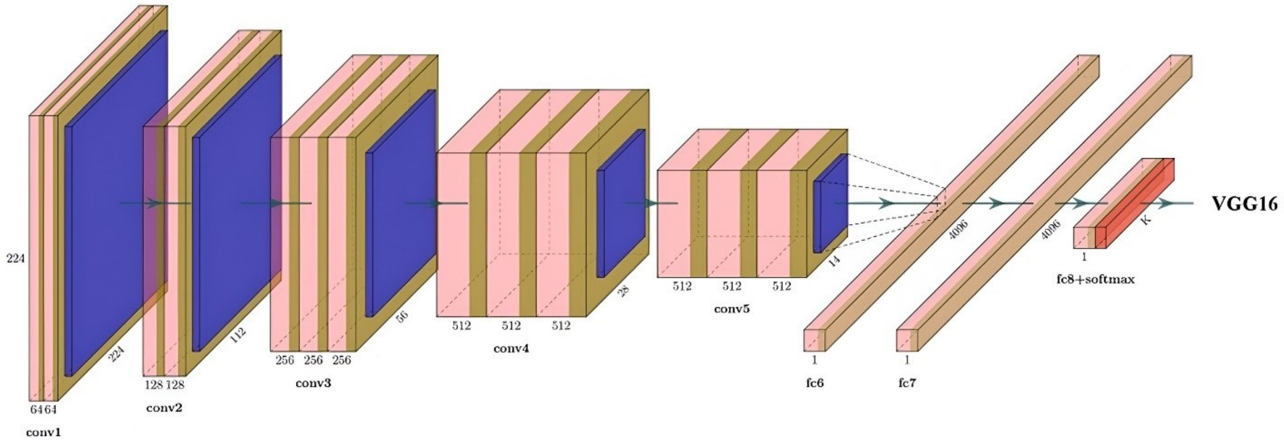


Figure 1. The structure of the VGG16 used in this study (Each conv in this figure shows a frame to scroll the input image. Also, the numbers indicating the width and height illustrate the dimension of the frame and the depth number shows the numbers of nodes in the relevant layer) [32].

been fine-tuned for face liveness detection, achieving a testing accuracy of 100% in specific scenarios. The models were evaluated using diverse datasets, highlighting their effectiveness in distinguishing between live and spoofed faces [29]. A modified VGG-16 model has been utilized to generate secure encryption keys from fingerprint images, achieving over 99% accuracy. This approach emphasizes the potential of VGGNet in enhancing security through biometric encryption [8]. The Mini-VGG architecture has been applied to iris recognition, yielding impressive results with accuracy, precision, and recall rates of 98%, 0.99, and 0.99, respectively. The unique characteristics of iris patterns make them suitable for high-security applications, further demonstrating VGGNet's versatility [21]. One of the key challenges in biometric VGGNet-based authentication systems (and generally in DL-based authentication systems) is adding and removing users. In general, the approaches used to perform these two operations can affect the model execution time and its accuracy [26]. For example, it could consider a situation where a user's access needs to be restricted, if this process requires retraining the whole model, the system will be suspended until the new model is ready, or it will not detect unauthorized access. One suggested approach that can be used for this purpose is the use of transfer learning (TL).

TL models leverage knowledge gained from one task to improve performance on another. This approach is particularly beneficial in scenarios where data is scarce or expensive to obtain. The structure of TL models can vary significantly depending on the application, but they generally consist of a source model, a target model, and a transfer mechanism that facilitates knowledge sharing. The source model is trained on a large dataset, while the target model is adapted to a smaller. For instance, in microwave structure behavior prediction, a high-performance model is developed to expedite predictions using TL, significantly reducing data requirements and training time [16]. This mechanism allows the model to transfer learned features or parameters from the source to the target. In Bayesian transfer learning, a dual-modeler framework is employed, enhancing robustness against model misspecification by conditioning the target on the source's predictive distribution [22]. The general concept of transfer learning is shown in Figure 2.

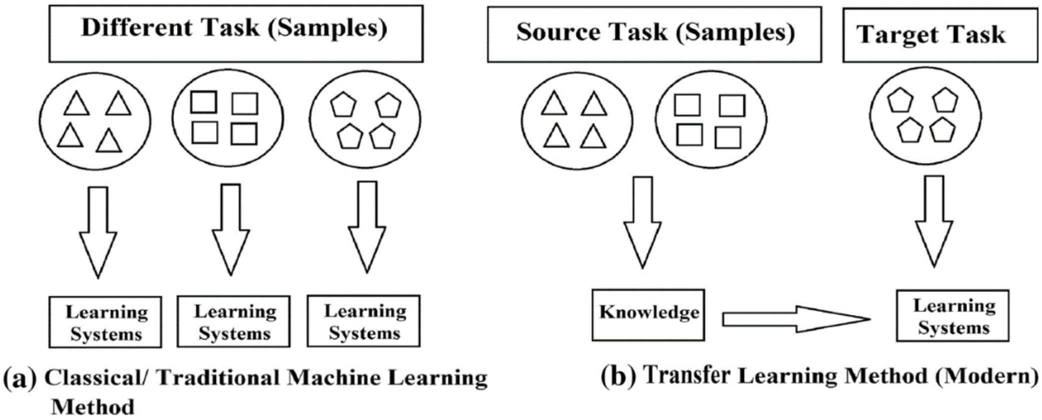


Figure 2. The concepts of classic machine learning (a) and transfer learning (b) [10].

In this research, a novel algorithm for user adding and removing in a biometric VGG16-based authentication system using transfer learning is introduced and examined. As a result, the main question we seek to answer in this research is whether using the proposed algorithm for user adding or removing can reduce the time required to prepare the biometric authentication system while maintaining the accuracy of the system within an acceptable range.

2 Materials and Methods

2.1 The Proposed Algorithm

In the classic deep learning approach, when data is added to or subtracted from the model, the model must be completely retrained [3,9]. The proposed algorithm is designed in such a way that, by using the Transfer Learning (TL) approach, this process does not require complete retraining of the VGG16 model, which can reduce the time for preparing the authentication system, while simultaneously maintaining the accuracy of the trained model at a desirable level. An overview of the proposed algorithm is summarized in Figure 3.

In the following, the method of generating a VGG16 model has been described [28], which is consistent with creating a deep learning model for processing image data. Assume an n-dimension feature vector from a user u is

$$x_u = [x_1, x_2, \ldots, x_n].$$

Also, assume the activation vector of k hidden nodes is

$$\hat{x}_u = [s_1, s_2, \ldots, s_k].$$

In this study, $k = 2$ because there are two desired output states including valid or invalid

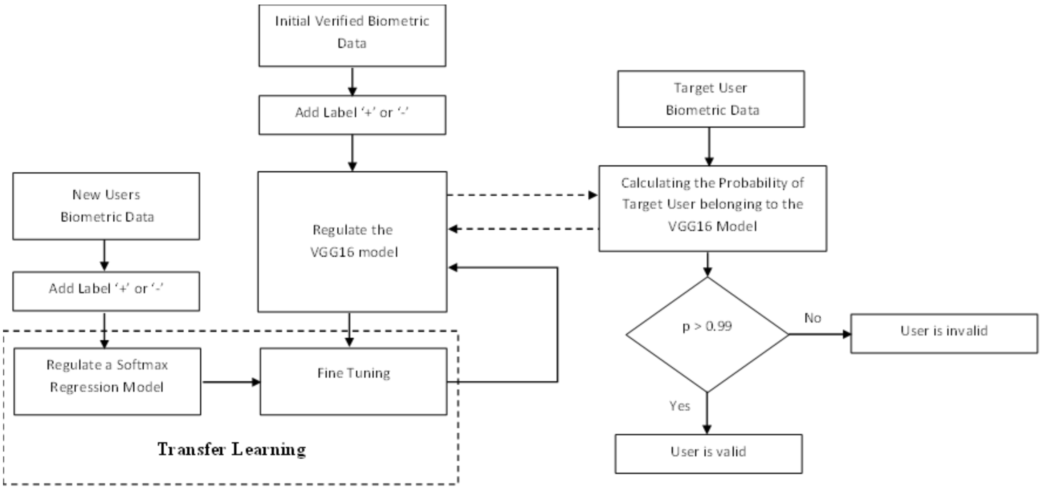

Initial Verified Biometric Data
Add Label '+' or '-'
Regulate the VGG16 model
Target User Biometric Data
Calculating the Probability of Target User belonging to the VGG16 Model
New Users Biometric Data
Add Label '+' or '-'
p > 0.99
No
User is invalid
Yes
User is valid
Regulate a Softmax Regression Model
Fine Tuning
Transfer Learning

Figure 3. The structure of the proposed algorithm.

access states, which are shown by '+' and '-' labels, respectively. The hidden nodes of a user are activated using encoding weights W and bias b by

$$\hat{x}_u = f(Wx_u + b).$$

If

$$z = [z_1, z_2, \ldots, z_m]$$

represents the actual status of m users, then

$$\hat{z} = [\hat{z}_1, \hat{z}_2, \ldots, \hat{z}_m]$$

represents the model output status of those users. Therefore, the cost function of the approach can be modeled as [25]:

$$\begin{aligned} E(W,b) = & \frac{1}{n}\sum_{j=1}^{n}\sum_{i=1}^{m}(\hat{z}_{ij} - z_{ij})^2 \\ & + \frac{\lambda}{2}\sum_{j=1}^{m}\sum_{i=1}^{k}(w_{ij})^2 \\ & + \beta\sum_{i=1}^{k}\left[\rho\log\frac{\rho}{\rho'_i} + (1-\rho)\log\frac{1-\rho}{1-\rho'_i}\right], \end{aligned} \tag{1}$$

where the first part is the mean squared error between $\hat{z}_{ij}$ and z_{ij} among all users and features. The second part represents the L_2 regularization term on weight w_{ij} from node i to node j, where λ is the penalty coefficient. The third part shows the sparsity regularization based on the Kullback–Leibler divergence, where β is the sparsity coefficient and

$$\rho_i' = \frac{1}{n}\sum_{t=1}^{n} z_i(x_t)$$

indicates the average activation of hidden node i over the training set. Weights and bias are optimized using a scaled conjugate gradient descent algorithm to minimize the cost function [20].

In the proposed approach, a VGG16 model is fitted on the data by considering Equation (1). Therefore, a DL-based model to identify the validity of users is organized. The proposed model is supervised and, by using a SoftMax activation function, the output indicates the probability that a user belongs to each final node (valid or invalid access).

In the proposed algorithm, the user adding and removing processes are performed using the combination of a TL prototype and the VGG16 model (TL-VGG16). The algorithm is designed such that during user removal, no user data are deleted from the system and only the user access status in the model is changed. The reason for this approach is that maintaining user history in authentication systems is important even when access is restricted.

In the proposed algorithm, by combining a DL prototype and transfer learning (a DL-TL model), a complex model for users with new access states is generated. Assume a new dataset of q labeled users represented as

$$(u_1,z_1),(u_2,z_2),\ldots,(u_q,z_q).$$

A high-level feature vector r_i and the relevant labels are extracted from the input u_i to train a new SoftMax regression model. Using this model, the class probabilities are estimated as

$$p(z_i = j \mid u_i), \qquad j \in \{1,\ldots,\Pi\}$$

for a Π-class problem (in this study $\Pi = 2$).

The SoftMax hypothesis function, which outputs a probability vector over all classes, is computed as follows [13]:

$$h(r_i) = \frac{1}{\sum_{j=1}^{\Pi} e^{\theta_j^T r_i}} \begin{bmatrix} e^{\theta_1^T r_i} \\ e^{\theta_2^T r_i} \end{bmatrix}, \tag{2}$$

where θ is the coefficient vector of the model. These coefficients are optimized by minimizing the cross-entropy cost function [13]:

$$E(\theta) = -\frac{1}{q}\sum_{i=1}^{q}\sum_{j=1}^{\Pi}\left[h(r_i)_j \ln z_{ij} + \left(1 - h(r_i)_j\right)\ln\left(1 - z_{ij}\right)\right], \tag{3}$$

where z_{ij} is the output of node j for user i from the SoftMax regression model.

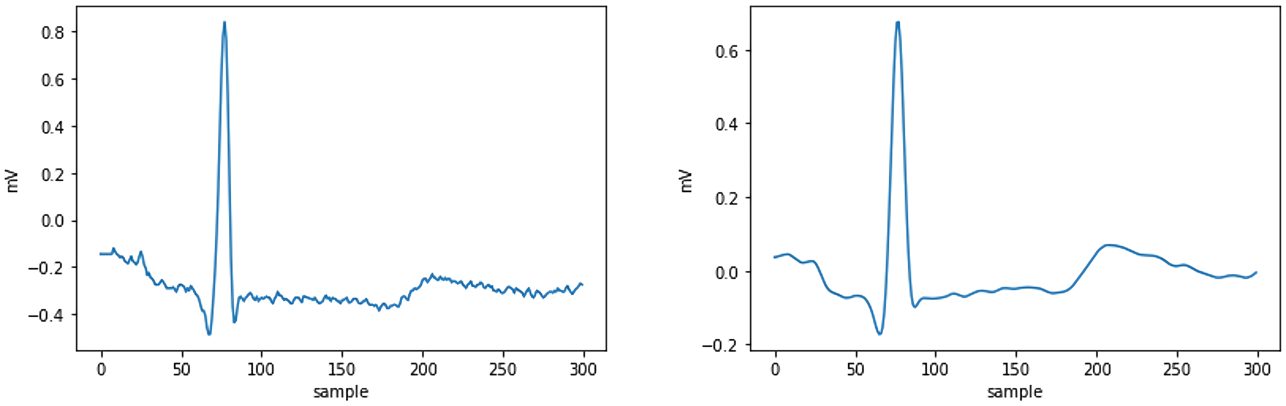
After training the SoftMax regression model, the DL-TL model is ready. It is then combined with the previous VGG16 model to form the TL-VGG16 model using supervised fine-tuning optimization [9]. In this process, weights and biases from all layers of the original VGG16 model and the SoftMax coefficients are tuned simultaneously at each iteration using the scaled conjugate gradient descent scheme [20].

This study focuses on the biometric verification task (1:1 matching), which confirms or denies a user's claimed identity. This differs from identification (1:N matching), where a system determines a user's identity among many candidates. A modified binary SoftMax architecture was designed specifically for verification (”genuine user” vs. ”impostor”). Fine-tuning stops when the target cost function is reached or the maximum number of epochs is met. In this study, the desired model accuracy was set to 99%.

2.2 Data Preparation

Whereas, the proposed algorithm can use all types of biometric data that can be processed as images due to the structure of the VGG16 platform, electrocardiogram (ECG) signals are used as the biometric data in this study. The reason for this choice is that the ECG signal can be easily captured using electronic devices available on the market and converted into an image in the form of a graph. This signal also depends on the user being alive and cannot be easily faked for a dead user. This research utilizes the MIT-BIH Arrhythmia Database Version 1.0.0 (MITDB) as a reliable source for ECG signals [7]. The MITDB is a publicly available database containing 34713 ECG records collected from 48 people (user) over a 30-minute period between 1975 and 1979. These subjects were chosen due to the inherent complexity of their ECG signals, which provide richer data for training DL models in ECG-based authentication systems. The signals are measured at a sampling frequency of 360 Hz using an 11-bit resolution frame per channel within a range of ±10 millivolts.

After capturing the ECG signals from the MITDB, they must be filtered to remove noise and inharmonic oscillations which can affect the authentication process. This process is called data cleaning and NeuroKit toolbox [17] was used for this purpose in this study. See Figure 4 as a sample of NeuroKit data cleaning.



(a) Raw Data

(b) Cleaned Data

Figure 4. The effect of using the noise reduction filter by the Neurokit toolbox on a sample ECG signal [5].

In this study, the segmentation of ECG signals into consecutive, non-overlapping windows of 5 seconds (equal to 1800 samples at a sampling rate of 360 Hz). The reason for the choice of length of window was to try to capture at least one full cardiac cycle and to also give enough contextual information. For each user, we then randomly selected 20 windows for image conversion. Each signal window was then converted to a 2-dimensional (2D) image using a Continuous Wavelet Transform (CWT) which produced a scalogram, which we resized to 224×224 pixels to match the requirements of the VGG16 input layer.

2.3 Executing the Model

All required codes were programmed by Python and were run on the Google Colab Pro environment with 32GB of RAM and P100/T4 GPUs to address the high computational demands of processing large datasets. The batch size was set to 64 and a total of 100 epochs were used to train the VGG16 model.

To mitigate overfitting and obtain generalization in our model, the study followed the 80-20 split of training to validation. In addition, the Early Stopping technique was used with a patience of 5 epochs based on validation loss, where training would terminate if no improvement was observed. The model was retrained on the full training set (train + validation splits) for the optimal epochs that was found (10 epochs in our results). The curve of loss for training and validation has been amended to figure 5 to illustrate the convergence of curves and absence of overfitting.

To mitigate overfitting and obtain generalization in our model, the study followed the 80-20 split of training to validation. In addition, the Early Stopping technique was used with a patience of 5 epochs based on validation loss, where training would terminate if no improvement was observed. The model was retrained on the full training set (train + validation splits) for the optimal epochs that was found (10 epochs in our results). The curve of loss for training and validation has been amended to figure 5 to illustrate the convergence of curves and absence of overfitting.

2.4 Evaluation of the Proposed Algorithm

Due to evaluating the proposed algorithm to use in biometric authentication systems, the first question is whether the algorithm can correctly perform authentication process using ECG signals. To answer this question, the data was divided into two categories, with 70% of classes in one category as a dataset for identified users and the other 30% of classes in another category as a dataset for unidentified users. The first category group was then randomly labeled so that 50% of them had label ′+′ and the other 50% had label ′-′ having both valid and invalid user access. All data in the second category was labeled ′+′ due to test of fake valid users. Next, the VGG16 model was trained on the data from the first category and the testing process was done by both categories for the whole data.

Both at training and testing, each signal window, is considered an independent sample. The model produces an access label (valid / invalid) for each window independently. In considering the overall access decision for a user during testing, we implement a majority voting scheme: specifically, if better than fifty percent of the windows presented by a user are classified as 'valid', access is granted to the user. In this section, the invalid access data (indicated with '-') was generated through a flow that was often more representative of reality: (1) to induce a real impostor attack, ECG signals were obtained from users who were not previously present in the current 'identified' set, and (2) to have greater variability in the data, a variety of data augmentation techniques were applied (Gaussian Noise [25] and Short Time-Warping [26]) to the authorized user's dataset. In this way, we designed a much more realistic and difficult setting for the model.

In machine learning, various indicators such as precision, accuracy, recall, and F1 score are commonly used to assess the accuracy of a trained model [28]. These indicators need some variables which described in Table 1.

Variable	Description
True Positive (TP)	An experimental result that correctly shows the occurrence of a condition.
False Positive (FP)	An experimental result that mistakenly shows the occurrence of a condition.
True Negative (TN)	An experimental result that correctly shows the absence of conditions.
False Negative (FN)	An experimental result that mistakenly shows the absence of a condition.

Table 1. The required variable to calculate precision, accuracy, recall, and F1 score.

Accuracy as a general metric calculates the proportion of correctly classified instances. Precision addresses the issue of class imbalance by focusing on the positive predictive value. Recall, also known as sensitivity, addresses a limitation of accuracy in imbalanced class scenarios. Recall focuses on the model's ability to correctly identify true positive cases and is calculated as the proportion of positive cases the model correctly classifies. The F1 score addresses this challenge by incorporating both recall and precision into a single metric. It represents the harmonic mean between recall and precision, providing a balanced view of the performance of the model to identify positive cases. The relevant equations to calculate the introduced indicators are presented in Table 2.

Indicator	Equation Formula	Equation Number
Accuracy	$(TP+TN)/(TN+TP+FN+FP)$	(4)
Precision	$TP/(TP+FP)$	(5)
Recall	$TP/(TP+FN)$	(6)
F1	$2(Precision * Recall)/(Precision + Recall)$	(7)

Table 2. The equation to calculate the described indicators.

After evaluating the VGG16 model for using as a biometric authentication based on the ECG signals, the ability of the proposed algorithm to user adding and removing to this base VGG16 model should be evaluated (it means examining the TL-VGG16 model). Hence, two

different scenarios were examined.
In scenario 1, the process of adding new users by the TL-VGG16 approach was evaluated. In this way, two sub-scenarios include Only-VGG16 and TL-VGG16 were examined. Therefore, all data were labeled with '+' as valid users. In both sub-scenarios, the first user was directly added into the VGG16 model and the model was trained. To add the second user, in sub-scenario Only-VGG16 the entire model was completely retrained for both users. But in sub-scenario TL-VGG16, new users are added to the model using the DL-TL approach. For both cases, the training time of the new model and its accuracy were evaluated. This process is repeated in a similar manner to add other new users and the results obtained from both sub-scenarios were compared.

Scenario 2 demonstrates the ability of the TL-VGG16 approach to remove users from a base VGG16 model. For this purpose, the base VGG16 model was first trained using all the data labeled with '+'. Then, similarly to the scenario 1, two sub-scenarios include Only-VGG16 and TL-VGG16 were examined again. Then, a user is selected to remove his/her access. Because each user in the base VGG16 model has been previously present with valid access, when introducing the user with the label '-' to the model, different iterations of the user are introduced into the model to evaluate the optimal iteration. In sub-scenario TL-VGG16, the data of removed-access user is added to the model using the DL-TL approach, but in sub-scenario Only-VGG16 the entire model was completely retrained after adding the data of the removed-access user. Similar to the scenario 1, the training time of the new model and its accuracy were evaluated for both sub-scenarios. This process is repeated in a similar manner to remove other new users from the base VGG16 model and the results obtained from both sub-scenarios were compared.

3 Results and Discussion

As explained in the previous sections, the VGG16 model's ability to be used in biometric authentication based on ECG signals was firstly evaluated. Figure 5 shows the loss values of the VGG16 model during the training process.

As presented in Figure 5, both the training and validation loss curves displayed converging behavior, which became significantly stable (less than 0.1%) after epoch 10. The proximity and converging behavior show that the model was able to learn the data without being overfitted. We also used Early Stopping with a patience of 5 epochs based on the validation loss to ensure that the model would generalize. As there was no significant improvement in validation loss after epoch 10, this would be the point in time selected for the optimal stopping point. The model was retrained on the full training dataset (training and validation splits together) to report the final results for 10 epochs.

The results obtained show that the VGG16 model was able to fit the ECG signal data well, so that even in low epoch, the loss value was less than 1%. After that, all data was examined by the trained model to predict the access type of each user. The results showed that the average time to check each user's access status (the system response time) was about 37 milliseconds

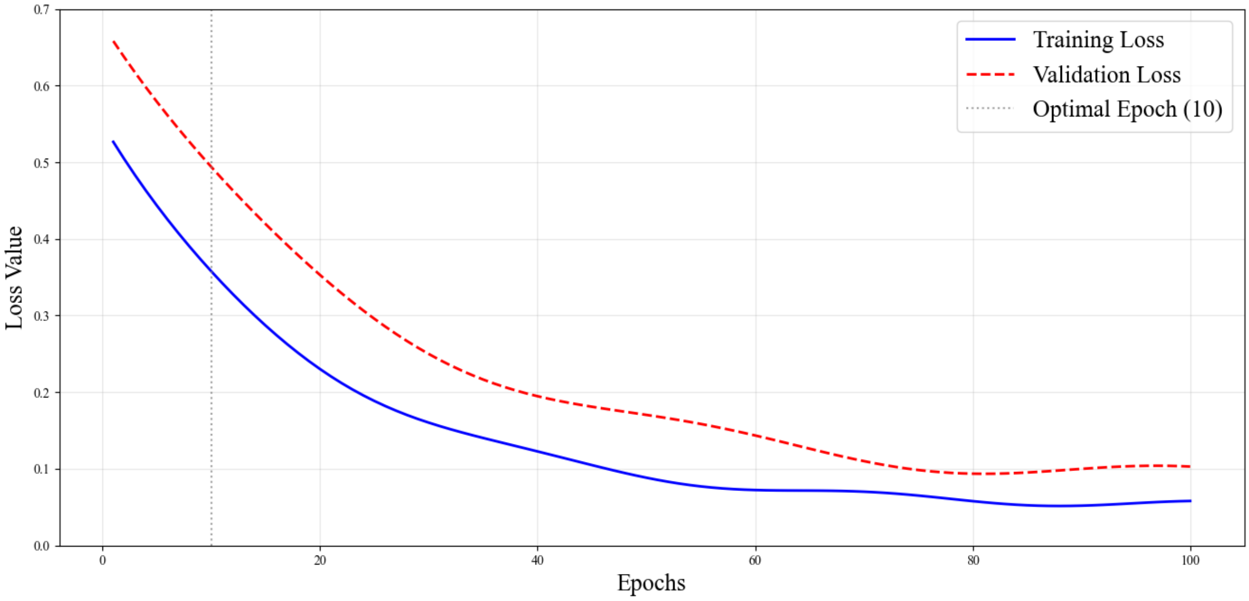


Figure 5. Results of loss values of training and validation of the VGG16 model.

that is acceptable for authentication systems. As it was said in the previous section, the data was equally labeled with '+' and '-' and both valid and invalid access types were examined. The results showed that in the VGG16 model for ECG data, the epoch greater than or equal to 10 always leads to the loss value less than 0.1%. Consequently, in the continuation of this study, the epoch value for training all the models was considered to be equal to 10. The results of the performance indicators of the base VGG16 model are summarized in Table 3.

Indicator	Value
Accuracy (%)	99.45
Precision (%)	99.23
Recall (%)	99.36
F1 (%)	99.29

Table 3. Summary of performance evaluation of the VGG16 model equipped with ECG signals to use as a biometric authentication system.

After confirming the effectiveness of the examined model to use as a biometric authentication system, the Scenario 1 was implemented. As explained in the previous sections, considering two different sub-scenarios, the model is first trained by 1 user, and in the next steps other users are added to the model separately. In the scenario Only-VGG16, the model is completely retrained for each new user, and in the scenario TL-VGG16, new data is introduced to the model using the DL-TL approach. In the both cases, the retraining time and the accuracy of the trained model were measured. The results showed that preparing the data for a new user by the DL-TL model equipped with the 30 nodes took an average of 9 seconds.The results for the total preparing time of the VGG16 model in the Scenario 1 are reported in Table 4.

User	Only-VGG16	TL-VGG16	Difference (%)	User	Only-VGG16	TL-VGG16	Difference (%)
1	10	12	20.00	25	127	15	-88.19
2	14	15	7.14	26	132	11	-91.67
3	18	19	5.56	27	136	15	-88.97
4	21	22	4.76	28	140	14	-90.00
5	26	15	-42.31	29	144	22	-84.72
6	31	12	-61.29	30	147	17	-88.44
7	34	12	-64.71	31	152	17	-88.82
8	40	16	-60.00	32	155	11	-92.90
9	44	16	-63.64	33	161	15	-90.68
10	47	12	-74.47	34	166	21	-87.35
11	54	15	-72.22	35	172	21	-87.79
12	58	17	-70.69	36	179	15	-91.62
13	64	16	-75.00	37	182	14	-92.31
14	69	15	-78.26	38	186	20	-89.25
15	73	21	-71.23	39	189	19	-89.95
16	80	12	-85.00	40	192	13	-93.23
17	87	13	-85.06	41	127	15	-88.19
18	93	19	-79.57	42	132	11	-91.67
19	100	15	-85.00	43	136	15	-88.97
20	103	19	-81.55	44	140	14	-90.00
21	106	20	-81.13	45	144	22	-84.72
22	109	21	-80.73	46	147	17	-88.44
23	115	14	-87.83	47	152	17	-88.82
24	122	16	-86.89	48	155	11	-92.90

Table 4. Results of the preparing time of the final VGG16 model in scenario 1 for adding new users to the model (in second).

According to the results, adding a new user using the DL-TL approach has reduced the preparing time of the model by an average of 75.42% compared to the classical approach. Based on the results, it was determined that the TL-VGG16 approach will result in a significant reduction in model retraining time for more than 5 users. It can also be seen that there is a direct relationship between the number of users in the model and the reduction in the retraining time of the final VGG16 model, and it can be concluded that having the more users in the TL-VGG16 model will reduce the time required to prepare the final VGG16 model significantly. Also, the accuracy of the final VGG16 model to identify user access in Scenario 1 was evaluated for all users and the results is shown in Table 5.

The results showed that the Only-VGG16 model was averagely 99.42% accurate in assessing the user access after retraining process and it was averagely 99.49% while using TL-VGG16 to add new users. As a result, using TL-VGG16 approach to add new users has been able to increase the model's accuracy by about 0.08% on average compared to the Only-VGG16 approach.

Next, the results of scenario 2, which deals with changing the access of existing users in the base VGG16 model, were evaluated. As explained in the previous sections, removing a user from the model requires examining more states. Given that in the proposed algorithm, the user removing process is also performed as adding the user with a different access type,

User	Only-VGG16	TL-VGG16	Difference (%)	User	Only-VGG16	TL-VGG16	Difference (%)
1	99.31	99.50	0.19	25	99.42	99.49	0.07
2	99.33	99.50	0.17	26	99.44	99.50	0.06
3	99.18	99.49	0.31	27	99.42	99.49	0.07
4	99.33	99.50	0.16	28	99.44	99.50	0.06
5	99.37	99.49	0.12	29	99.43	99.50	0.07
6	99.41	99.49	0.08	30	99.44	99.50	0.06
7	99.39	99.50	0.10	31	99.43	99.49	0.06
8	99.45	99.50	0.05	32	99.45	99.49	0.04
9	99.41	99.49	0.08	33	99.43	99.49	0.07
10	99.44	99.49	0.06	34	99.45	99.49	0.05
11	99.42	99.50	0.08	35	99.44	99.50	0.06
12	99.41	99.50	0.08	36	99.43	99.50	0.07
13	99.44	99.49	0.05	37	99.44	99.49	0.05
14	99.43	99.49	0.06	38	99.45	99.50	0.05
15	99.39	99.50	0.11	39	99.44	99.50	0.06
16	99.44	99.50	0.05	40	99.45	99.50	0.05
17	99.40	99.49	0.09	41	99.44	99.50	0.06
18	99.44	99.50	0.05	42	99.43	99.49	0.07
19	99.43	99.49	0.06	43	99.44	99.49	0.05
20	99.44	99.49	0.05	44	99.45	99.50	0.05
21	99.43	99.49	0.06	45	99.44	99.50	0.05
22	99.43	99.50	0.07	46	99.44	99.50	0.06
23	99.43	99.49	0.06	47	99.43	99.49	0.06
24	99.41	99.49	0.08	48	99.45	99.50	0.05

Table 5. Results of the accuracy of the final VGG16 model in scenario 1 for adding new users to the model (in percent).

and this requires training an intermediate DL-TL model, measuring the training time of this intermediate model for different numbers of user data repetitions is important. Therefore, the data of each user was entered into the intermediate DL-TL model in iterations 1 to 10, and the training time and accuracy of the model were measured. The results obtained are presented in Table 6.

Iteration	Training Time (second)	Accuracy (%)
1	9	97.21
2	11	98.12
3	12	99.01
4	14	99.14
5	17	99.27
6	21	99.31
7	24	99.49
8	27	99.57
9	33	99.64
10	39	99.70

Table 6. Results of the accuracy and the training time of the DL-TL model with 30 nodes for different iterations of user data as the input.

The results show that increasing the number of user data iterations increases the training time and also increases the accuracy of the model. Given that in this study, 99% accuracy is considered as the desired goal, iteration 3, in which the accuracy of the DL-TL reached above 99% for the first time, was selected as the optimal iteration. This is because although more iterations have better accuracy, the model training time has also increased, which is an undesirable parameter. As a result, scenario 2 was examined by considering 3 iterations for the user data, and the results related to the training time of the final VGG16 model are presented in Table 7.

User	Only-VGG16	TL-VGG16	Difference (%)	User	Only-VGG16	TL-VGG16	Difference (%)
1	221	21	-90.50	25	115	20	-82.61
2	217	18	-91.71	26	109	21	-80.73
3	214	21	-90.19	27	106	15	-85.85
4	211	16	-92.42	28	103	18	-82.52
5	204	16	-92.16	29	100	18	-82.00
6	199	17	-91.46	30	93	16	-82.80
7	196	15	-92.35	31	87	19	-78.16
8	192	16	-91.67	32	80	18	-77.50
9	189	19	-89.95	33	73	17	-76.71
10	186	15	-91.94	34	69	18	-73.91
11	182	16	-91.21	35	64	21	-67.19
12	179	15	-91.62	36	58	15	-74.14
13	172	17	-90.12	37	54	23	-57.41
14	166	23	-86.14	38	47	16	-65.96
15	161	22	-86.34	39	44	22	-50.00
16	155	23	-85.16	40	40	20	-50.00
17	152	16	-89.47	41	34	19	-44.12
18	147	22	-85.03	42	31	20	-35.48
19	144	23	-84.03	43	26	17	-34.62
20	140	15	-89.29	44	21	18	-14.29
21	136	16	-88.24	45	18	21	16.67
22	132	20	-84.85	46	14	19	35.71
23	127	19	-85.04	47	10	17	70.00
24	122	22	-81.97	48	-	-	-

Table 7. Results of the preparing time of the final VGG16 model in scenario 2 for removing a user from the model (in second).

It should be noted that the data in the first row of the table is related to the removing the first user from the base VGG16 model and so on (note that the base VGG16 model included data from all users, in this case the first user from 48 users). The results show that the model retraining time in TL-VGG16 approach is reduced by an average of 70.35% compared to Only-VGG16 approach. Also, examining the results shows that the proposed algorithm for removing a user from the authentication system when the number of users is less than 4 has no advantage over the classical approach. It should be noted that the results for the user in row 48 could not be calculated because removing the 48th user would empty the VGG16 model. The results of the accuracy assessment in scenario 2 are presented in Table 8.

An examination of the results shows that the accuracy of the model in TL-VGG16 approach shows an average decrease of 0.14% compared to Only-VGG16 approach, but the values obtained, except for the case where the model has only one user, have always been above 99%.

User	Only-VGG16	TL-VGG16	Difference (%)	User	Only-VGG16	TL-VGG16	Difference (%)
1	99.45	99.27	-0.18	25	99.41	99.26	-0.15
2	99.43	99.26	-0.17	26	99.43	99.26	-0.17
3	99.44	99.30	-0.14	27	99.43	99.28	-0.15
4	99.44	99.29	-0.15	28	99.43	99.32	-0.11
5	99.45	99.29	-0.16	29	99.44	99.33	-0.11
6	99.44	99.23	-0.21	30	99.43	99.29	-0.14
7	99.43	99.28	-0.15	31	99.44	99.27	-0.17
8	99.44	99.33	-0.11	32	99.40	99.31	-0.09
9	99.45	99.34	-0.11	33	99.44	99.30	-0.14
10	99.44	99.36	-0.08	34	99.39	99.25	-0.14
11	99.45	99.31	-0.14	35	99.43	99.28	-0.15
12	99.44	99.30	-0.14	36	99.44	99.34	-0.10
13	99.43	99.22	-0.21	37	99.41	99.25	-0.16
14	99.44	99.33	-0.11	38	99.42	99.29	-0.13
15	99.45	99.28	-0.17	39	99.44	99.31	-0.13
16	99.43	99.22	-0.21	40	99.41	99.26	-0.15
17	99.45	99.36	-0.09	41	99.45	99.37	-0.08
18	99.43	99.23	-0.20	42	99.39	99.24	-0.15
19	99.44	99.23	-0.21	43	99.41	99.21	-0.20
20	99.43	99.33	-0.10	44	99.37	99.24	-0.13
21	99.44	99.31	-0.13	45	99.33	99.24	-0.09
22	99.42	99.30	-0.12	46	99.18	99.16	-0.02
23	99.44	99.36	-0.08	47	99.33	99.22	-0.11
24	99.42	99.28	-0.14	48	99.31	98.99	-0.32

Table 8. Results of the accuracy of the final VGG16 model in scenario 2 for removing a user from the model (in percent).

Combining the results obtained from scenarios 1 and 2, the average training time and model accuracy in TL-VGG16 approach for user adding and removing are shown in Figures 6 and 7, respectively.

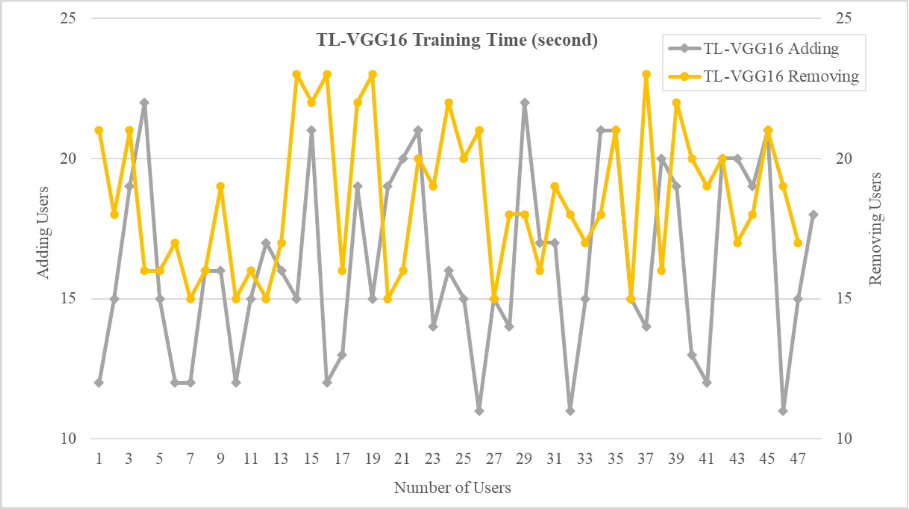


Figure 6. Results of the average training time in the TL-VGG16 scenario.

Summarizing the results obtained, it was shown that using the Only-VGG16 model in an ECG-based authentication system led to have an accuracy about 99.45% for the investigated 48

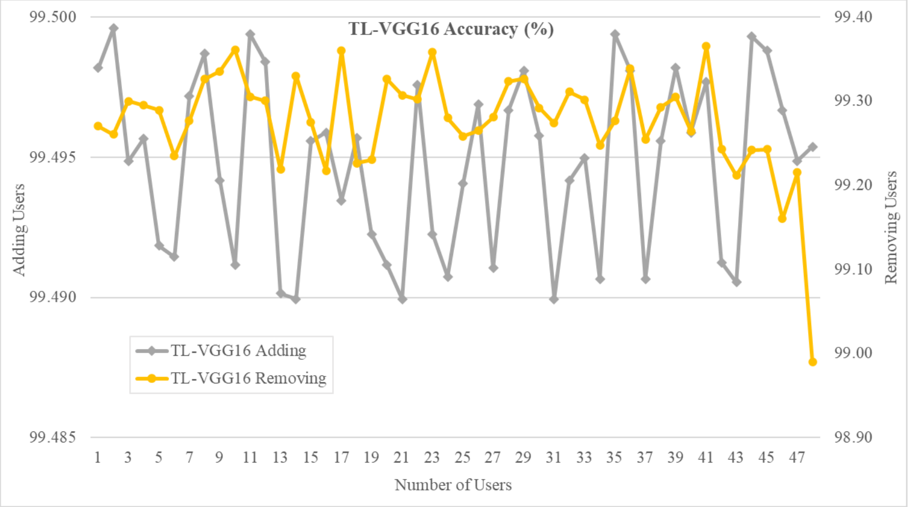


Figure 7. Results of the accuracy in the TL-VGG16 scenario.

users. Also, the TL-VGG16 model for user adding and removing had at least 99.16% accuracy and an examination of the obtained trend shows that if the number of users increases, the TL-VGG16 model's accuracy will probably also increase. A comparison between the accuracy obtained in this study and other similar studies for the same dataset is presented in Table 9.

Author	Database	Year	Method	Accuracy (%)
Wang et al. [30]	MITDB	2020	MSDF	94.68
Chu et al. [5]	MITDB	2019	CNN	95.99
Belo et al. [2]	MITDB	2020	RNN	97.92
Tan et al. [27]	MITDB	2017	DWT	98.00
Li et al. [14]	MITDB	2020	GNMF	98.03
Lynn et al. [15]	MITDB	2019	CNN	98.40
Maleki [18]	MITDB	2022	CNN	99.00
TL-VGG16	MITDB	2024	CNN	99.16

Table 9. Comparison of the accuracy of the proposed algorithm with previous studies on the MITDB dataset to make a biometric authentication system.

It is clear that the accuracy of the proposed algorithm shows significant improvements over other studies. Also, the results show that the TL-VGG16 approach was able to execute the user adding process with an average time of 16.25 seconds and 18.53 seconds for user removing. These times have shown a significant reduction compared to the Only-VGG16 approach and can adjust the authentication system downtime for re-preparation within an acceptable range. It should be noted that in this study, general hardware was used to run the model, and better time results can be expected if dedicated hardware is used. Considering the accuracy, retraining time, and the time of new user access evaluation, it can be stated that the proposed algorithm has been able to provide a suitable approach for a biometric authentication system based on the ECG signals.

4 Conclusion

The production of authentication systems and algorithms has long been an important research topic in computer science. In this regard, different approaches have been studied, each of which has specific advantages over other approaches. In general, when evaluating authentication systems, at least three parameters include system preparation time, system response time, and its accuracy are examined. On the other hand, there is a tendency to use more complex data in authentication systems to reduce the possibility of identity fraud and unauthorized access. Studies have shown that using biometric data as one type of complex data and using deep learning models have been able to create more secure authentication systems. Although the use of deep learning can lead to complex and accurate models, it presents a fundamental challenge involving the time it takes to train the model, especially when changes are made to the data. To solve this problem, in this study, a novel algorithm was proposed and evaluated. In the proposed algorithm, a base VGG16 model (as a deep learning model) based on the ECG signals is used, in which the process of user adding or removing was combined to the base model using the transfer learning approach. Transfer learning is an approach that can add new data to a trained model without requiring the model to be completely retrained. In the proposed algorithm, to add a new user or to change the access of a user (for removing his/her access), the coefficients of the SoftMax regression of the user are first calculated and then added to the base VGG16 model considering the soft tuning (as an approach of transfer learning). In this study, the data from MITDB dataset version 1.0.0 was used, which includes 34713 ECG signals from 48 individuals (users). Next, the VGG16 model was trained using data (one user's data each time) and the training time and accuracy of the model were measured. The results showed that in training of the VGG16 model for the ECG signals, considering the epoch equal to 10 resulted in a loss value about 0.1. One of the most important challenges of this study was finding a suitable computing device, which in this study was the Google Colab Pro environment with 32GB of RAM and P100/T4 GPUs. Although the machine has adequate processing power, it is being shared by different users and it is predicted that if a suitable dedicated processing machine is used, the model retraining time will be less than the obtained value. The proposed model in this study was evaluated on the available data for 48 users (to comparison with similar studies). Although the values of retraining time and model accuracy for different numbers of users fluctuated within a relatively small range, it is suggested that the proposed algorithm be re-evaluated with a larger number of users and the results obtained be compared with this study. Moreover, while the results are promising on the MIT-BIH dataset, it will also be important to validate that the proposed algorithm generalizes on a larger and more diverse dataset in the future work.

Funding

This research received no external funding.

Data Availability Statement

Data is contained within the article.

Conflicts of Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

[1] M. M. A. Abuqadumah, M. A. M. Ali, R. R. O. Al-Nima, Personal authentication application using deep learning neural network, in: 2020 16th IEEE International Colloquium on Signal Processing and Its Applications (CSPA), 2020, pp. 186–190. https://doi.org/10.1109/CSPA48992.2020.9068706

[2] D. Belo, N. Bento, H. Silva, A. Fred, H. Gamboa, ECG biometrics using deep learning and relative score threshold classification, Sensors 20(15) (2020) 1–20. https://doi.org/10.3390/s20154078

[3] Y. Bengio, Y. LeCun, Scaling learning algorithms toward AI, in: Large-Scale Kernel Machines, MIT Press, 2007. https://doi.org/10.7551/mitpress/7496.003.0016

[4] C. Boncelet, Chapter 7 – Image noise models, in: The Essential Guide to Image Processing, Academic Press, 2009, pp. 143–167. https://doi.org/10.1016/B978-0-12-374457-9.00007-X

[5] Y. Chu, H. Shen, K. Huang, ECG authentication method based on parallel multi-scale one-dimensional residual network with center and margin loss, IEEE Access 7 (2019) 51598–51607. https://doi.org/10.1109/ACCESS.2019.2912519

[6] H. S. Desai, A. M. Gonsai, Hybrid CNN-VGG19 model for real-time face recognition system, Educ. Adm. Theory Pract. 30(6) (2024) 427–433. https://doi.org/10.53555/kuey.v30i6.6141

[7] A. L. Goldberger et al., PhysioBank, PhysioToolkit, and PhysioNet, Circulation 101(23) (2000) e215–e220. https://doi.org/10.1161/01.CIR.101.23.e215

[8] M. I. Hashem, K. Hasen Kuban, Key generation method from fingerprint image based on deep convolutional neural network model, Nexo Sci. J. 36(06) (2023) 906–925. https://doi.org/10.5377/nexo.v36i06.17447

[9] G. E. Hinton, R. R. Salakhutdinov, Reducing the dimensionality of data with neural networks, Science 313(5786) (2006) 504–507. https://doi.org/10.1126/science.1127647

[10] A. Hosna, E. Merry, J. Gyalmo, Z. Alom, Z. Aung, M. A. Azim, Transfer learning: a friendly introduction, J. Big Data 9(1) (2022) 102. https://doi.org/10.1186/s40537-022-00652-w

[11] A. A. Kuznetsov, D. O. Zakharov, Deep learning-based models' application to generating a cryptographic key from a face image, Radiotekhnika 2(213) (2023) 31–40. https://doi.org/10.30837/rt.2023.2.213.03

[12] T. Lam, S. Nilsson, Application of convolutional neural networks for fingerprint recognition, Master's Thesis, Mathematical Sciences, 2018. http://lup.lub.lu.se/student-papers/record/8949667

[13] H. Li, N. A. Parikh, L. He, A novel transfer learning approach to enhance deep neural network classification of brain functional connectomes, Front. Neurosci. 12 (2018) 00491. https://doi.org/10.3389/fnins.2018.00491

[14] R. Li, G. Yang, K. Wang, Y. Huang, F. Yuan, Y. Yin, Robust ECG biometrics using GNMF and sparse representation, Pattern Recognit. Lett. 129 (2020) 70–76. https://doi.org/10.1016/j.patrec.2019.11.005

[15] H. M. Lynn, S. B. Pan, P. Kim, A deep bidirectional GRU network model for biometric electrocar-

diogram classification based on recurrent neural networks, IEEE Access 7 (2019) 145395–145405. https://doi.org/10.1109/ACCESS.2019.2939947

[16] J. Ma, S. Dang, G. Watkins, K. Morris, M. Beach, A high-performance transfer learning-based model for microwave structure behavior prediction, TechRxiv (2023). https://doi.org/10.36227/techrxiv.23700054.v1

[17] D. Makowski et al., NeuroKit2: a Python toolbox for neurophysiological signal processing, Behav. Res. Methods (2021) 1–8. https://doi.org/10.3758/s13428-020-01510-y

[18] S. Maleki, Analysis and design bio-signals based access control schemes, M.Sc. thesis, Dept. of Electrical Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran, 2020.

[19] S. Minaee, A. Abdolrashidiy, Y. Wang, An experimental study of deep convolutional features for iris recognition, in: 2016 IEEE Signal Processing in Medicine and Biology Symposium (SPMB), 2016, pp. 1–6. https://doi.org/10.1109/SPMB.2016.7846859

[20] M. F. Moller, A scaled conjugate gradient algorithm for fast supervised learning, Neural Networks 6(4) (1993) 525–533. https://doi.org/10.1016/S0893-6080(05)80056-5

[21] A. Pantanowitz et al., Effective deep learning approach based on VGG-mini architecture for iris recognition, Informatics Med. Unlocked 26 (2021) 4718–4726. https://doi.org/10.1016/J.IMU.2021.100727

[22] M. Papez, A. Quinn, Transferring model structure in Bayesian transfer learning for Gaussian process regression, Knowledge-Based Syst. 251 (2022) 108875. https://doi.org/10.1016/j.knosys.2022.108875

[23] D. Sharma, A. Selwal, Biometrics: introduction and applications, in: Leveraging Computer Vision to Biometric Applications, 2024, pp. 1–18. https://doi.org/10.1201/9781032614663-1

[24] Y. Shi, Construction of the convolutional neural network based on the increase optimizers provided and atomic layers provided, in: 2022 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE), 2022, pp. 676–679. https://doi.org/10.1109/ICCECE54139.2022.9712718

[25] H.-C. Shin, M. R. Orton, D. J. Collins, S. J. Doran, M. O. Leach, Stacked autoencoders for unsupervised feature learning and multiple organ detection in a pilot study using 4D patient data, IEEE Trans. Pattern Anal. Mach. Intell. 35(8) (2013) 1930–1943. https://doi.org/10.1109/TPAMI.2012.277

[26] A. Singh, A. Nigam, RETRACTED ARTICLE: Effect of identity mapping, transfer learning and domain knowledge on the robustness and generalization ability of a network: a biometric based case study, J. Ambient Intell. Humaniz. Comput. 11(5) (2020) 1905–1922. https://doi.org/10.1007/s12652-019-01297-z

[27] R. Tan, M. Perkowski, Toward improving electrocardiogram (ECG) biometric verification using mobile sensors: a two-stage classifier approach, Sensors 17(2) (2017). https://doi.org/10.3390/s17020410

[28] J. Tao, Y. Gu, J. Sun, Y. Bie, H. Wang, Research on vgg16 convolutional neural network feature classification algorithm based on transfer learning, in: 2021 2nd China International SAR Symposium (CISS), 2021, pp. 1–3. https://doi.org/10.23919/CISS51089.2021.9652277

[29] S. D. Thepade, M. Dindorkar, P. Chaudhari, S. Bang, Face presentation attack identification optimization with adjusting convolution blocks in VGG networks, Intell. Syst. with Appl. 16 (2022) 200107. https://doi.org/10.1016/j.iswa.2022.200107

[30] K. Wang, G. Yang, Y. Huang, Y. Yin, Multi-scale differential feature for ECG biometrics with collective matrix factorization, Pattern Recognit. 102 (2020) 107211. https://doi.org/10.1016/j.patcog.2020.107211

[31] Z. Wen, S. Han, Y. Yu, X. Xiang, S. Lin, X. Xu, Empowering robust biometric authentication: the fusion of deep learning and security image analysis, Appl. Soft Comput. 154 (2024) 111286. https://doi.org/10.1016/j.asoc.2024.111286

[32] H. Yang, J. Ni, J. Gao, Z. Han, T. Luan, A novel method for peanut variety identification and classification by improved VGG16, Sci. Rep. 11(1) (2021) 15756. https://doi.org/10.1038/s41598-021-95240-y

[33] Z. Zhang, R. Tavenard, A. Bailly, X. Tang, P. Tang, T. Corpetti, Dynamic time warping under limited warping path length, Inf. Sci. 393 (2017) 91–107. https://doi.org/10.1016/j.ins.2017.02.018

Citation: N. Eshaghi, M. Habibi, N. Bagheri, Ali Khatibi, Enhancing ECG-based authentication systems using VGG16 model and transfer learning, J. Disc. Math. Appl. 11(1) (2026) 13–32.

https://doi.org/10.22061/jdma.2025.12571.1169