A New Method for Face-Based Recognition Using a Fuzzy Face Deep Model

Zainab Hashim
Computers Department, College of Basic Education, Mustansiriyah University, Baghdad, Iraq
zainab.hashim@uomustansiriyah.edu.iq

Hind Moutaz Al-Dabbas
Department of Computer Science, College of Education for Pure Science/Ibn Al-Haitham, University of Baghdad, Baghdad, Iraq
hind.moutaz@ihcoedu.uobaghdad.edu.iq (corresponding author)

Received: 22 February 2025 | Revised: 14 April 2025 and 25 April 2025 | Accepted: 27 April 2025

 DOI: https://doi.org/10.48084/etasr.10679

ABSTRACT

Face recognition is a crucial biometric technology used in various security and identification applications. Ensuring accuracy and reliability in facial recognition systems requires robust feature extraction and secure processing methods. This study presents an accurate facial recognition model using a feature extraction approach within a cloud environment. First, the facial images undergo preprocessing, including grayscale conversion, histogram equalization, Viola-Jones face detection, and resizing. Then, features are extracted using a hybrid approach that combines Linear Discriminant Analysis (LDA) and Gray-Level Co-occurrence Matrix (GLCM). The extracted features are encrypted using the Data Encryption Standard (DES) for security and then sent to the cloud server hosting the deep model. Upon reaching the server, the features are decrypted and fed into the proposed Fuzzy Face Deep Model (FFDM), which incorporates a fuzzy layer to enhance recognition accuracy. The model was evaluated using the MUCT and LFW datasets, demonstrating high accuracy and notable results, with precision of 99.65% and 100% on MUCT and LFW, respectively.

Keywords-cloud environment; DL; face recognition; GLCM; LDA

I. INTRODUCTION

The domains of image classification and biometrics have attracted significant interest from researchers because of their diverse applications in classification and security. Identification of physical characteristics inherent to people can be effectively employed in recognition systems, such as item classification, facial recognition, and verification of personal identity [1]. Personal identity has become increasingly significant, and biometric verification is widely considered one of the most secure and challenging authentication methods [2]. Biometric systems enable efficient and automated individual identification, providing a more viable alternative to traditional methods such as passwords [3]. Deep Learning (DL) methods have demonstrated exceptional performance in face recognition [4, 5]. Convolutional Neural Networks (CNNs), frequently employed in computer vision applications, provide a significant advantage in autonomous visual feature extraction [6]. Recent advances in DL have greatly enhanced the accuracy and efficiency of biometric detection systems.

CNNs often consist of several convolutional layers, each including several filters of varying sizes, enabling the acquisition of progressively intricate visual features [7, 8]. Neural networks simulate the way human brain neurons process data by classifying and analyzing inputs through interconnected nodes. Within biometric cryptosystems, biometric data facilitate the generation or retrieval of keys, overcoming the challenges posed by inherent biometric variability. Unlike conventional systems that provide a binary response, these systems aim to achieve high accuracy in key generation, ensuring robust security [9]. Cloud computing, with its ability to grant controlled access to network resources, has gained popularity for outsourcing data storage and reducing local resource demands [10]. However, the storage of sensitive information on remote servers poses privacy concerns. Biometric authentication strengthens security in such scenarios by ensuring that only authorized individuals can access cloud-stored data [11]. To achieve this, user data must be encrypted during processing, ensuring that no unauthorized entities, including the servers themselves, can access them. Upon completion, the results are securely transmitted to the user, with only him possessing the decryption key [10, 11].

This study presents an intelligent DL-based trust model for secure user authentication using cloud computing to enhance the accuracy, security, and robustness of facial recognition systems, addressing key challenges in traditional approaches. Leveraging face recognition as a biometric, the proposed approach ensures robust and efficient cloud service access.

II. RELATED WORK

In [12], a hybrid approach was proposed for facial recognition, combining a Modified Local Binary Pattern (MLBP) with a Layered-Recurrent Neural Network (L-RNN). This method demonstrated a high classification accuracy of 98%, according to evaluations on the MUCT dataset and comparative analyses of various ANN techniques. In [13], enlarged kernels were utilized to enhance the performance of HOG, incorporating feature extraction from color images to develop a color component fusion and selection technique. Experimental results on multiple facial benchmark datasets demonstrated notable accuracy improvements through these advanced color component analysis methods, achieving accuracy rates of 75.00% on the Georgia dataset, 49.77% on the CLV dataset, and 93.47% on the MUCT dataset.

In [14], a comprehensive iris recognition system was proposed, which applied Contrast-Limited Adaptive Histogram Equalization (CLAHE) after preprocessing to enhance the MMU dataset. A novel two-dimensional CNN (2D-CNN) was employed for iris pattern classification and feature extraction. GPU-based experiments demonstrated a training accuracy of 95.33%, with the model completing 400 epochs in 17 minutes and 59 seconds. In [15], a three-layered system was introduced that integrated conventional authentication, biometric verification, and searchable encryption. This method demonstrated strong performance in moderate to advanced network infrastructures and provided an optimal experience in cloud environments.

In [16], CNN-based classifiers with various ensemble structures were compared to advance the simplification of classification systems. Experimental evaluations on the MUCT dataset revealed that a well-designed ensemble significantly improved classification accuracy, achieving a recognition rate of 99.3%. In [17], a model was proposed for face detection and recognition with Face Mesh, which functioned in diverse situations, including fluctuating illumination and backdrop. The model also accommodated non-frontal images of individuals of different genders, ages, and ethnicities. The Labeled Wild Face (LWF) dataset and real-time recorded images were utilized to train the deep neural network. During testing, if the facial landmarks of the test image corresponded to those of the training images, the model identified the individual; otherwise, it outputs "unknown." This model achieved an accuracy of 94.23% in facial recognition. In [18], a facial classification system was proposed using J48 with Linear Discriminant Analysis (LDA) for feature extraction and a one-dimensional CNN Hybrid Model (1D-CNNHM). The MUCT database was employed for both training and evaluation. The J48 model achieved an accuracy of 96.01%, while the 1D-CNNHM, which incorporated LDA with Mutual Information (MI) and ANOVA, achieved a perfect classification accuracy of 100%.

III. METHODOLOGY

This methodology outlines a facial recognition-based authentication system for securing access to cloud-based environments. The system ensures that only authorized users can access sensitive data and services stored in the cloud. The MUCT and LFW datasets were selected [19, 20]. Specifically, the system uses a client-server model over the TCP/IP protocol, where extracted features are transmitted from the client device to a remote server hosted on a cloud platform. This transfer mechanism is integral to the system architecture and simulates a real-world biometric authentication scenario deployed in cloud-connected environments. The process begins on the client side, where facial images are captured. To enhance input quality, several preprocessing steps are applied, including grayscale conversion, histogram equalization, Viola-Jones detection, facial region cropping, and resizing. Next, two feature extraction techniques, GLCM and LDA, are utilized to capture the most distinctive facial characteristics. This hybrid approach leverages the strengths of multiple extraction methods, ensuring a comprehensive facial representation.

To maintain privacy and integrity, the extracted features are encrypted using the Data Encryption Standard (DES) before transmission. Then the encrypted vectors of features are securely sent to the server. Upon arrival, the server decrypts them using the same DES algorithm, restoring the original feature representations for further processing. The proposed model is integrated within an AI agent, featuring a suggested Face Fuzzy Deep Model (FFDM). The model comprises 25 layers, designed to identify individuals, and was rigorously trained on two separate datasets to ensure strong performance. The AI agent generates the choice concerning facial recognition and transmits it back to the client. Figure 1 and Algorithm 1 describe the proposed algorithm.

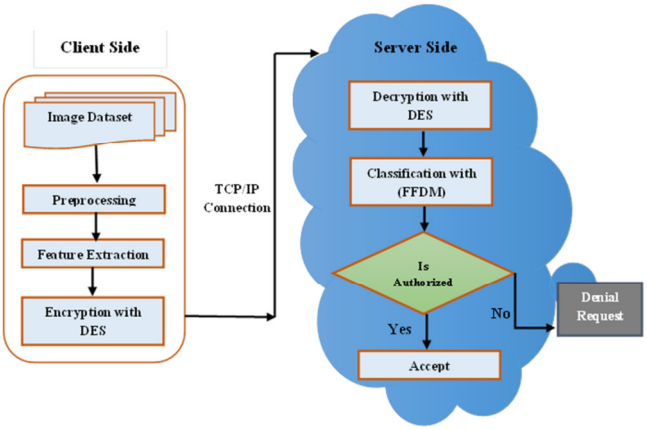

Fig. 1. The architecture of the proposed face-based recognition system.

```
Algorithm 1: Proposed facial-based
authentication model
Input: Datasets
Output: Decision of Authentication
Begin
1: Acquire facial data
2: Perform preprocessing
     Convert images to Grayscale
     Apply Histogram Equalization
     Detect facial features using the
     Viola-Jones algorithm
     Resize the image
3: Extract features using LDA and GLCM.
```

```
4: Encrypt extracted features using DES.
5: Send data with the result of the
   previous step to the cloud by TCP/IP.
6: Decrypt data using DES.
7: Implement the proposed FFDM.
8: Verify the database to retrieve
   information regarding the individual's
   acceptance or rejection status.
End
```

A. Preprocessing Stage

Data preparation is an essential phase in facial recognition, with the objective of improving the quality of facial images and facilitating the extraction of distinguishing features. The subsequent operations constitute this preprocessing phase.

1) Gray-Scale Image

The initial preprocessing phase involves transforming signature images from the conventional RGB color format to 8-bit grayscale images with the luminosity approach [18]. The usage of grayscale images, which require less data per pixel, streamlines the signature extraction process and enhances processing performance [21]:

$$greyscale = (0.3 * R) + (0.5 * G) + (0.11 * B) \quad (1)$$

2) Histogram Equalization (HE)

HE is utilized to improve image contrast. This technique redistributes the most frequent intensity values to enhance the quality of low-contrast images, thereby improving facial recognition. By adjusting the image's dynamic range, HE enhances the visibility of key facial features, making them more distinguishable [22, 23].

3) Face Detection with Viola-Jones Algorithm

The Viola-Jones algorithm is a widely used method for object detection, particularly face detection, known for its speed and accuracy. It employs four main concepts:

- Haar features, which involve analyzing differences in pixel intensities within rectangular regions of the image to capture patterns characteristic of faces.
- The Integral Image is a technique that accelerates feature computation by enabling rapid summation of pixel values above and to the left of a point.
- Adaboost is an algorithm to selects the most relevant features from a large set, reducing them to a smaller, efficient set of weak classifiers.
- Cascading is a multi-stage process where increasingly complex classifiers progressively filter out non-face regions, ensuring only the most likely face regions proceed to subsequent stages [24, 25].

After detection, the identified regions are resized using bicubic interpolation, cropped, and prepared for further analysis [26, 27]. Bicubic interpolation considers a pixel's 16 closest neighbors, as demonstrated in (2):

$$\text{i,j}=\left[W_{-1}(S_Y)\, W_0(S_Y)\, W_1(S_Y)\; W_2(S_Y)\right]$$

$$\begin{pmatrix} f_{i-1,j-1} & f_{i,j-1} & f_{i+1,j-1} & f_{i+2,j-1} \\ f_{i-1,j} & f_{i,j} & f_{i+1,j} & f_{i+2,j} \\ f_{i-1,j+1} & f_{i,j+1} & f_{i+1,j+1} & f_{i+2,j+1} \\ f_{i-1,j+2} & f_{i,j+2} & f_{i+1,j+2} & f_{i+2,j+2} \end{pmatrix} \begin{bmatrix} W_{-1}(S_X) \\ W_0(S_X) \\ W_1(S_X) \\ W_2(S_X) \end{bmatrix} \quad (2)$$

where:

$$W_{-1}(S_X) = \frac{-S^3+2S^2-S}{2},$$

$$W_0(S_X) = \frac{3S^3-5S^2+2}{2},$$

$$W_1(S_X) = \frac{-3S^3+4S^2+2}{2},$$

$$W_2(S_X) = \frac{S^3-S^2}{2}.$$

B. Feature Extraction

Feature extraction plays a crucial role in face recognition. In the proposed model, a fused face feature vector is generated using a combination of features based on appearance and texture. This approach integrates two distinct feature extraction techniques, LDA and GLCM, ensuring a comprehensive representation of facial characteristics [28, 29]. LDA can classify and extract features that are extremely discriminative between different faces, such as the distance between key facial landmarks, the width and height of the face, eyes, nose, or mouth, and the shape of the jawline, cheekbones, and forehead. LDA is designed to enhance class separability by projecting data into a lower-dimensional space, ensuring that the most critical features for distinguishing between classes are retained. This method excels at reducing the dimensionality while preserving the relevant information for classification tasks. On the other hand, GLCM focuses on the capture of intricate texture details of an image by analyzing spatial relationships between pixel intensities [30]. By combining LDA's ability to highlight discriminative features with GLCM's capacity to enrich the data with detailed texture descriptors, this integrated approach results in a robust and highly informative feature representation. The number of extracted LDA features depends on the number of classes in each dataset, determined using the formula: $number\_of\_classes - 1$. This results in an LDA feature vector of size (275 × 1). Additionally, six GLCM features, Energy, Contrast, Entropy, Homogeneity, Mean, and Inverse, are extracted, forming a GLCM feature vector of size (6×1). These features capture both global and fine-grained texture patterns in facial images. Contrast and Entropy help in edge detection and detail enhancement. Energy and Homogeneity ensure smoothness and noise resistance. Mean and Inverse provide global texture information for better classification. The resulting hybrid characteristics (281×1) were later utilized as input for the proposed DL model to identify individuals.

C. The proposed Face Fuzzy Deep Model (FFDM)

The fundamental objective of the model is to classify hybrid features extracted using the proposed feature extraction approach to determine an individual's identity. The model consists of 25 layers, including seven convolutional layers with filter sizes of 16, 32, 64, 128, 256, 512, and 395. Additionally,

it incorporates six max-pooling 1D layers, six Leaky-ReLU 1D layers, four dense 1D layers, a fuzzy layer, and a flatten layer. The input layer processes a one-dimensional feature vector with a size of (281×1) for the MUCT dataset and (5755×1) for the LFW dataset. All subsequent layers and their parameters are constructed as one-dimensional rather than two-dimensional layers. The straightforward and compact configuration of the 1D layers results in minimal computational requirements, facilitating real-time and cost-effective hardware implementation. The model was trained with a batch size of 64, over 100 epochs, and a learning rate of 0.001. The training process utilizes Adam optimizer, maintaining a learning rate of 0.001 for efficient optimization.

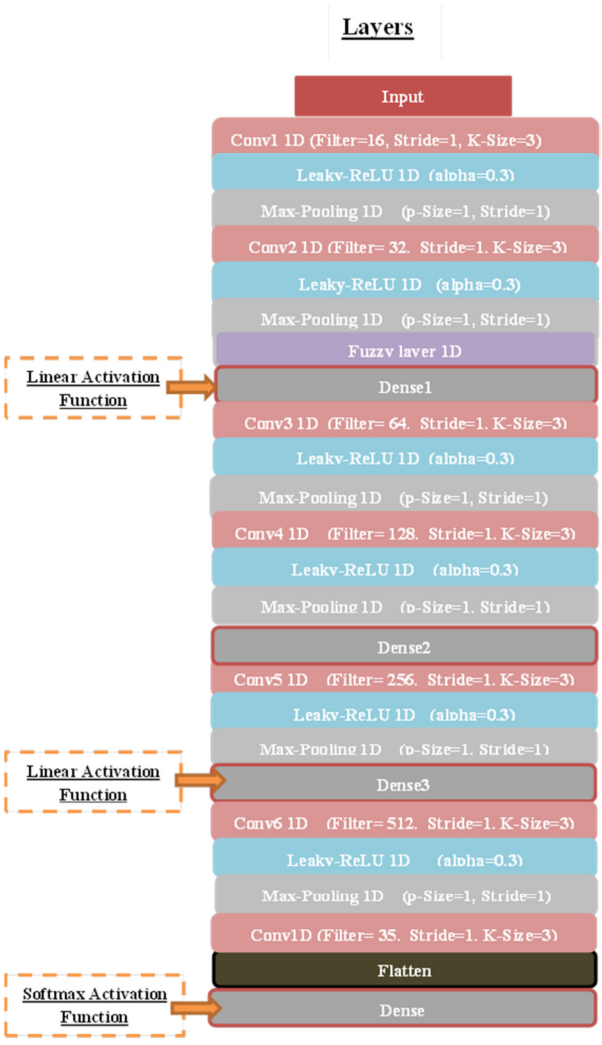

Fig. 2. The architecture of the proposed FFDM.

The main consideration in FFDM is to build weights inside the model that are different and spaced between each other to avoid overfitting. A fuzzy logic layer in a face recognition model helps handle uncertainty and variability in facial features caused by factors such as lighting, pose, and expressions. This enhances the model's ability to differentiate faces by representing features with degrees of membership rather than rigid boundaries, improving robustness and accuracy. By introducing a fuzzy layer, the model gains the ability to process uncertain and imprecise data more effectively. Traditional DL models struggle with abrupt changes in facial attributes, but the fuzzy approach allows for gradual transitions, improving classification accuracy and adaptability. Moreover, by assigning confidence levels rather than absolute labels, the fuzzy layer enhances resilience to environmental changes, mitigating the impact of noise, distortions, and overlapping features. This leads to more informed predictions, particularly in complex scenarios where traditional classification boundaries may fail. Additionally, integrating a fuzzy layer influences decision-making by enabling nonlinear analysis of facial patterns, which is crucial for distinguishing ambiguous or overlapping cases. For instance, when tested on datasets such as MUCT and LFW that contain variations in facial angles, lighting, and expressions, the fuzzy layer effectively adapts by representing facial information in flexible degrees of membership. Figure 2 shows the architecture of the FFDM.

To simulate fuzzy logic behavior, each input element x_i is potentially transformed using a Gaussian membership function defined as:

$$\mu(x_i) = \exp\left(\frac{-(x_i - c_i)^2}{2{\sigma_i}^2}\right) \quad (3)$$

where c_i denotes the center of the membership function (interpreted as the ideal or reference value), and ${\sigma_i}^2$ represents the spread, controlling the degree of fuzziness or uncertainty. When applied over the full input vector x, the fuzzy transformation can be expressed as:

$$x_{fuzzy} = \mu(x) = \exp\left(\frac{-(x-c)^2}{2\sigma^2}\right) \quad (4)$$

This function introduces non-linearity into the network and enables a soft encoding of input values based on proximity to learned fuzzy centers. Such representation enhances the model's generalization ability by tolerating small intra-class variations and mitigating the effect of noise. This adaptive approach strengthens the model's ability to maintain accuracy under challenging conditions.

IV. RESULTS AND DISCUSSION

The two datasets were utilized independently to evaluate the efficacy and performance of the proposed method against alternative methods. A learning rate of 0.001 was employed to train the FFDM, using 100 epochs and a batch size of 64. The total number of parameters derived by FFDM was 2,235,698. The datasets were randomly split into training (70%) and testing (30%) subsets. Five performance indicators were used to evaluate the effectiveness of the FFDM: accuracy, precision, recall, F1-score, and loss. The ratio of True Positive (TP) and True Negative (TN) classified points to the total points is referred to as accuracy:

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \quad (5)$$

FP and FN represent False Positive, and False Negative outcomes, respectively. The F1-score is the harmonic mean of precision and recall, while precision and recall are calculated as follows [31].

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (6)$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \quad (7)$$

$$\text{F1} - \text{score} = \frac{2*\text{Precision}*\text{Recall}}{\text{Precision+Recall}} \quad (8)$$

Table I presents a comparison of the proposed FFDM using the proposed and traditional feature extraction methods on the MUCT face dataset. The use of LDA demonstrated competitive results with a precision of 98.10% and a recall of 100%, leading to an F1-score of 99.00%. However, despite the high precision and perfect recall, using LDA offered a lower accuracy of 95.32%, which indicates that, although it correctly identifies faces in most cases, it does not generalize as well in certain situations. In contrast, using GLCM showed significantly poorer results across all performance metrics, with a precision of 21.45%, a recall of 26.06%, and an F1-score of 23.54%, highlighting the method's inefficiency in capturing discriminative features in the dataset. The FFDM with hybrid feature extraction outperformed both using LDA or GLCM by a substantial margin, achieving a near-perfect precision of 99.65% and a recall of 100%, resulting in an exceptional F1-score of 99.82%. The accuracy of 100% and the remarkably low loss of 0.0000086401 demonstrate the model's superior ability not only to classify faces with great accuracy but also to generalize effectively to the dataset, avoiding overfitting. These results highlight the strength of the proposed fuzzy logic layer, which contributes to the model's flexibility and robustness in handling variations in facial features.

TABLE I. RESULTS OF FFDM WITH FEATURES ON MUCT

Method	Precision	Recall	F1-score	Accuracy	Loss
LDA with FFDM	98.l0%	100%	99.00%	95.32%	0.00056201
GLCM with FFDM	21.45%	26.06%	23.54%	30.42%	5.0073
Hybrid features with FFDM	99.65%	100%	99.82%	100%	0.00000864

Table II compares the proposed FFDM and traditional feature extraction methods on the LFW dataset. Similarly to the MUCT dataset, the proposed FFDM achieved perfect performance with 100% precision, 100% recall, and 100% accuracy, along with a very low loss of 0.0000088609, demonstrating the superiority of the fuzzy logic layer in handling variability and achieving outstanding results.

TABLE II. RESULTS OF FFDM WITH FEATURES ON LFW

Method	Precision	Recall	F1-score	Accuracy	Loss
LDA with FFDM	98.68%	99.50%	99.12%	95.32%	0.0003439
GLCM with FFDM	18.75%	20.00%	19.35%	30.42%	7.0256
Hybrid features with FFDM	100%	100%	100%	100%	0.00000886

The comparisons in Tables III and IV demonstrate the significant superiority of FFDM over traditional ML algorithms. Naïve Bayes struggled with a relatively low accuracy of 54.50% and 55% F1-score, highlighting its limited ability to capture complex patterns in facial data, possibly due to its simplistic assumptions. KNN shows improved performance with an accuracy of 80.65%, but still falls short compared to the proposed model, as it may not generalize well to new data despite its reasonable precision and recall. Adaboost and Decision Tree both provided moderate results, indicating that these models, while effective in some contexts, are insufficient for facial recognition, as they struggle with feature complexity and noise. In contrast, the proposed FFDM achieved 100% accuracy and near-perfect precision and recall. This can be attributed to the fuzzy logic layer that enhances the model's flexibility, enabling it to better handle variations in facial features such as lighting and expressions, which traditional models fail to address effectively.

TABLE III. PERFORMANCE COMPARISON OF FFDM WITH ML ALGORITHMS ON MUCT

Algorithm	Accuracy	Precision	Recall	F1-score
Naïve Bayes	54.50%	69%	58%	55%
K-NN	80.65%	81%	78%	78%
Adaboost	70.10%	67%	67%	67%
Decision Tree	69.40%	65%	67%	67%
Proposed FFDM	100%	99.65%	100%	99.82%

TABLE IV. PERFORMANCE COMPARISON OF FFDM WITH ML ALGORITHMS ON LFW

Algorithm	Accuracy	Precision	Recall	F-score
Naïve Bayes	50.70%	67%	51%	55%
K-NN	77.65%	78%	78%	78%
Adaboost	67.37%	67%	67%	67%
Decision Tree	66.66%	67%	67%	67%
Proposed FFDM	100%	100%	100%	100%

V. CONCLUSIONS

This study presented a hybrid feature-based approach for face authentication within a cloud environment and introduced a fuzzy face deep learning model (FFDM) that was trained and tested on the MUCT and LFW datasets. Facial images were preprocessed, including grayscale conversion, histogram equalization, Viola-Jones detection, and scaling. Then, LDA and GLCM were employed to extract hybrid features, which were further encrypted using DES before transmission to the cloud server. After decryption, the features were input into the FFDM, which incorporated a fuzzy layer to improve recognition precision. FFDM exhibited exceptional accuracy and significant enhancements, with a precision of 99.65% and 100% for MUCT and LFW, respectively, underscoring its ability to adeptly manage variances in facial features. The results underscore the efficacy of the fuzzy logic layer in improving recognition performance and ensuring optimal generalization.

Future work will focus on augmenting FFDM by incorporating additional biometric modalities, such as iris and voice recognition, to enhance security and resilience. Furthermore, the model will be evaluated using larger and more heterogeneous datasets and include more metrics to establish optimal thresholds, ensuring the system's ability to ensure improved generalization across various demographics and real-world contexts.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest to report regarding this present study.

REFERENCES

[1] M. Zulfiqar, F. Syed, M. J. Khan, and K. Khurshid, "Deep Face Recognition for Biometric Authentication," in *2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, Swat, Pakistan, Jul. 2019, pp. 1–6, https://doi.org/10.1109/ICECCE47252.2019.8940725.

[2] E. Setiawan and A. Muttaqin, "Implementation of K-Nearest Neightbors Face Recognition on Low-power Processor," *TELKOMNIKA*, vol. 13, no. 3, pp. 949–954, Sep. 2015, https://doi.org/10.12928/telkomnika.v13i3.713.

[3] H. M. Al-Dabbas, R. A. Azeez, and A. E. Ali, "Digital Watermarking, Methodology, Techniques, and Attacks: A Review," *Iraqi Journal of Science*, pp. 4169–4186, Aug. 2023, https://doi.org/10.24996/ijs.2023.64.8.37.

[4] S. Sharma, M. Bhatt, and P. Sharma, "Face Recognition System Using Machine Learning Algorithm," in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, India, Jun. 2020, pp. 1162–1168, https://doi.org/10.1109/ICCES48766.2020.9137850.

[5] B. Manesh, "Machnine Learning Algorithms – A Review," *International Journal of Science and Research*, vol. 9, no. 1, pp. 381-386, Jan. 2020.

[6] N. Singhal, V. Ganganwar, M. Yadav, A. Chauhan, M. Jakhar, and K. Sharma, "Comparative study of machine learning and deep learning algorithm for face recognition," *Jordanian Journal of Computers and Information Technology*, vol. 7, no. 3, pp. 313–325, 2021, https://doi.org/10.5455/jjcit.71-1624859356.

[7] M. R. Mahmood, M. B. Abdulrazzaq, S. R. M. Zeebaree, A. K. Ibrahim, R. R. Zebari, and H. I. Dimo, "Classification techniques' performance evaluation for facial expression recognition," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 2, pp. 1176–1184, Feb. 2021, https://doi.org/10.11591/ijeecs.v21.i2.pp1176-1184.

[8] A. Hasan and M. Mazinani, "Detection of Keratoconus Disease Depending on Corneal Topography using Deep Learning," *Kufa Journal of Engineering*, vol. 16, no. 1, pp. 463–478, Feb. 2025, https://doi.org/10.30572/2018/KJE/160125.

[9] N. A. Taha, Z. Qasim, A. Al-Saffar, and A. A. Abdullatif, "Steganography using dual tree complex wavelet transform with LSB indicator technique," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 9, no. 2, pp. 1106–1114, Jun. 2021, https://doi.org/10.21533/pen.v9i2.2060.

[10] M. Prabhu, G. Revathy, and R. R. Kumar, "Deep learning based authentication secure data storing in cloud computing," *International Journal of Computer and Engineering Optimization*, vol. 1, no. 01, pp. 10–14, 2023.

[11] I. H. Sarker, "Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions," *SN Computer Science*, vol. 2, no. 6, Nov. 2021, Art. no. 420, https://doi.org/10.1007/s42979-021-00815-1.

[12] A. Al-Qaisi, M. S. AlTarawneh, A. ElSaid, and Z. Alqadi, "A Hybrid Method of Face Feature Extraction, Classification Based on MLBP and Layered-Recurrent Network," *Traitement du Signal*, vol. 37, no. 4, pp. 555–561, Oct. 2020, https://doi.org/10.18280/ts.370402.

[13] H. Nguyen-Quoc and V. T. Hoang, "A Revisit Histogram of Oriented Descriptor for Facial Color Image Classification Based on Fusion of Color Information," *Journal of Sensors*, vol. 2021, no. 1, 2021, Art. no. 6296505, https://doi.org/10.1155/2021/6296505.

[14] B. K. O. C. Alwawi and A. F. Y. Althabhawee, "Towards more accurate and efficient human iris recognition model using deep learning technology," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 20, no. 4, pp. 817–824, Aug. 2022, https://doi.org/10.12928/telkomnika.v20i4.23759.

[15] M. I. Mihailescu and S. L. Nita, "A Searchable Encryption Scheme with Biometric Authentication and Authorization for Cloud Environments," *Cryptography*, vol. 6, no. 1, Mar. 2022, Art. no. 8, https://doi.org/10.3390/cryptography6010008.

[16] R. Szmurło and S. Osowski, "Ensemble of classifiers based on CNN for increasing generalization ability in face image recognition," *Bulletin of the Polish Academy of Sciences Technical Sciences*, pp. 141004–141004, Apr. 2022, https://doi.org/10.24425/bpasts.2022.141004.

[17] S. Hangaragi, T. Singh, and N. N, "Face Detection and Recognition Using Face Mesh and Deep Neural Network," *Procedia Computer Science*, vol. 218, pp. 741–749, 2023, https://doi.org/10.1016/j.procs.2023.01.054.

[18] H. M. Al-Dabbas, R. A. Azeez, and A. E. Ali, "Two Proposed Models for Face Recognition: Achieving High Accuracy and Speed with Artificial Intelligence," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13706–13713, Apr. 2024, https://doi.org/10.48084/etasr.7002.

[19] S. Milborrow, J. Morkel, and F. Nicolls, "The MUCT landmarked face database." 2010, [Online]. Available: http://www.milbo.org/muct/.

[20] "Labelled Faces in the Wild (LFW) Dataset." Kaggle, [Online]. Available: https://www.kaggle.com/datasets/jessicali9530/lfw-dataset.

[21] W. A. Mustafa and M. M. M. Abdul Kader, "A Review of Histogram Equalization Techniques in Image Enhancement Application," *Journal of Physics: Conference Series*, vol. 1019, Jun. 2018, Art. no. 012026, https://doi.org/10.1088/1742-6596/1019/1/012026.

[22] Z. Hashim, H. Mohsin, and A. Alkhayyat, "Signature verification based on proposed fast hyper deep neural network," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 13, no. 1, pp. 961–973, Mar. 2024, https://doi.org/10.11591/ijai.v13.i1.pp961-973.

[23] Z. Hashim, H. Mohsin, and A. Alkhayyat, "Offline Handwritten Signature Identification based on Hybrid Features and Proposed Deep Model," *Iraqi Journal For Computer Science and Mathematics*, vol. 5, no. 1, pp. 220–236, Feb. 2024, https://doi.org/10.52866/ijcsm.2024.05.01.016.

[24] M. N. Chaudhari, M. Deshmukh, G. Ramrakhiani, and R. Parvatikar, "Face Detection Using Viola Jones Algorithm and Neural Networks," in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, Pune, India, Aug. 2018, pp. 1–6, https://doi.org/10.1109/ICCUBEA.2018.8697768.

[25] H. M .Al-Dabbas, R. A. Azeez, and A. E. Ali, "High-accuracy models for iris recognition with merging features," *International Journal of Advanced and Applied Sciences*, vol. 11, no. 6, pp. 89–96, Jun. 2024, https://doi.org/10.21833/ijaas.2024.06.010.

[26] M. K. Dabhi and B. K. Pancholi, "Face Detection System Based on Viola - Jones Algorithm," *International Journal of Science and Research (IJSR)*, vol. 5, no. 4, pp. 62–64, 2013.

[27] W. H. Abdulsalam, R. S. Alhamdani, and M. N. Abdullah, "Facial Emotion Recognition from Videos Using Deep Convolutional Neural Networks," *International Journal of Machine Learning and Computing*, vol. 9, no. 1, pp. 14–19, 2019, https://doi.org/10.18178/ijmlc.2019.9.1.759.

[28] W. H. Abdulsalam, R. S. Alhamdani, and M. N. Abdullah, "Emotion Recognition System Based on Hybrid Techniques," *International Journal of Machine Learning and Computing*, vol. 9, no. 4, pp. 490–495, Aug. 2019, https://doi.org/10.18178/ijmlc.2019.9.4.831.

[29] M. Norouzi and A. Arshaghi, "A Survey on Face Recognition Based on Deep Neural Networks," *Majlesi Journal of Telecommunication Devices*, vol. 12, no. 4, pp. 193–199, 2023, https://doi.org/10.21203/rs.3.rs-1367031/v1.

[30] N. H. Barnouti, "Improve Face Recognition Rate Using Different Image Pre-Processing Techniques," *American Journal of Engineering Research*, vol. 5, no. 4, pp. 46–53, 2016.

[31] A. B. S. Salamh and H. I. Akyüz, "A Novel Feature Extraction Descriptor for Face Recognition," *Engineering, Technology & Applied Science Research*, vol. 12, no. 1, pp. 8033–8038, Feb. 2022, https://doi.org/10.48084/etasr.4624.