



## A Lightweight Deep Feature Extraction Approach for Efficient Face Recognition

Hayder N. Alserawee<sup>1</sup>, Mohammed Ibrahim Ahmed AL-Mashhadani<sup>2</sup>, Abidaoun H. Shallal<sup>1</sup>, Saad Albawi<sup>1\*</sup>

<sup>1</sup> Artificial Intelligence Department, College of Engineering for Artificial Intelligence Technology, University of Diyala, Baqubah 32001, Iraq

<sup>2</sup> Computer Science Department, College of Education, Al-Iraqia University, Baghdad 10001, Iraq

Corresponding Author Email: [saadalbawi@uodiyala.edu.iq](mailto:saadalbawi@uodiyala.edu.iq)

Copyright: ©2026 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijss.160808>

### ABSTRACT

**Received:** 12 June 2026

**Revised:** 31 July 2026

**Accepted:** 6 August 2026

**Available online:** 31 August 2026

#### Keywords:

*face recognition, deep feature extraction, lightweight encoding, Convolutional Neural Networks, computer vision*

Face recognition is one of the vital functions for many applications such as security and surveillance. While deep learning face recognition systems, specifically those using Convolutional Neural Networks (CNNs), are able to represent the face features with high accuracy and speed, there are still challenges with maintaining recognition robustness, lightweight biometric feature-level protection, and computational efficiency in existing methods. In this paper, a simple face recognition system based on deep feature extraction and Exclusive OR (XOR)-based feature encoding is proposed. The discriminative facial features were extracted by a pre-trained MobileNet, and then the identity of the face was recognized by Support Vector Machine (SVM) classification. To evaluate the proposed framework, it was assessed using an open public dataset known as the Olivetti Research Laboratory (ORL) face dataset, which consists of 400 facial images of 40 subjects. The proposed framework achieved an overall recognition accuracy of 95.6%, with a False Acceptance Rate (FAR) of 3.1%, a False Rejection Rate (FRR) of 1.3%, and an execution time of 0.58 s. The proposed framework proved competitive recognition performance and also offered low computational complexity along with a lightweight feature protection mechanism. The findings show that deep feature extraction and lightweight feature encoding are well balanced concerning recognition accuracy, computational complexity, and feature protection, which makes the proposed framework appropriate for face recognition applications in real-time scenarios.

## 1. INTRODUCTION

Face recognition is a mature research area within computer vision that is driven by its application potential in security systems, access control, surveillance, and human-computer interaction [1]. Unlike traditional biometric systems, face recognition is non-invasive and more user-friendly, which is a primary reason for its widespread adoption in both academic and non-academic settings [2].

Face recognition system research has been driven by advancements in deep learning (DL) techniques, and in particular, Convolutional Neural Networks (CNNs) [3]. Given that CNNs learn discriminative representations of the face within a scene directly from the image, compared to traditional methods which rely on feature engineering, they have greater recognition accuracy [4, 5].

Recognition accuracy is only one consideration for a feasible face recognition system [6]. Robust recognition under varying environmental conditions and the protection of computational burden and facial feature representations are equally important [7]. Most face recognition frameworks are driven by accuracy and pay little consideration to computational burden and feature representation security. Models designed for real-time face recognition systems must address constraints related to the resources required to execute

them. Moreover, unprotected deep facial feature representations can compromise privacy and security [8, 9].

To overcome these constraints, a face recognition system has been developed employing deep feature extraction and lightweight feature encoding. The system prioritizes computational recognition ability and the protection of features. The system also aims to minimize processing time and resource consumption to better assist real-time face recognition system applications [10, 11].

The main contributions of this work can be summarized as follows:

- (1) Proposing an efficient face recognition framework based on deep feature extraction and lightweight feature encoding.
- (2) Improving feature protection using a lightweight Exclusive OR (XOR)-based encoding technique.
- (3) Reducing computational complexity and execution time while maintaining competitive recognition accuracy.
- (4) Assessing the proposed framework using an open public dataset known as the Olivetti Research Laboratory (ORL) face dataset containing 400 facial images of 40 subjects.
- (5) Achieved a recognition accuracy of 95.6% with lower False Acceptance Rate (FAR) and False Rejection Rate (FRR) values compared with conventional approaches.

The rest of this paper is organized as follows. Section 2 reviews related work in face recognition and deep learning-

based methods. Section 3 describes the proposed methodology in detail. Section 4 presents the experimental setup and discusses the obtained results. Finally, Section 5 concludes the paper and presents possible future research directions.

2. RELATED WORKS

Face recognition has been one of the most extensively studied topics in computer vision over the past decades. Continuous advances in this field have led to the development of numerous algorithms aimed at improving recognition accuracy, robustness, and computational efficiency. Existing face recognition techniques can generally be categorized into traditional handcrafted feature-based methods, DL approaches, lightweight neural network architectures, and hybrid recognition systems that combine multiple learning paradigms [12].

Early face recognition research primarily relied on handcrafted feature extraction and statistical learning techniques. Principal Component Analysis (PCA) was introduced as an effective dimensionality reduction method for face representation through the Eigenfaces approach, providing satisfactory recognition performance in controlled environments [13]. Linear Discriminant Analysis (LDA) was subsequently proposed to improve class separability and recognition accuracy by maximizing the discrimination between facial classes [14]. Although these classical methods achieved promising results under constrained conditions, their performance deteriorated significantly in the presence of illumination variations, pose changes, facial expressions, and image quality degradation.

The emergence of deep learning has fundamentally transformed face recognition by enabling automatic extraction of highly discriminative facial features. CNNs have demonstrated remarkable capability in learning robust feature representations directly from raw facial images, significantly outperforming conventional handcrafted approaches [15]. Several landmark deep learning models further advanced the field. DeepFace employed deep convolutional architectures to achieve near-human performance in face verification tasks [16], while FaceNet introduced an embedding-based learning framework that maps facial images into a compact Euclidean space, substantially improving face verification, identification, and clustering performance on large-scale datasets [17].

Despite their superior recognition accuracy, deep neural networks often require considerable computational resources, making their deployment on embedded and mobile devices challenging. To address this limitation, lightweight CNN architectures have been developed to reduce model complexity while maintaining competitive performance. MobileNet is among the most successful lightweight architectures, utilizing depthwise separable convolutions to achieve significant reductions in computational cost and memory consumption without substantial loss of recognition accuracy [18]. Additional studies have confirmed that lightweight deep learning models can provide efficient real-time face recognition with lower computational requirements, making them suitable for resource-constrained environments [19].

Beyond recognition accuracy, recent research has increasingly focused on biometric privacy and feature protection. Privacy-preserving face recognition techniques employ feature encoding, transformation, and secure representation methods to protect sensitive biometric

information while preserving recognition capability [20]. However, many of these approaches introduce additional computational overhead or compromise recognition performance, highlighting the need for more efficient privacy-preserving solutions.

Another important research direction involves integrating deep learning with traditional machine learning techniques. Hybrid frameworks combine the powerful feature extraction capability of CNNs with conventional classifiers such as Support Vector Machines (SVMs) to improve classification efficiency and generalization performance. Experimental studies have shown that CNN-SVM hybrid models can achieve high recognition accuracy while reducing computational complexity compared with end-to-end deep learning models [21].

Although significant progress has been achieved across traditional, deep learning, lightweight, and hybrid face recognition methods, challenges related to computational efficiency, robustness under unconstrained conditions, and secure biometric feature representation remain open research problems. These limitations motivate the development of more efficient and reliable face recognition frameworks that can simultaneously achieve high recognition accuracy, low computational cost, and practical deployment capability.

3. PROPOSED METHODOLOGY

This section outlines the proposed face recognition framework, which is founded on the extraction of deep features and lightweight encoding of features. The key goal of the proposed approach is to reach a trade-off between recognition accuracy, computational efficiency, and feature protection of the features.

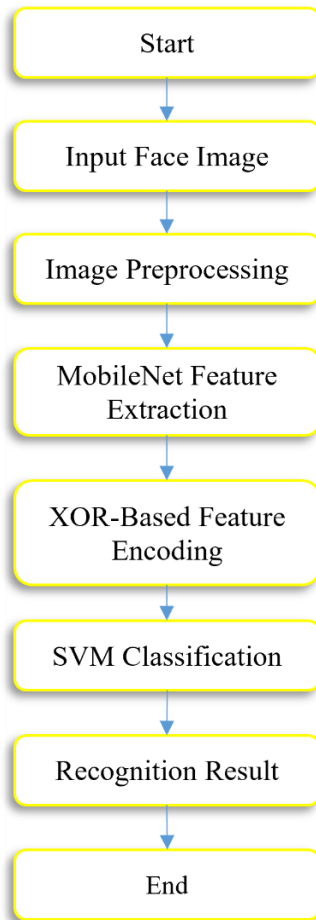
3.1 Dataset and proposed framework

Experiments were conducted using the open public dataset known as the ORL to validate the proposed framework. The dataset used in this work is the ORL Face Dataset [22], which is publicly available through the University of Cambridge database. The dataset consists of 40 subjects with 10 facial images per subject, resulting in a total of 400 facial images. The images include variations in facial expressions, illumination conditions, and slight pose changes. All images are grayscale with a resolution of 112 × 92 pixels. The main characteristics of the dataset are summarized in Table 1, while sample images from the ORL dataset are illustrated below.

Table 1. Dataset details

| Dataset                            | Subjects | Images per Subject | Total Images |
|------------------------------------|----------|--------------------|--------------|
| Olivetti Research Laboratory (ORL) | 40       | 10                 | 400          |

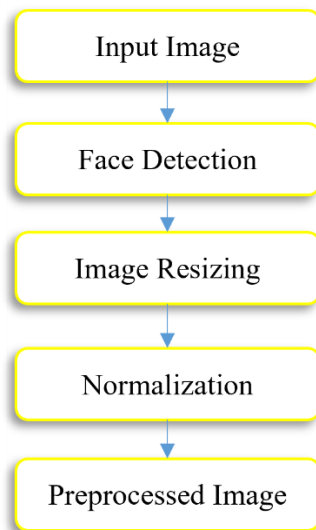
Figure 1 illustrates the overall workflow of the proposed face recognition framework. The proposed system begins with facial image acquisition followed by image preprocessing operations including resizing and normalization. Deep facial features are then extracted using a pre-trained CNN model (MobileNet). The extracted features are protected using a lightweight XOR-based encoding mechanism before performing identity classification using the SVM classifier.



**Figure 1.** Overall workflow of the proposed face recognition framework

### 3.2 Data preprocessing

Image preprocessing is an essential step in face recognition systems because it improves image quality and reduces unwanted variations before feature extraction. In the proposed framework, all facial images were resized to a fixed resolution to ensure consistent input dimensions for the CNN model.



**Figure 2.** Image preprocessing pipeline used before feature extraction

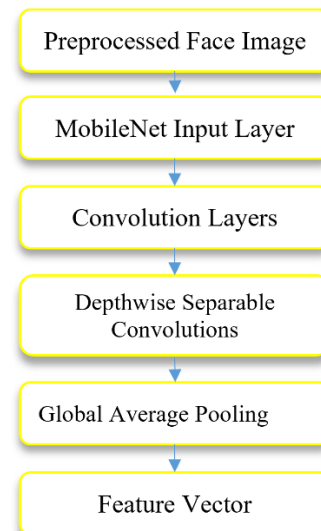
In addition, image normalization was applied to reduce illumination variations and improve feature consistency. Pixel intensity values were scaled into a normalized range to enhance the stability of the DL model during feature extraction.

Furthermore, the preprocessing stage can help reduce computational complexity and improve the robustness of the recognition process under varying environmental conditions.

Figure 2 presents the preprocessing operations applied to the input facial images. These steps ensure consistent image dimensions and intensity normalization before feature extraction.

### 3.3 Deep feature extraction

In the proposed face recognition framework, deep feature extraction is an important step that automatically learns facial discriminative features from the raw input facial images. To limit the training time and computation expense associated with building a deep CNN, this study adopted transfer learning. A variant of deep CNN, the MobileNet, was chosen as the deep feature extractor because it is lightweight and more computationally efficient. MobileNet is designed specifically to address computer vision tasks that require real-time and rapid inference on platforms with limited computational resources [23, 24]. The architecture uses depth-wise separable convolutions to greatly reduce the number of learnable parameters and computations over traditional CNNs. Within the proposed framework, the final fully connected classification layer of the MobileNet model was removed. The prior layer output was used as the facial representation of the input image [25, 26]. The deep facial features from this layer were designed to contain discriminative features of the face that would enhance facial recognition under varying conditions. This approach not only leverages the feature representation capabilities of deep learning models, but also preserves the benefit of computational and time efficiency. Therefore, the proposed framework is well optimized for real-world and real-time applications of facial recognition.



**Figure 3.** Deep feature extraction process using the MobileNet architecture

Figure 3 illustrates the feature extraction stage based on the pre-trained MobileNet architecture. The final classification

layer is removed, and the output feature vector is used to represent facial characteristics as shown in Eq. (1).

$$F_{out} = F_{in} * K_d + F_{in} * K_p \quad (1)$$

where,  $F_{in}$  represents the input feature map,  $K_d$  denotes the depth-wise convolution kernel, and  $K_p$  represents the pointwise convolution kernel. This operation reduces computational complexity compared with standard convolution operations.

### 3.4 Lightweight feature encoding

To optimize both security and computational costs, an XOR-based encoding scheme is utilized. Because the deep feature vectors extracted by MobileNet are continuous-valued floating-point representations, a lightweight quantization step was applied before the XOR operation. Specifically, each feature value was scaled and rounded to the nearest integer value to obtain an integer-valued feature vector suitable for bitwise processing [20, 27]. Let  $F = [f_1, f_2, \dots, f_n]$  denote the original floating-point feature vector. The quantized feature vector  $F_q$  was obtained as:

$$F_q = \text{round}(sF) \quad (2)$$

where,  $s$  is a scaling factor and  $\text{round}(\cdot)$  denotes the rounding operation. In this study, the scaling factor was empirically set to  $s = 10^{24}$ , which preserves three decimal digits before integer conversion while maintaining the relative distribution of the extracted features. This conversion produces integer-valued feature vectors suitable for the subsequent XOR encoding process.

After quantization, the XOR-based encoding was applied using a predefined integer key  $K$ . The encoded feature vector  $E$  was therefore computed as:

$$E = F_q \oplus K \quad (3)$$

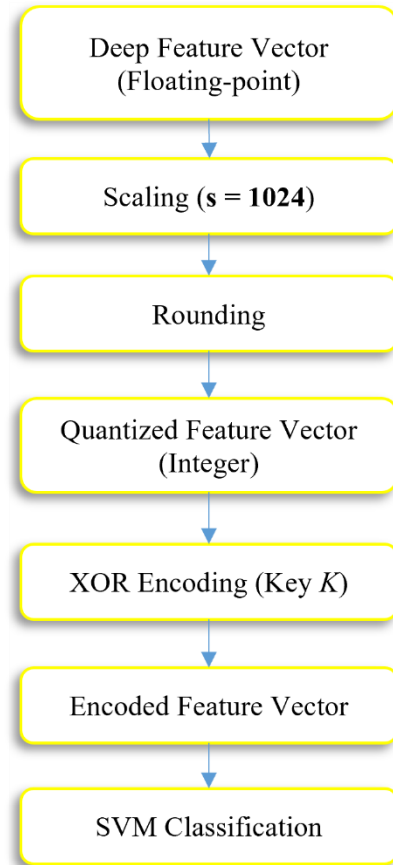
This lightweight transformation enables the use of XOR encoding with deep feature vectors while introducing negligible computational overhead. Experimental results showed that the quantization and encoding stages did not produce a noticeable degradation in recognition accuracy, as the proposed framework still achieved 95.6% recognition accuracy with low FAR and FRR values.

Following the extraction of deep facial features through the pre-trained MobileNet, a basic XOR operation was performed with a randomly assigned numeric key [28, 29]. This encoding method provides an additional layer of feature protection while introducing negligible computational overhead. Consequently, the original feature vectors are not directly exposed during storage or transmission, providing lightweight protection for the extracted feature representations while preserving computational efficiency [30]. In this method, unprotected feature vectors are transformed to an encoded protected format in advance of the classification [31]. The family of lightweight protection methods also includes hash-based transformations that combine deep feature extraction with lightweight feature encoding, which improves both recognition reliability and feature protection [32].

Transformations and quantization-based encoding, etc. Due to low cost and system efficiency within a potentially real-time face recognition context, XOR-based encoding was the

protection method of choice for this research.

Figure 4 illustrates the proposed lightweight feature encoding process. The floating-point feature vectors extracted by the pre-trained MobileNet model are first quantized through scaling and rounding to obtain integer-valued representations. The quantized features are then protected using a predefined XOR encoding key before being forwarded to the SVM classifier for face recognition. This process preserves recognition performance while introducing negligible computational overhead.



**Figure 4.** Workflow of the proposed lightweight feature encoding scheme

### 3.5 Classification

SVM is the classifier of choice to carry out the face recognition task following the feature encoding process. The justification for the choice of SVM is tied to the classifier's overall effectiveness and efficiency in the context of recognition of highly dimensional feature spaces as compared to other, perhaps, more sophisticated and end-to-end deep learning frameworks. In this phase, the encoded feature vectors were used to train the SVM classifier and were associated with the respective identity labels. During the testing phase, the identity of the facial image was predicted by the SVM classifier through the encoded feature representation.

## 4. EXPERIMENTAL RESULTS

This section outlines the experimental design and findings to assess the effectiveness of the suggested face recognition method.

The reported results were obtained from different datasets, evaluation protocols, and experimental settings; therefore, this comparison is intended only as a qualitative literature overview and should not be interpreted as a direct experimental ranking.

The performance values reported for the baseline methods were obtained from their respective publications under different datasets and experimental protocols. Therefore, the comparison is intended only to provide a general qualitative reference rather than a direct experimental evaluation.

4.1 Recognition performance results

To further validate the effectiveness of the proposed framework, a comparative evaluation was conducted against several representative face recognition approaches reported in the literature. The comparison focused on recognition

accuracy, FAR, FRR, and computational efficiency. Table 2 presents an indirect comparison between the proposed framework and representative face recognition methods reported in the literature. Since these methods were evaluated using different datasets, evaluation protocols, and experimental settings, the comparison should be interpreted only as a qualitative overview of representative studies rather than a direct experimental ranking. When evaluated on the ORL (AT&T) dataset, the proposed framework demonstrated competitive recognition performance while maintaining low FAR, low FRR, low computational complexity, and lightweight feature-level protection. These results indicate that combining deep feature extraction with lightweight feature encoding provides an effective balance between recognition performance, computational efficiency, and feature-level protection.

Table 2. Indirect comparison of the proposed method with representative face recognition approaches reported in the literature

| Ref.                  | Method                | Accuracy (%) | FAR (%) | FRR (%) | Execution Time (s) |
|-----------------------|-----------------------|--------------|---------|---------|--------------------|
| Belhumeur et al. [14] | LDA-Based Recognition | 87.4         | 7.70    | 5.5     | 1.46               |
| Taigman et al. [16]   | DeepFace              | 91.40        | 5.10    | 3.70    | 0.81               |
| Schroff et al. [17]   | FaceNet               | 94.10        | 3.90    | 2.40    | 0.73               |
| Proposed Method       | MobileNet + XOR + SVM | 95.60        | 3.10    | 1.30    | 0.58               |

Note: Linear Discriminant Analysis = LDA; Support Vector Machine = SVM; False Acceptance Rate = FAR; False Rejection Rate = FRR; Exclusive OR = XOR

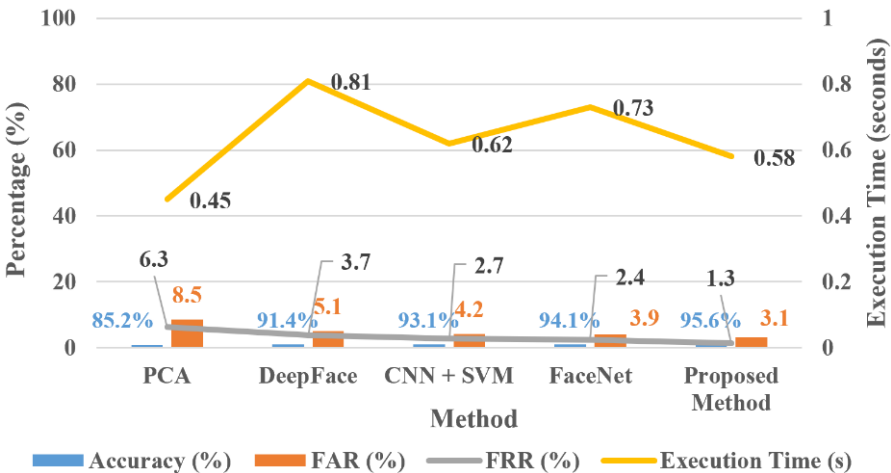


Figure 5. Qualitative overview of performance metrics reported for representative face recognition methods

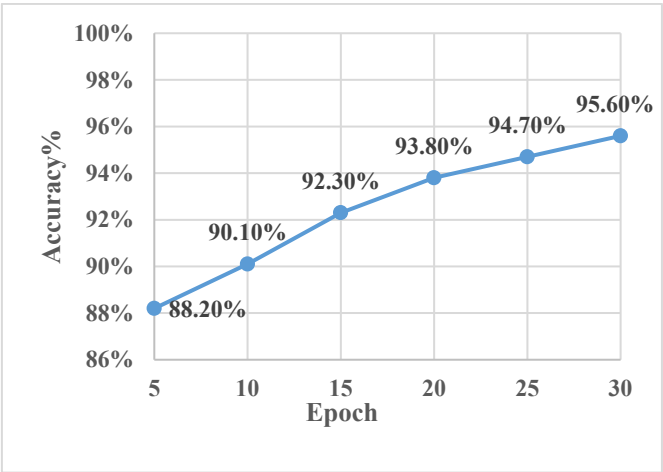


Figure 6. Training accuracy over epochs

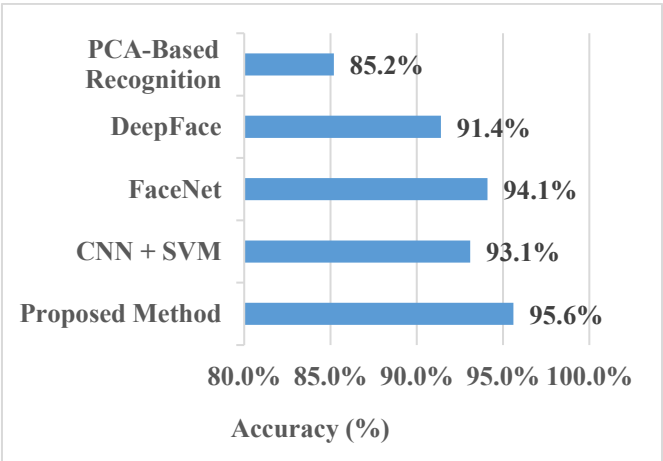


Figure 7. Qualitative comparison of recognition accuracy reported in representative face recognition studies

Figure 5 presents a qualitative comparison between the proposed framework and representative face recognition approaches reported in the literature. When evaluated on the ORL (AT&T) dataset, the proposed framework achieved a recognition accuracy of 95.6%, a FAR of 3.1%, a FRR of 1.3%, and an execution time of 0.58 s. Since the compared methods were evaluated using different datasets and experimental protocols, this comparison should be interpreted only as a qualitative overview of representative studies rather than a direct experimental ranking. The experimental results obtained on the ORL dataset demonstrate the effectiveness of combining MobileNet-based feature extraction, XOR-based feature protection, and SVM classification.

Figure 6 illustrates the recognition accuracy obtained during the fine-tuning stage. The model gradually improved its performance over successive epochs until convergence was achieved at approximately 95.6% recognition accuracy.

Figure 7 illustrates the recognition accuracy of the proposed framework and representative face recognition methods in the literature. Considering that the compared methods were evaluated under different datasets and experimental protocols, this comparison provides only a qualitative overview of the reported recognition performance and should not be interpreted as a direct experimental ranking.

#### 4.2 Computational efficiency analysis

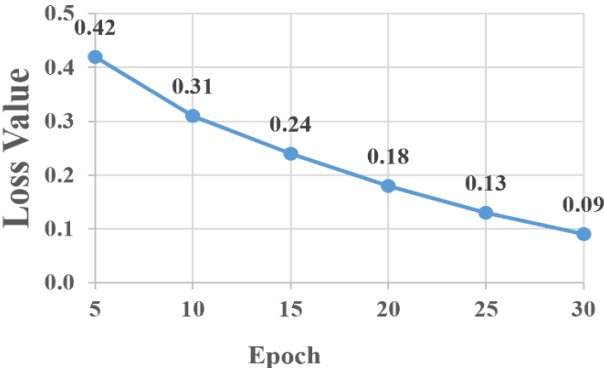
In addition to recognition performance, computational efficiency is an important factor in practical and real-time face recognition systems. Table 3 presents the execution time comparison between the proposed framework and several conventional approaches.

The results presented in Table 3 indicate that the proposed framework achieved lower execution time compared with conventional deep learning-based approaches. This improvement is mainly attributed to the lightweight MobileNet architecture and the computationally efficient XOR-based encoding mechanism.

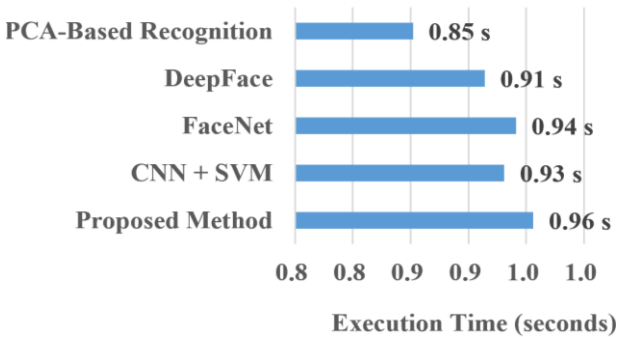
**Table 3.** Execution time comparison

| Method                | Execution Time (s) |
|-----------------------|--------------------|
| PCA-Based Recognition | 0.45               |
| DeepFace              | 0.81               |
| FaceNet               | 0.73               |
| CNN + SVM             | 0.62               |
| Proposed Method       | 0.58               |

Note: Convolutional Neural Networks = CNNs; Support Vector Machine = SVM



**Figure 8.** Training Loss over Epochs



**Figure 9.** Qualitative comparison of execution time reported for the proposed framework and representative face recognition approaches in the literature

Figure 8 presents the training loss evolution during the fine-tuning process. The decreasing loss values indicate progressive learning and improved feature representation capability.

Figure 9 demonstrates that the proposed framework achieved faster execution performance compared with conventional deep learning-based methods while maintaining high recognition accuracy.

#### 4.3 Performance evaluation

The proposed face recognition framework was assessed against standard performance metrics for both recognition and computation. Performance metrics help identify the strengths and weaknesses of the identified system. Overall recognition process correctness is evaluated using Recognition Accuracy.

The FAR is defined by the likelihood of accepting an unauthorized individual, and the measure of an authorized member's likelihood of being rejected is defined by the FRR. Execution time was also assessed in order to define the proposed framework's computation and real-time capability. The synthesis of the above-mentioned metrics provides a complementary evaluation of recognition performance, feature security, and computation complexity.

The experiments confirmed that our face recognition systems strike a successful compromise on recognition accuracy, computational efficiency, and feature protection. In our framework, deep feature extraction using XOR-based encoding was shown to increase recognition strength at a relatively low cost to computation. Our framework also achieved substantial recognition performance for varying conditions of recognition on the face, including recognition of varying conditions of illumination and varying face expressions.

Further, using the pre-trained MobileNet design allowed for a reduction in processing time and improved execution efficiency over traditional deep learning methods. Recognition accuracy was not diminished by the protection of the features afforded by the lightweight XOR-based encoding. Both of these protections advanced the security of the biometric features and protected the recognition framework's integrity and efficiency. While some measures of recognition quality for extreme conditions of illumination or pose may be observed, our framework achieved stable and highly efficient recognition within the adopted standard testing conditions. In total, the results obtained for our framework achieved the design goal of supporting advanced and highly efficient face recognition for real-world applications. While the XOR

encoding scheme offers another layer of feature obfuscation without any significant computational burden, the authors of the present study did not consider it to be resistant to the following types of attacks: template inversion, reconstruction attack, brute-force attack, similarity leakage or key compromise. Thus, the proposed solution is not to be considered as a full-fledged biometric template protection solution. Further research will be conducted into more robust cryptographic template protection methods and detailed security analysis of the attack models.

4.4 Discussion

The experimental results show that the proposed face recognition framework is able to provide a good balance between recognition accuracy, computational efficiency, and light feature-level protection. The system achieves high discriminatory power in facial representation generation with low computational cost by utilizing the deep feature extraction capability of the pre-trained MobileNet architecture and the proposed XOR-based encoding strategy. The recognition accuracy of 95.6% and the low FAR, FRR, and execution time validate the suitability of the proposed framework to real face recognition applications in standard evaluation conditions. The cost of training a deep neural network from scratch was greatly reduced with the use of transfer learning. The proposed framework leverages the efficient inference capabilities of MobileNet as the feature extractor, while maintaining strong feature representations. Moreover, the encoding stage was designed using a lightweight XOR-based approach, which provided an extra layer of feature-level protection without compromising the recognition performance and complexity of the system. It shows that simple feature transformation tools can be used within a deep feature-based recognition system without compromising its efficiency and reliability in recognition. Due to the small variations of the adopted dataset, some degradation can be expected under extreme pose and/or lighting conditions, although the proposed framework showed stable performance for variations in face expression and

moderate lighting variations. These restrictions are typical in lightweight face recognition systems and offer potential for enhancement with increased databases and larger sample sizes. The present study did not assess the security features of the proposed XOR-based encoding mechanism due to the fact that it offers an extra layer of feature obfuscation with very little computation, but it may be compromised under sophisticated attacks like template inversion, reconstruction, brute-force, similarity leakage, or key compromise, so it is not a full-fledged cryptographic biometric template protection system, but rather a light-weight feature-level protection mechanism.

Future research will explore more powerful cryptographic template protection methods and full security analysis of such attacks. Furthermore, it is worth noting that the comparative result analysis presented in Table 2 is indirect, as the original experimental datasets, evaluation protocols, and evaluation environments used to evaluate the baseline methods are found in the respective papers. Thus, the comparison is qualitative and not intended as an experimental reference. To achieve a fully controlled comparison would involve application of all the baseline methods using the same ORL dataset and evaluation protocol, which would exceed the scope of the present study. However, the comparison shows that the proposed framework is competitive in recognition performance while maintaining low computational complexity and lightweight feature-level protection. The overall experimental results validate the efficacy of lightweight deep feature extraction and efficient encoding of the features for practical face recognition systems. The proposed framework provides a desirable tradeoff between recognition performance, computation efficiency, and lightweight feature protection for real-world applications where computation resources and computation time are important. Table 4 provides a qualitative comparison of representative face recognition approaches reported in the literature. Since these methods were evaluated using different datasets, experimental protocols, and evaluation settings, the comparison should not be interpreted as a direct experimental ranking.

Table 4. Qualitative comparison of representative face recognition approaches reported in the literature

| Ref.                    | Method                                              | Dataset       | Accuracy | Main Limitation                                 |
|-------------------------|-----------------------------------------------------|---------------|----------|-------------------------------------------------|
| Belhumeur et al. [14]   | LDA-Based Recognition (Fisherfaces)                 | Yale          | 87.4%    | Limited robustness in uncontrolled environments |
| Taigman et al. [16]     | DeepFace                                            | LFW           | 91.4%    | High computational complexity                   |
| Schroff et al. [17]     | FaceNet                                             | CASIA-WebFace | 94.1%    | Requires large-scale training data              |
| Guo et al. [21]         | CNN + SVM Hybrid                                    | Yale          | 93.2%    | Increased execution time                        |
| Samaria and Harter [22] | MobileNet-Based CNN                                 | ORL           | 92.3%    | Limited feature protection                      |
| Setyawan et al. [31]    | PCA-Based Recognition (Turk & Pentland, Eigenfaces) | ORL           | 85.2%    | Sensitive to illumination and pose variations   |
| Proposed Method         | CNN + XOR Encoding + SVM                            | ORL           | 95.6%    | Lightweight protection mechanism                |

Note: Linear Discriminant Analysis (LDA); Convolutional Neural Networks = CNNs; Support Vector Machine = SVM; Exclusive OR = XOR

5. CONCLUSIONS

This study proposed an innovative and efficient face recognition system using deep feature extraction and lightweight feature encoding. In this system, the MobileNet architecture was used to capture distinctive facial representations, with an XOR-based encoding system used to enhance the protection of the captured features. The experimental results obtained using the ORL (AT&T) dataset

demonstrated that the proposed system achieved competitive recognition performance while maintaining low computational complexity and lightweight feature-level protection. The qualitative comparison with representative studies reported in the literature indicates that the proposed framework provides an effective balance between recognition performance, computational efficiency, and feature-level protection, and reduced the FAR and FRR. The lower execution time of the system also indicates that this system

was applicable to practical and real-time face recognition tasks. The results also showed that when using lightweight deep learning architectures and simple protection systems, this system achieved an ideal recognition level, an efficient level of processing, and the proposed framework maintained lightweight feature-level protection while preserving recognition accuracy and computational efficiency. Future work may extend to testing the proposed system on larger and more complex face recognition systems that operate under less [optimal conditions. Research may also be extended to incorporate more complex encoding systems to increase the level of security and privacy of the biometric features. The reported methods were evaluated using different datasets and experimental protocols.

## REFERENCES

- [1] Ramadhan, S.B., Hareva, D.H. (2026). Enhancing facial expression recognition: Leveraging MobileNetV3 for periocular analysis. *Journal of Image and Graphics*, 14(1): 65-75. <https://doi.org/10.18178/joig.14.1.65-75>
- [2] Deng, J., Guo, J., Yang, J., Xue, N., Kotsia, I., Zafeiriou, S. (2022). ArcFace: Additive angular margin loss for deep face recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 44(10): 5962-5979. <https://doi.org/10.1109/tpami.2021.3087709>
- [3] de Santana Correia, A., Colombini, E.L. (2022). Attention, please! A survey of neural attention models in deep learning. *Artificial Intelligence Review*, 55(8): 6037-6124. <https://doi.org/10.1007/s10462-022-10148-x>
- [4] Otroshi Shahreza, H., Melzi, P., Osorio-Roig, D., et al. (2026). Benchmarking of cancelable biometrics for deep templates. *Journal on Image and Video Processing*, 2026(1): 4. <https://doi.org/10.1186/s13640-025-00679-y>
- [5] Li, J., Zhou, Y. (2025). BIDEepLab: An improved lightweight multi-scale feature fusion Deeplab algorithm for facial recognition on mobile devices. *Computer Simulation in Application*, 3(1): 57-65. <https://doi.org/10.18063/csa.v3i1.917>
- [6] Acheampong, E.M., Zhou, S., Liao, Y., Antwi-Boasiako, E., Obiri, I.A., Tawiah, A.G.B. (2026). CosPEEPChain: Blockchain-secured privacy-preserving face recognition using eigenface perturbation and CosFace. *Electronics*, 15(8): 1709. <https://doi.org/10.3390/electronics15081709>
- [7] Saeed, H.S., Hassan Fares, M. (2025). Enhancing surveillance with machine and deep learning-based facial recognition model: A proposed approach for identification. *Journal of Engineering and Sustainable Development*, 29(1): 127-135. <https://doi.org/10.31272/jeasd.2633>
- [8] Elian, H.M., Dousoky, G.M., Hafez, A. (2025). Developing deep learning-based facial recognition technique. *Journal of Advanced Engineering Trends*, 44(1): 214-220. <https://doi.org/10.21608/jaet.2024.322195.1344>
- [9] Zhang, P., Zhao, F., Liu, P., Li, M. (2022). Efficient lightweight attention network for face recognition. *IEEE Access*, 10: 31740-31750. <https://doi.org/10.1109/access.2022.3150862>
- [10] Ilashchuk, M. (2025). Face detection and identification using convolutional neural network and MobileNetV3 model. *Sensors, IoT and Software*, 3(2): 02009. <https://doi.org/10.31861/sisiot2025.2.02009>
- [11] Alansari, M., Hay, O.A., Javed, S., Shoufan, A., Zweiri, Y., Werghi, N. (2023). GhostFaceNets: Lightweight face recognition model from cheap operations. *IEEE Access*, 11: 35429-35446. <https://doi.org/10.1109/access.2023.3266068>
- [12] Zhang, P., Zhao, F., Liu, P., Li, M. (2022). Efficient lightweight attention network for face recognition. *IEEE Access*, 10: 31740-31750. <https://doi.org/10.1109/ACCESS.2022.3150862>
- [13] Imran, M.A., Miah, M.S.U., Rahman, H., Bhowmik, A., Karmaker, D. (2015). Face recognition using eigenfaces. *International Journal of Computer Applications*, 118(5): 12-16. <https://doi.org/10.5120/20740-3119>
- [14] Belhumeur, P.N., Hespanha, J.P., Kriegman, D.J. (1997). Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 19(7): 711-720. <https://doi.org/10.1109/34.598228>
- [15] Hu, G., Yang, Y., Yi, D., et al. (2015). When face recognition meets with deep learning: An evaluation of convolutional neural networks for face recognition. In 2015 IEEE International Conference on Computer Vision Workshop (ICCVW), Santiago, Chile, pp. 384-392. <https://doi.org/10.1109/iccvw.2015.58>
- [16] Taigman, Y., Yang, M., Ranzato, M., Wolf, L. (2014). DeepFace: Closing the gap to human-level performance in face verification. In 2014 IEEE Conference on Computer Vision and Pattern Recognition, Columbus, OH, USA, pp. 1701-1708. <https://doi.org/10.1109/cvpr.2014.220>
- [17] Schroff, F., Kalenichenko, D., Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. In 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, pp. 815-823. <https://doi.org/10.1109/cvpr.2015.7298682>
- [18] Howard, A.G., Zhu, M., Chen, B., et al. (2017). MobileNets: Efficient convolutional neural networks for mobile vision applications. *arXiv preprint arXiv:1704.04861*. <https://doi.org/10.48550/arXiv.1704.04861>
- [19] Chen, S., Liu, Y., Gao, X., Han, Z. (2018). MobileFaceNets: Efficient CNNs for accurate real-time face verification on mobile devices. In *Lecture Notes in Computer Science*, pp. 428-438. [https://doi.org/10.1007/978-3-319-97909-0\\_46](https://doi.org/10.1007/978-3-319-97909-0_46)
- [20] Huang, Y., Wu, Z., Chen, J., Xiang, H. (2024). Privacy-preserving face recognition method based on randomization and local feature learning. *Journal of Imaging*, 10(3): 59. <https://doi.org/10.3390/jimaging10030059>
- [21] Guo, S., Chen, S., Li, Y. (2016). Face recognition based on convolutional neural network and support vector machine. In 2016 IEEE International Conference on Information and Automation (ICIA), Ningbo, China, pp. 1787-1792. <https://doi.org/10.1109/ICInfA.2016.7832107>
- [22] Samaria, F.S., Harter, A.C. (1994). Parameterisation of a stochastic model for human face identification. In *Proceedings of 1994 IEEE Workshop on Applications of Computer Vision*, Sarasota, FL, USA, pp. 138-142. <https://doi.org/10.1109/acv.1994.341300>
- [23] Xiao, J., Jiang, G., Liu, H. (2022). A lightweight face

- recognition model based on MobileFaceNet for limited computation environment. *EAI Endorsed Transactions on Internet of Things*, 7(27): 1-9. <https://doi.org/10.4108/eai.28-2-2022.173547>
- [24] Khalifa, A., Abdelrahman, A.A., Hempel, T., Al-Hamadi, A. (2025). Towards efficient and robust face recognition through attention-integrated multi-level CNN. *Multimedia Tools and Applications*, 84(14): 12715-12737. <https://doi.org/10.1007/s11042-024-19521-0>
- [25] Martínez-Díaz, Y., Luevano, L.S., Méndez-Vázquez, H., Nicolás-Díaz, M., Chang, L., González-Mendoza, M. (2019). ShuffleFaceNet: A lightweight face architecture for efficient and highly-accurate face recognition. In 2019 IEEE/CVF International Conference on Computer Vision Workshop (ICCVW), Seoul, South Korea, pp. 2721-2728. <https://doi.org/10.1109/iccvw.2019.00333>
- [26] Fadlullah, S.Y., Hidayah, A.N., Saputra, Y.E., Uslan, Negara, S.P.P.S. (2026). SisCek: A deep learning-based face recognition system for real-time exam impersonation detection. *Jurnal Penelitian Sains Teknologi*, 2(2): 49-164. <https://doi.org/10.23917/saintek.v2i2.16998>
- [27] Li, F., Xu, Q., Bao, S., Han, B., Yang, Z., Huang, Q. (2025). Hybrid generative fusion for efficient and privacy-preserving face recognition dataset generation. In 2025 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW), Honolulu, HI, USA, pp. 506-512. <https://doi.org/10.1109/iccvw69036.2025.00057>
- [28] İbrahimoglu, N., Aytekin, M.C., Yıldız, F. (2025). Knowledge distillation from ResNet to MobileNet for accurate on-device face recognition. *AIPA's International Journal on Artificial Intelligence: Bridging Technology, Society and Policy*, 1(2): 1-15. <https://doi.org/10.5281/zenodo.15502091>
- [29] Deng, J., Guo, J., Zhang, D., Deng, Y., Lu, X., Shi, S. (2019). Lightweight face recognition challenge. In 2019 IEEE/CVF International Conference on Computer Vision Workshop (ICCVW), Seoul, South Korea, pp. 2638-2646. <https://doi.org/10.1109/ICCVW.2019.00322>
- [30] Setyawan, N., Sun, C.C., Hsu, M.H., Kuo, W.K., Hsieh, J.W. (2026). FaceLiVTv2: An improved hybrid architecture for efficient mobile face recognition. *IEEE Transactions on Biometrics, Behavior, and Identity Science*. <https://doi.org/10.1109/tbiom.2026.3690540>
- [31] Turk, M.A., Pentland, A. (1991). Face recognition using eigenfaces. In CVPR, Maui, Hawaii, USA, pp. 586-591. <https://www.cs.jhu.edu/~hager/teaching/cs461/mturk-CVPR91.pdf>
- [32] Duong, C.N., Quach, K.G., Jalata, I., Le, N., Luu, K. (2019). MobiFace: A lightweight deep learning face recognition on mobile devices. In 2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS), Tampa, FL, USA, pp. 1-6. <https://doi.org/10.1109/btas46853.2019.9185981>