SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V13I8P112
Volume 13 Issue 8, 196-211, August 2026

Original Article

AI-Driven Passwordless Authentication through MobileNetV2-Based Dynamic Password IrisCode Generation and Deep Iris Embedding Transformation

Swetha Margaret TA[1], Divya Midhunchakkaravarthy[2]

[1,2]*Faculty of Computer Science and Multimedia, Petaling Jaya , Lincoln University College, Malaysia.*

[1]*Corresponding Author : swetha.pdf@lincoln.edu.my*

Received: 15 June 2026 Revised: 08 August 2026 Accepted: 19 August 2026 Published: 31 August 2026

Abstract *- The widespread adoption of digital services, cloud infrastructure and smart access control has raised the demand for passwordless and secure authentication systems. The classic password-based authentication is susceptible to stolen credentials, phishing and replay attacks, leading to unauthorized access, whereas traditional iris authentication methods rely on fixed biometric templates with less flexibility and security. Here, proposing an AI-based passwordless authentication system using dynamic generation of Password IrisCode and iris embedding transformation. This framework utilizes a custom-designed Iris Acquisition Device with controlled lighting and a high-resolution capturing facility to secure a good-quality iris image. This captured data is then pre-processed and fed to the MobileNetV2 model to extract distinct iris features and generate compressed 128-dimension biometric features (iris embedding). Instead of traditional iris authentication using an iris feature vector, this extracted embedding is cryptographically hashed (using SHA-256) and converted to an encrypted Password IrisCode, thus securing the data while retaining the uniqueness. The proposed system authenticates the users by checking the similarity of generated iris features and the enrolled patterns. The framework is tested on a large dataset with variable illumination and acquisition conditions called CASIA-Iris-Thousand and has been able to achieve an accuracy of 95.0%, as against the accuracy of 67.09% of the IrisCode authentication system, and a failure rate has been reduced from 32.91% to 5.0%, and average processing time has been observed to be 0.4065sec for near real-time authentication. The AI-based feature extraction and the usage of dynamic Password IrisCode Generation, along with a dedicated hardware for iris acquisition, make the proposed system efficient, secure and scalable for modern passwordless access controls.*

Keywords *- Passwordless Authentication, Iris Recognition, MobileNetV2, Password IrisCode, Deep Learning, Biometric Security, Iris Embedding Transformation, SHA-256, Access Control, CASIA-Iris-Thousand.*

1. Introduction

Growing expansion of digital ecosystems, cloud services, financial and health services, and smart access control has boosted the requirements for strong and secure authentication systems. Authentication based on traditional passwords is still prevailing in various systems, however, it is exposed to password leakage, phishing attacks, credentials reuse, brute force attack and social engineering.

Due to rapid development in cyber-attacks, many organizations are attempting to use passwordless authentication with higher security and convenience to end users. Among various biometric methods which offer high security against authentication threats, iris recognition is the optimal method because the iris pattern of human being is unique and has long-term stability. With the advancements in deep learning, deep feature extraction from the iris image provides even more robust recognition.

Deep learning-based iris recognition has attracted considerable interest, and its successful application has been demonstrated in DeepIrisNet2 using learning deep iris representations for recognition under visible wavelength and Near-Infrared (NIR) imaging conditions [1]. Moreover, multimodal biometrics that combine iris and palm-print features has also achieved enhanced authentication performance with composite feature extraction and classification approaches [2]. The effects of iris normalization methods on deep learning-based recognition systems and the importance of preserving the discriminant iris information during the preprocessing are discussed in [3]. Recent works have been concerned with improving the separability of features and recognition performance using margin-based optimization strategies [4]. Lightweight convolutional neural network architectures with an attention mechanism have also been presented for efficient iris recognition with high classification accuracy [5]. With the wide usage of deep learning for biometric authentication, there have been many surveys about authentication approaches, databases, evaluation measures and future research problems for multiple biometric modalities [6].

Moreover, the best models after hyperparameter tuning have produced improved verification accuracy in biometric systems and highlighted the need for intelligent feature learning for secure authentication [7]. To handle concerns of privacy and template-security, transformation-based cancellable biometric frameworks have been developed, and this allows to safely generate a biometric template without losing all the biometric data compromise associated risks [8]. Nevertheless, numerous open problems are still not addressed. Typical iris recognition systems can work at two different levels: recognition and verification based on the acquisition of a static biometric template; authentication is sometimes performed with static feature representation, which is also vulnerable to template compromise or replay attack. Most previous work in iris recognition fails to take in consideration the iris acquisition hardware with a dedicated camera, the deep feature extraction, the dynamic biometric transformation and the password-less authentication simultaneously. Many existing systems of iris authentication lack dynamic credentials generated.

To tackle these drawbacks, this paper suggests a novel AI-based passwordless authentication framework relying on dynamic Password IrisCode generation and iris embedding transformation. The suggested framework comprises a specific iris acquisition device to capture a good quality image, a MobileNetV2 model to extract descriptive iris embeddings and cryptographic hashing to transform the embeddings to a set of dynamic Password IrisCodes, which adds a security layer but keeps the uniqueness property of the bio-metric. Authentication will be done by comparing the similarity between the transformed embeddings.

This study presents several experiments using CASIA-Iris-Thousand dataset and compared it with a classical or traditional authentication system relying on IrisCode. Experimental results confirmed that the proposed method provides better accuracy and security performance than the traditional approach (Daugman IrisCode-Based Authentication System) while meeting the real-time constraints. Combining hardware of acquisition (especially hardware dedicated to this process), the deep learning for feature extraction, generation of Password IrisCode on the fly and passwordless authentication forms a powerful framework of next-generation secure access control. The subsequent segments of this research broadside are organized as follows. In section 2, presenting related works and literature review. Section 3 talks about the problems, research gaps and motivation. Section 4 analyses the method proposed and the architecture of the system. Section 5 deals with experiments setup. Section 6 gives and discuss results of experiments and comparison. Section 7 concludes this research work and presents future work with prospects.

2. Related Works

Shende et al. [9] proposed a survey on various deep learning-based authentication schemes for smart devices and claimed that Convolution Neural Networks (CNNs) and deep architectures are more advantageous in improving authentication accuracy, robustness and security for multimodal biometrics. Built on the concepts proposed, Salturk and Kahraman [10] suggested a novel multimodal biometrics authentication using deep learning approaches in combining dynamic signature and facial recognition to gain enhanced security in online authentication and high authentication performance.

Due to the increasing trend of employing deep learning in iris recognition, research work has been carried out extensively to enhance iris recognition and classification. Nguyen et al. [11] carried out a comprehensive survey on the deep learning approaches for iris recognition. The paper described various aspects of the system, including datasets, segmentation methods, deep feature learning architectures and evaluation criteria. Similar work has also been presented by Yin et al. [12], which surveyed latest deep learning-based iris recognition, achieving significant recognition rate improvement through various sophisticated CNN architectures and optimal training processes. Furthermore, Sivasankari and Hanirex [13] presented a discussion on role of deep learning in iris recognition and classification and how it aids in extracting highly discriminative iris features to authenticate users.

Other than iris recognition itself, the use of biometrics has been extensively studied within the context of authentication. Mohammed et al. [14] proposed a multimodal biometric authentication scheme for access control over a network. It claimed that using multiple biometrics together greatly enhances the overall security and authentication rate. Dahan and Jaha [15] proposed a new quantum-inspired deep learning model for iris authentication, IRIS-QResNet, and showed that the model is good at feature representation for iris recognition, thereby achieves promising accuracy. In this context, Kadhim et al. [16] developed a synchronously spatiotemporal linear discriminant model for robust iris recognition. This model could resolve the problems of various acquired image qualities and boost recognition performance and stability. In addition to conventional iris recognition, distant iris recognition is also under consideration, and Rahman et al. [17] utilized distant iris recognition via deep feature transfer learning and machine learning methods to offer human identification through iris.

Recent studies also focus on making the authentication systems more robust through multiple learning techniques and application domains. Chethana and Ravi [18] proposed a deep segmentation-assisted residual spatio-textural ensemble feature learning framework for multimodal person authentication to enhance the authentication rate and feature extraction. To tackle this issue in the financial technology domain, Alangaram et al. [19] proposed an AI-powered and secure payment system based on iris-based eye recognition for wallet authentication. Additionally, Sheela and Radhika [20] presented a deep learning-based fusion framework of iris biometrics for multimodal authentication, highlighting the benefits of biometric fusion on reliability with the highest security levels maintained.

Although most works above aim at recognizing, classifying or fusing multiple biometric traits. Little focus has been placed on transforming biometric features into dynamic authentication credentials to empower password-less authentication systems. Moreover, few studies integrate dedicated iris acquisition hardware with deep embedding transformation and dynamically generating authentication tokens.

3. Research Gap and Motivation

The prevalent deep learning methods have been effectively used to enhance biometric authentication systems. Authentication frameworks built using deep learning techniques have shown to be highly secure and achieve accurate authentication on various biometrics modalities [9, 10]. Likewise, deep neural networks have remarkably enhanced iris feature extraction, recognition, and classification over traditional methods [11-13]. Moreover, intelligent access control and multimodal biometric systems have increased the security of authentication systems in various application environments [14-17]. Recent developments in multimodal person authentication, AI-based secure payment, and biometric fusion have greatly expanded the application domains of biometric systems [18-20].

Despite these improvements in biometric authentication, most of the systems utilize fixed biometric template for authentication and are mostly dedicated to biometric recognition and verification. These methods ensure accurate biometric recognition, but fail in the case of unauthorized template usage, replay attacks, template leakage. In these methods, authentication is considered as a classification problem, in which dynamic authentication credential is not generated directly using the biometric feature [11-20]. A second issue lies with integrating specialized iris acquisition hardware with intelligent authentication frameworks. Most research attention has been dedicated to software-based biometric recognition and multimodal biometric authentication models [15-20]. However, little research has explored a safe transformation of deep iris embeddings into dynamically generated authentication tokens suitable for password-less authentication.

Based on these challenges, this research presents an AI-based password-less authentication framework by integrating a dedicated iris acquisition device, mobileNetV2-based feature extraction, an iris embedding transformation, and a dynamic Password IrisCode generation.

The framework integrates deep learning, secure embedding transformation, and cryptographic hashing methods to dynamically authenticate a user by generating authentication tokens using iris biometrics, making it less vulnerable to replay attacks and a more secure choice for next-generation, scalable, password-less systems.

4. Proposed Methodology

The proposed AI-powered passwordless authentication framework intends to ensure reliable and secure user verification through dynamically generating the Password IrisCode and transforming the iris embedding. There are 5 broad phases of the system: Iris acquisition, Image pre-processing, Deep feature extraction, Password IrisCode generation, and authentication.

To begin with, Iris images are taken from using the proposed iris acquisition device with high resolution camera and a controllable illumination mechanism. This acquisition module allows acquisition of a consistent iris image and reduces the interference of ambient factors to the recognition performance. Then, collected iris images were processed with a pre-processing step for the purpose of enhancing image quality and preparing for feature extraction stage.

After pre-processing, Deep Learning framework MobileNetV2 was used for learning highly discriminative iris features. This architecture was selected based on its light weight, efficient computation, and high ability of feature learning. It can then represent input iris images in a compact embedding vector with a dimension size of 128, while maintaining the unique features of the Iris.

These extracted iris embeddings are then cryptographically hashed using the SHA-256 algorithm to derive secure and dynamic Password IrisCodes. This method prevents a static biometric template from being vulnerable to unauthorized use and compromise, in contrast to a typical iris authentication mechanism that enrols and compares against such a template.

In the verification phase, an incoming Iris embedding is compared against an enrolled embedding, and if the similarity score (based on cosine similarity) passes, then an authentication threshold will be verified.

A combined integrated system comprising of specialized iris acquisition hardware, mobile-based features extraction (MobileNetV2), iris embedding transformation, and Password IrisCode generation provides a passwordless authentication system that offers high security, scalability, and real-time verification.

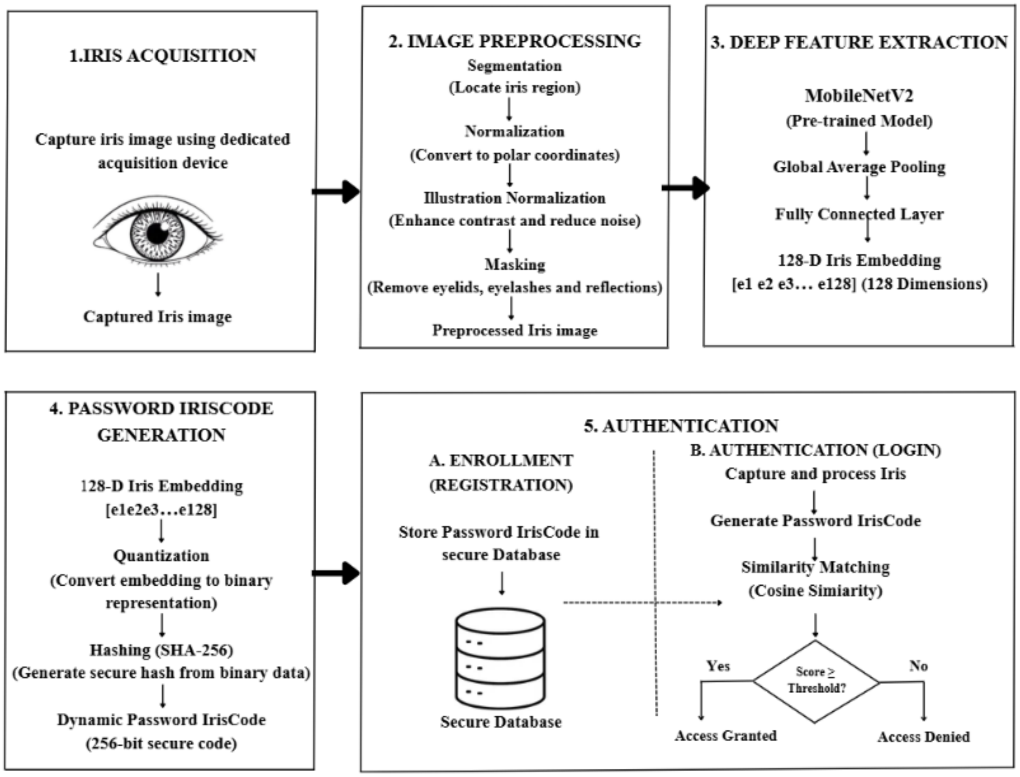

Fig. 1 Overall workflow of the proposed AI-driven passwordless authentication system

Figure 1 shows the system framework of the AI-powered passwordless authentication system. The proposed system first starts with acquiring the iris images, and using the developed iris acquisition device to get high-quality iris images. The obtained iris images are then pre-processed by a set of algorithms: segmentation, normalization, illumination correction and noise removal to improve the quality of the images, to effectively extract the iris area. After that, the pre-processed iris image data is fed into the MobileNetV2 for deep feature extraction to get iris embeddings of 128 dimensions, which are then quantized and cryptographically hashed with SHA-256 to achieve the unique dynamic.

Password IrisCode. The derived Password IrisCode is stored into the authentication database during enrolment, and compared to the enrolled iris pattern using cosine similarity-based matching in the authentication during login phase, to decide whether to accept or reject based on whether the similarity measure falls above or below a specified threshold. The combined unique iris acquisition hardware, deep feature extraction, dynamic password IrisCode and passwordlessauthentication mechanisms can ensure a reliable and safe next-generation access control system.

4.1. Iris Acquisition Device

The proposed authentication framework employs a dedicated iris acquisition device designed to capture high-quality iris images under controlled illumination conditions. The device (Figure 2) consists of a high-resolution camera module, integrated illumination ring, touchscreen interface, and embedded control unit for image acquisition and user interaction.

Fig. 2 Proposed Iris Acquisition Device - The hardware product is UK design patented in the year 2025

The illumination mechanism minimizes the impact of environmental lighting variations and improves iris visibility during image capture. The acquired iris images serve as the primary input to the authentication pipeline. By incorporating a dedicated acquisition device, the proposed framework ensures improved image consistency, reduced noise, and enhanced recognition reliability compared to conventional camera-based acquisition systems.

4.2. Iris Image Processing

Iris images, acquired at different times, first pass through a pre-processing step to refine the quality of the images and extract effective information for deep features extraction. Image quality enhancement involved segmented, normalized, illumination corrected and de-noised iris images. Image segmentation is used to separate the iris from the context of eyelids and eyelashes. Normalization compensates for scale and positional changes of the iris. Illumination normalization enhances the contrast and compensates for brightness and color.

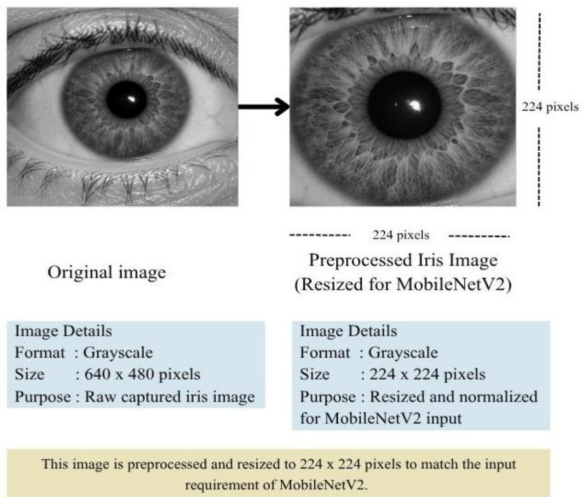

Fig. 3 Transformation of a raw iris image through the pre-processing stage prior to deep feature extraction

The pre-processed iris images serve as appropriate inputs to further processes of feature extraction and authentication. Figure 3 displays an example image from the CASIA-Iris-Thousand dataset along with its pre-processed version as an input to the MobileNetV2 network. In the pre-processing step, the input iris image is reduced to 224 X 224 pixels. This step is necessary to fit the input resolution requirement for the Deep Learning network. Resizing all the images to the same resolution makes the dimensions consistent and retains sufficient iris texture information necessary for learning features. This pre-processed image is then input to the MobileNetV2 architecture that learns discriminative iris features and converts them to a small embedding vector, which will then be converted to Password IrisCode for authentication.

4.3. MobileNetV2 - based Deep Feature Extraction

After the pre-processing procedure, iris images are fed into MobileNetV2 to extract features from them. The MobileNetV2 architecture is chosen over other deep learning models because it is a light-weight and fast network for generating discriminative features with a minimal number of trainable parameters. The lightness of the network allows real-time application of the system as well as use of the system in constrained computational environments. The 224 × 224 pre-processed iris images are then feed into the MobileNetV2 feature extraction network. This network utilizes depth-wise separable convolutions and inverted residual bottleneck layers that significantly reduce the number of computations without a loss in features representation capabilities. It differs from the typical iris recognition systems by its automatic learning of the iris features (hierarchical patterns) directly from the iris images rather than using the traditional handcrafted (Daugman IrisCode-Based Authentication System) iris texture descriptors. To extract useful and distinctive features, the last classification layers of the MobileNetV2 model is trained for classification of images are replaced with a Global Average Pooling layer followed by a fully connected dense layer, thus transforms extracted features maps into an IrisCode embedding of 128 dimensions. This 128-dim iris embedding represents individual characteristics from the iris image with a reduction in dimensions and computational redundancy and serves as a discriminative biometric feature for further Password IrisCode generation and authentication.

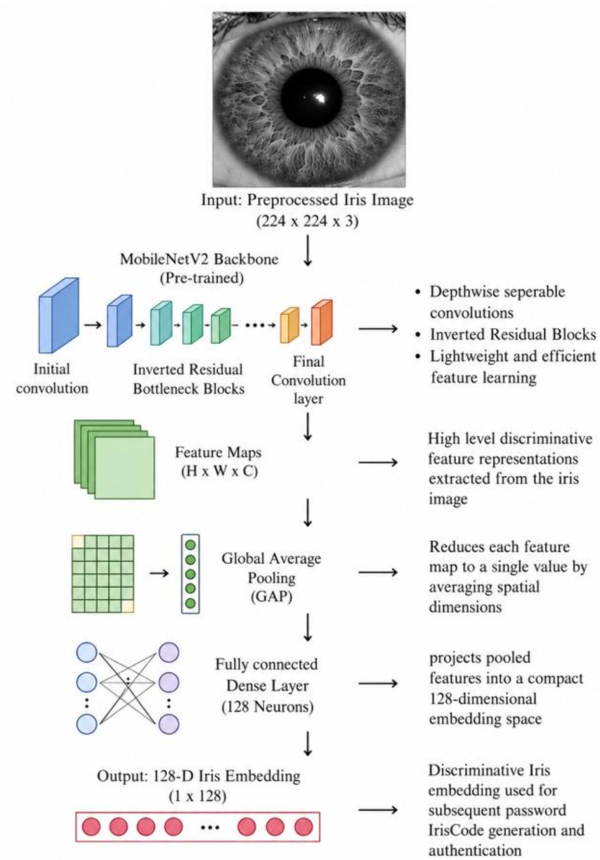

Fig. 4 MobileNetV2-based deep feature extraction framework for generating 128-dimensional iris embeddings

As Figure 4 shows, MobileNetV2 can transfer a pre-processed iris image to the small embedding representation by cascaded operations of convolution and feature pooling. The resultant 128-dimensional embedding can represent the discriminate features of iris and become the main biometrics for online Password IrisCode generation. The embedding can be efficiently stored, securely transferred and accurately authenticate; also reducing the computation comparing with old feature extraction methods.

4.4. Iris Embedding Transformation and Dynamic Password Iriscode Generation

The 128-dimensional iris embedding produced by the MobileNetV2 network is a concise biometric representation of the input iris image. While this embedding maintains the discriminatory characteristics of the iris, it is not suitable for storing as secure credentials and authentication. Therefore, an embedding transformation is executed on the obtained feature representation to convert it to a secured and dynamic Password IrisCode.

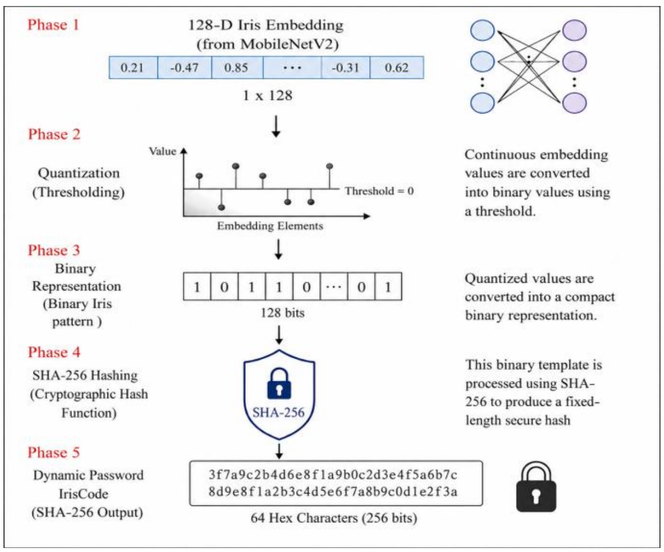

Fig. 5 Dynamic password IrisCode generation through iris embedding transformation and SHA-256 hashing

To begin with the transformation, the output embedding vector undergoes quantization where its continuous values features are mapped to binary format based on a threshold value. This transformation process converts the vector to a concise feature binary string, while still keeping the original features in a discriminative way.

This binary string is used as a biometric template that is ready for secured transformation. Next, the binary iris representation is processed through a SHA-256 cryptographic hashing algorithm.

This operation will result a fixed-length 256-bit security code that is solely generated based on the iris feature embedding. The resulting hash code is the Dynamic Password IrisCode, which will be used as authentication credentials instead of the raw biometrics.This protects user's biometric data compared to common iris systems that use stored static biometric pattern. The derived Password IrisCode will be used in both enrollment phase and authentication phase. The generated Password IrisCode is stored in the authentication database during the enrollment phase, whereas in the authentication phase, the Password IrisCode will be derived from query image, then be compared to find if the query image matches to the enrolled password code or not.

Figure 5 depicts the transformation procedure applied on the produced iris-embedding to produce secure Password IrisCode. The step of quantization translates the continuous values of the embedding in binary values, which then will be handled by SHA-256 hashing function. The obtained Password IrisCode becomes a fixed-length secure credential used in passwordless identification, and also the identity represented in the feature-space, of the iris, is preserved. This method adds security in the pattern.

4.5. Authentication and Access Decision

There are two main operative phases involved in the authentication phase, which is enrolment and verification. During enrolment, the iris image from the proposed iris acquisition system is acquired and processed through the MobileNetV2 feature extraction system. A 128-dimensional iris-embedding extracted is converted to Dynamic Password IrisCode through the proposed embedding transformation and SHA-256 hashing process.

The obtained Password IrisCode is stored in the authentication database along with its iris-embedding for future verification. During verification, the iris image from the user is captured again, and the same preprocessing, feature extraction and Password IrisCode generation are performed on the newly acquired iris image. Then, the newly obtained iris-embedding is compared with its corresponding enrolled iris-embedding by computing cosine similarity.

The cosine similarity calculation of two embedding vectors can be regarded as an effective means to measure similarity between biometrics with less computation. A fixed authentication threshold is set. If the similarity score of the matching is above the threshold, the user is regarded as a genuine one, and access is granted. On the contrary, if the similarity score is below the threshold, the attempt is rejected, and the access is denied.

Figure 6 shows the entire authentication process in the presented framework. Once enrollment is completed, the generated Password IrisCode and associated iris embedding are stored securely in the authentication database. At verification, the query iris image generates a new Password IrisCode that is then compared with the enrolled record by cosine similarity-based matching. The match score obtained then decides to grant or deny access based on the given threshold value, thus ensuring a secure and effective passwordless authentication.

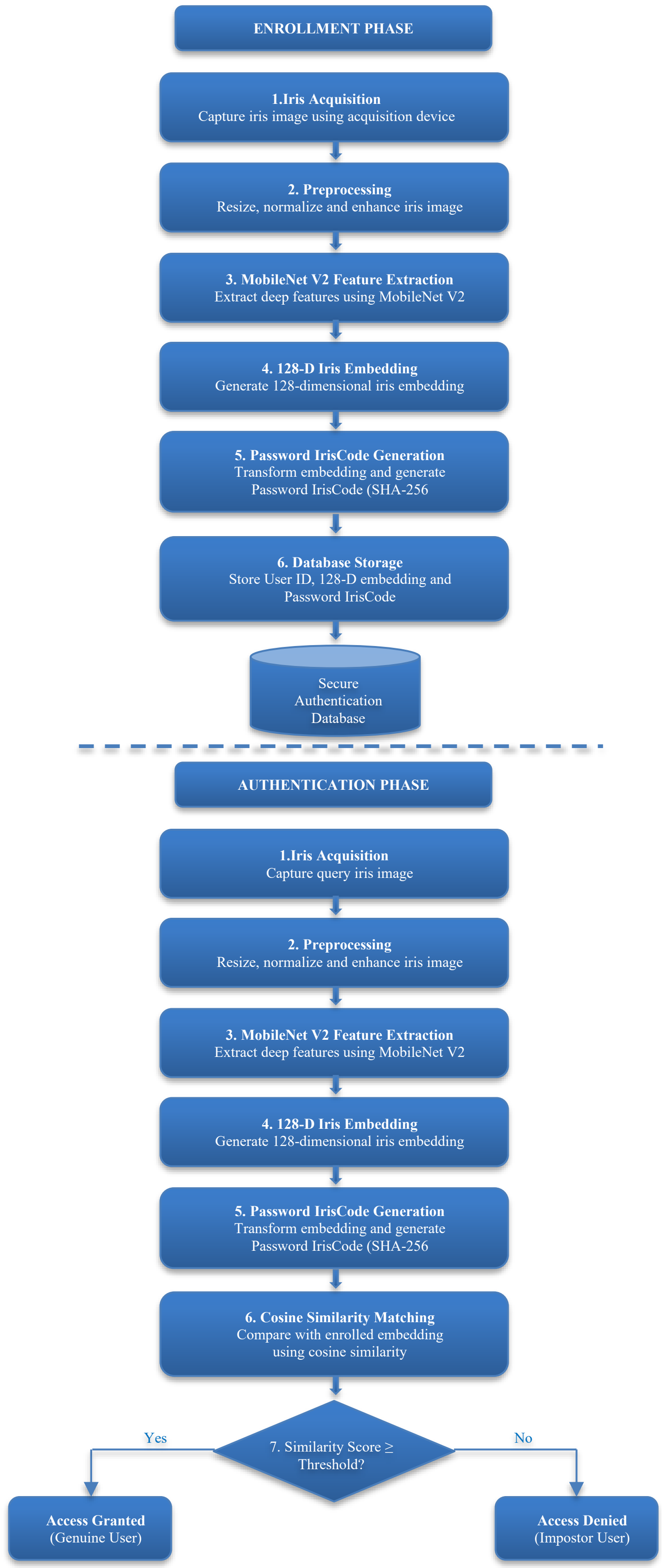

Fig. 6 Enrollment and authentication workflow of the proposed Password IrisCode-based access control framework

4.6. Analytical Formulation of The Proposed Framework for Authentication

The authentication mechanism proposed authenticates an individual by converting an input iris image into a secure Password IrisCode and thereafter performing an identity authentication. The analytical formula for the proposed framework is dependent on the four main phases, which include Iris Embedding Generation, Iris Embedding Quantization, Password IrisCode generation and authentication through cosine similarity.

To begin with, the input of the preprocessed iris image into the MobileNetV2 feature extraction network generates a 128-dimensional iris embedding, which is a compact biometric template useful in describing the texture variations of an iris of a human being. Through threshold-based quantization, the produced iris embedding can be converted into a binary iris template, which can then be securely used to represent the iris with limited space complexity.

The binary iris template can then be passed through a cryptographic hashing function of the type SHA-256 to yield a Dynamic Password IrisCode. This ensures that the direct biometric information from the template will not be exposed, and a non-reversible security credential is obtained during the authentication process.

During authentication, a given query iris image can pass through the same system processes to yield the query embedding and Password IrisCode. Through the cosine similarity function, a similarity score can be obtained between the query embedding and the enrolled embedding. High values of similarity score imply that both query and enrolled iris images match with high accuracy.

Finally, a given threshold can be used to verify and grant or reject access. Thus, the analytic formula for the whole authentication process can be established for the framework proposed for a passwordless authentication through Password IrisCode.

MobileNetV2 Embedding Generation
After feature extraction:

$$E = F(I)$$

Where:

I = Pre-processed iris image
F(.)= MobileNetV2 feature extraction function
E = 128-dimensional iris embedding

The MobileNetV2 network converts the pre-processed iris image I into the condensed feature vector E, which represents the biometric pattern for the identification.
The algorithm is given in Algorithm 1.

Embedding Quantization
Before Password IrisCode generation:

$$B_i = \begin{cases} 1, & E_i \geq T \\ 0, & E_i < T \end{cases}$$

Where:

- E_i= ith embedding element
- T= threshold value
- B_i= binary representation

Password IrisCode Generation

Using SHA-256: PIC = SHA256(B)

Where:

- B = Binary iris template
- PIC = Password IrisCode

Quantized Iris pattern is converted to a secure Password IrisCode by the cryptographic hash function SHA-256.

Cosine Similarity Matching

$$Similarity(E_q, E_r) = \frac{E_q \cdot E_r}{\parallel E_q \parallel \ \parallel E_r \parallel}$$

Where:

- E_q= Query iris embedding
- E_r= Registered iris embedding

Authentication Decision Rule

$$Access = \{Granted, Similarity \geq \tau \\ Denied, Similarity < \tau\}$$

Where:

- τ = Authentication threshold

The above analytical formulation explains the functional mechanism of the presented Password IrisCode-based authentication system in the form of mathematical representations.

Starting from MobileNetV2-based iris embedding generation to transforming biometric templates to secured binary values and then generating Dynamic Password IrisCode using SHA-256 hashing, the system verifies the query through cosine similarity-based matching of the registered and the query templates to confirm the true identity.

Through deep feature extraction, secured credential generation and similarity-based matching, a secure and well-recognized password-less authentication system has been developed. Performance validation has been carried out by experiment with the help of CASIA-Iris-Thousand database in the following section.

Algorithm 1: Dynamic Password IrisCode Generation and Authentication

Input : Preprocessed iris image I
Output : Dynamic Password IrisCode PIC (256-bit / 64 hex characters)

```
Start
  // Phase 1: 128-D Iris Embedding Generation
  E ← MobileNetV2(I)                                  // E is a 1 × 128 embedding vector
  // Phase 2: Quantization (Thresholding)
  Input: Embedding vector E = [E_1, E_2, ..., E_128], threshold T
  B ← empty binary vector of length 128               // Binary iris template
  for i ← 1 to 128 do
      if E_i ≥ T then
          B_i ← 1
      else
          B_i ← 0
      end if
  end for
  // Phase 3: Binary Representation
  B = [B_1, B_2, ..., B_128]   // 128-bit binary iris representation
  // Phase 4: SHA-256 Hashing
  PIC ← SHA256(B)                                     // PIC is 256-bit hash
  // Phase 5: Dynamic Password IrisCode (Output)
  PIC_hex ← Convert PIC to 64 hexadecimal characters
  return PIC_hex                                      // Dynamic Password IrisCode
----------------------------------------------------------------------------
                       AUTHENTICATION PROCEDURE
  Input: Query iris image I_q, Stored PIC (PIC_stored)
  Generate embedding: E_q ← MobileNetV2(I_q)
  Quantize: B_q ← Quantize(E_q, T)
  Generate query code: PIC_q ← SHA256(B_q)
  Compare: s ← Similarity(PIC_q, PIC_stored)
  if s ≥ τ then                                       // τ is decision threshold
      Access Granted
  else
      Access Denied
  end if
End
```

Notation:
- I : Preprocessed iris image
- E : 128-D iris embedding
- T : Quantization threshold
- B : 128-bit binary iris template
- PIC : Dynamic Password IrisCode (256-bit)
- τ : Authentication threshold

5. Experimental Setup and Implementation

The proposed Password IrisCode authentication system uses MobileNetV2 as a backbone deep feature extractor network. Transfer learning was utilized from the well-trained pre-trained MobileNetV2 network by removing the top classification layers and adding a Global Average Pooling and a 128-neuron fully connected layer for feature embedding generation.

Pre-processed iris images with a size of 224x224x3 were fed to the input. To have the quick convergence, Adam optimizer was chosen for training, and the loss function used was categorical cross-entropy. The dataset was divided into a ratio of 80:20 for performing effective evaluation of the trained model. In the training process, the network tunes its parameters iteratively so that the classification loss gets reduced and the discriminative ability for distinguishing between different iris classes get increased. During the training process, accuracy and loss metrics were used to identify whether the model is converging or not. The resulting 128-dimensional iris embeddings obtained from trained MobileNetV2 were then used for dynamic Password IrisCode generation and authentication. By training the network, a highly discriminative representation for iris was learned.

5.1. Dataset Description

The proposed Password IrisCode-based authentication framework was tested against the CASIA-Iris-Thousand dataset. The dataset consists of iris images of many different subjects recorded under stable illumination and varying imaging conditions. Such variations provide good discriminative features, such as wide difference in the texture patterns of the irises, differences in illuminations, and differences in the imaging angles for a biometric authentication system to use. All the iris images were scaled to size 224×224 pixels, prior to the training phase, so that they fit the input requirements for the MobileNetV2 architecture.

5.2. Data Preparation

Pre-processing was performed on each of the captured iris images (resizing, normalization, enhancing). Each processed sample of iris image dataset was then split into 80-20 ratio of training and testing to measure learning ability and generalization of proposed framework.

5.3. Implementation Environment

The proposed framework was developed and evaluated using the Anaconda software environment. This study uses libraries such as TensorFlow and Keras for developing the deep learning models, and also OpenCV, NumPy, Pandas, Matplotlib, and Scikit-learn for performing image processing, feature analysis, visualization and evaluation of our performance. The experimental setup in this environment helped us in easy model training, testing and Password IrisCode generation.

5.4. Configuration of MobileNetV2

MobileNetV2 architecture was chosen for backbone feature extraction network since it is efficient and lightweight. The architecture took an input size of 224 × 224 × 3 for its input images and extracted discriminative features with the use of depth-wise separable convolutions and inverted residual bottleneck blocks.

In order to use it for iris authentication have replaced the default classification layers of the model with a Global Average Pooling layer followed by a dense layer with 128 neurons that extracted compressed iris embeddings that are used to generate the Password IrisCodes.

5.5. Generation of Password IrisCode

The 128-bit iris embeddings were extracted from the network, and then they were quantized to convert the vector to a binary template, which was then fed to the cryptographic hashing algorithm (SHA-256) to generate a dynamic Password IrisCode which can serve as non-reversible, securely encrypted form of the authentication information.

5.6. Evaluation Measures

This study is evaluated by the proposed model based on the following measures, such as accuracy, success rate, failure rate, loss, processing time and cosine similarity score. (Table 1).

Accuracy indicates the percentage of correctly matched data. Success and failure rates represent the reliability of authentication. Processing time indicates the efficiency, and cosine similarity score indicates the matching rate.

Table 1. Experimental configuration

Parameter	Configuration
Dataset	CASIA-Iris-Thousand
Number of Subjects	20
Image Resolution	224 × 224 × 3
Feature Extractor	MobileNetV2
Embedding Layer Size	128 Dimensions
Authentication Representation	AI IrisCode Embedding
Password Generation Method	SHA-256 Hashing of Iris Embedding
Classification Layer	Dense + Softmax
Optimizer	Adam
Loss Function	Categorical Cross-Entropy
Batch Size	16
Evaluation Metrics	Accuracy, Precision, Recall, F1-Score, FAR, FRR, EER, AUC
Programming Language	Python 3.x
Deep Learning Framework	TensorFlow / Keras

5.7. Performance Evaluation Metrics

The proposed Password IrisCode authentication framework was evaluated on the basis of various parameters to check for performance regarding authentication effectiveness, computational cost, and model learning ability.

Authentication Accuracy, the percentage of authentication attempts correctly classified was computed. The reliability of user verification was calculated by computing Success rate and Failure rate, which represent the percentage of successful and unsuccessful authentication attempts, respectively. The learning ability of the MobileNetV2 model was measured by using training loss, which tells how much the predictions differ from the truth while optimizing. The less loss, the better the convergence and feature learning ability of the model. Processing time was used to check the average time needed to finish one authentication cycle, including feature extraction, Password IrisCode generation and authentication. Additionally, Cosine similarity was used as the matching function for comparing the enrolled and the probe iris embeddings. It returns how much similar the two biometric features are. All these measures give an indication about the accuracy of recognition, computational efficiency, security of system and accuracy.

Where:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \times 100$$

- TP = True Positives

- TN = True Negatives
- FP = False Positives
- FN = False Negatives

$$Success\ Rate = \frac{Successful\ Authentications}{Total\ Authentication\ Attempts} \times 100$$

$$Failure\ Rate = \frac{Failed\ Authentication\ Attempts}{Total\ Authentication\ Attempts} \times 100$$

6. Results and Discussions

To evaluate the feasibility of the presented Password IrisCode-based framework for secure biometric authentication, we have performed an experiment on CASIA-Iris-Thousand dataset.

Based on the obtained experimental results, it can be found that the presented framework with MobileNetV2 could successfully obtain the discriminative iris embeddings, secure Password IrisCodes, authenticate efficiently and accurately. The detailed outcomes are analyzed for training efficiency, authentication accuracy, comparison with IrisCode.

6.1. MobileNetV2 Training Performance

The learning performance of the presented MobileNetV2 model was examined by looking at the train and validation accuracy as well as the loss. The model shows the change in train accuracy with the increase of number of epochs.

The training accuracy was increased from roughly 17% in first epoch to nearly 99% in last epoch, showing that it learned the iris features discriminatively. Similarly, validation accuracy has increased quickly and become quite stable from the middle of training, as 93%, indicating it generalizes well on the testing set.

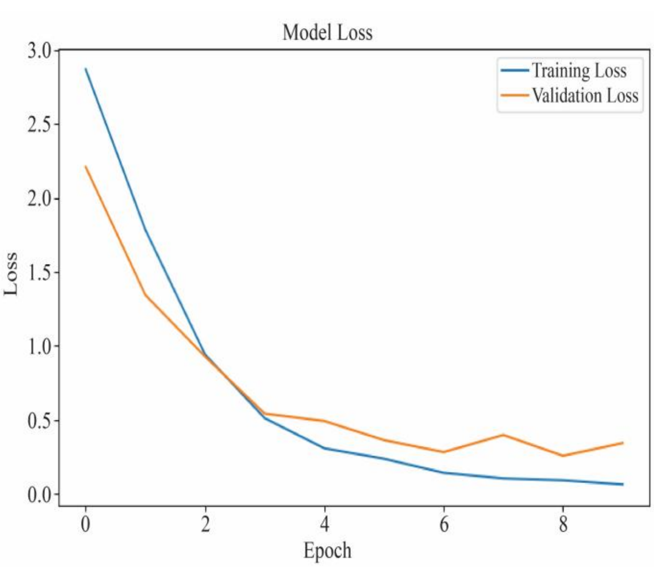

Fig. 7 Training and validation accuracy of the proposed mobilenetv2-Based Password IrisCode Authentication Framework

Figure:7 displays the training and validation accuracy obtained by the proposed MobileNetV2-based authentication framework throughout the learning phase. It is observed that the training accuracy increased gradually from ~16% in the first epoch to 99% in the last epoch, which suggests the successful learning of discriminative iris features by the model.

The validation accuracy increased gradually from 45% in the first epoch to >90% in the last epoch. Both curves increase and keep close to each other, which means the learning process is stable and not overfitting. It is converged well, which confirms that MobileNetV2 has captured the characteristic features of irises, generating highly distinctive feature embeddings for DP-IC generation and passwordless authentication.

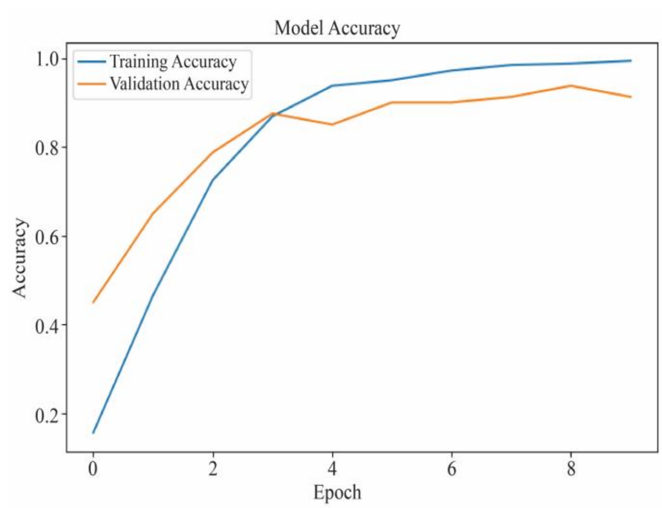

Fig. 8 Training and validation loss curves of the proposed MobileNetV2-based password IrisCode authentication framework

Figure 8 The training and validation loss curves from the learning procedure of our proposed MobileNetV2 are depicted in Figure. 8. Training loss drops drastically from nearly 2.9 to 0.1 during epoch 1 to the end, respectively. Validation loss is also largely decreased from approximately 2.2 to near 0.3, and demonstrates its better prediction ability for unseen iris samples.

In spite of a bit fluctuate on latter epochs, the overall decreasing trends show the convergence stability and parameter optimized well. The drop on both training and validation loss shows our model effectively learning the discrimination of iris and is capable of maintaining a good generalization ability. Thus, MobileNetV2 is effective for learning iris representation.

6.2. Authentication Performance Evaluation

To evaluate the efficiency, reliability and security of the biometric authentication system, it’s important to do an evaluation on the performance of the authentication (Table 2).

Table 2. Authentication performance metrics of the proposed mobilenetV2

S. No	Metric	Value
1	Dataset	CASIA-Iris-Thousand
2	Model	MobileNetV2
3	Accuracy (%)	95.0
4	Success Rate (%)	95.0
5	Failure Rate (%)	5.0
6	Loss	0.2123
7	Embedding Size	128
8	Password Length	64 Hex Characters
9	Average Processing Time (s)	0.4065
10	Feature Extraction	MobileNetV2
11	Password IrisCode	SHA-256 Generated
12	Security Level	High

The main objective is to find out how the proposed framework can differentiate a legitimate user from imposters. Evaluation also includes the computing capability, feature representation power, credential creation and the security of the authentication in general. Through this evaluation, it will be able to have a clear view on how well the framework works. Table 2 shows the authentication performance for the proposed MobileNetV2-based Password IrisCode authentication framework. These were the authentication performance resulted for MobileNetV2 based Password IrisCode authentication framework experimented on the CASIA-Iris-Thousand data set.

The authentication accuracy was measured at 95.0%, this clearly shows that the system is very good at recognizing valid users and preventing intruders' access. And the authentication success rate was measured at 95.0%, failure rate at 5.0%, again validating its high authentication reliability. The deep features extracted by the MobileNetV2 were discriminating and effective enough for Iris identification. The system generates small 128-bit size Iris embeddings from the mobile net, and these iris features were then used with a SHA-256 crypto hashing function to generate the secure Password IrisCode. The generated password IrisCode was of a fixed size 64-bit hexadecimal password. The authentication performed well with high biometric template protection and reduced the possibility of template recovery. The final loss was recorded at 0.2123, indicating proper convergence and feature learning on the network. The average time of authentication was 0.4065 s, showing it's a practical authentication technique.

6.3. Classification and Recognition Analysis

To continue the evaluation of the proposed MobileNetV2-based Password IrisCode authentication system, the additional classification and recognition measures are examined.

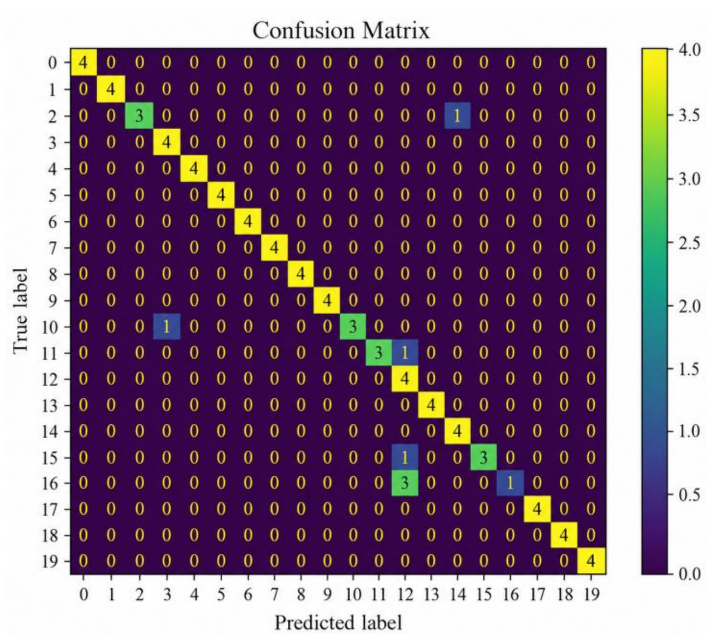

Fig. 9 Confusion matrix of the proposed mobilenetv2-based authentication framework

These allow for a better estimation of how well the model can correctly classify iris identities and how strong the system is when confronted with varied authentication scenarios. The examination includes the use of the confusion matrix evaluation, receiver operating characteristic analysis, area under the curve and the equal error rate analysis.

In Figure 9 depicts the confusion matrix for the authentication framework is generated. It is certain to notice that most of the samples are gathered along the main diagonal. It corresponds to the number of iris identities which have been correctly classified. A few entries, which are in off-diagonal cells, correspond to the misclassified samples. Majority of entries in the diagonal confirms that the extracted MobileNetV2 embeddings represent the iris features discriminatively. The research work has been able to correctly differentiate between the different users with minimum misclassification. Therefore, the total authentication accuracy obtained is 95.0%.

Although a higher rate of authentication accuracy will certainly imply better performance of the biometric system as a whole, in order to evaluate a biometric authentication framework comprehensively, analysis on the performance on classification and recognition is necessary. It is also vital that a biometric system could differentiate genuine users from an impostor; otherwise, a conflict between security and usability would always exist. Thus, sophisticated performance measures, Receiver Operating Characteristic (ROC), False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER), are studied in order to evaluate the performance of the proposed Password IrisCode based authentication framework using MobileNetV2.

Figure 10 (a-c) displays the authentication performance test of the proposed MobileNetV2 based Password IrisCode. Results using ROC curve, FAR-FRR, and EER graphs are shown in the figure. The ROC curve shows an AUC value of 0.9775. Such AUC means that the discriminability of legitimate and impostor authentication can achieve a great performance. Furthermore, the FAR-FRR shows a good compromise between security and usability for the authentication, whereas the EER is very low, which reflects the strong stability of the threshold for the authentication. These experiments justify that the deep features extracted using MobileNetV2, combined with the generation of Dynamic Password IrisCode by SHA-256 is effective. Unlike the traditional methods (Daugman IrisCode-Based Authentication System) of hand-crafted matching of IrisCode feature, the proposed system learns the iris image's discriminative features and transform it into the password for authentication. The AUC obtained can reflect high distinctiveness of the biometric features, while the other error curves demonstrate good error rate and security performance.

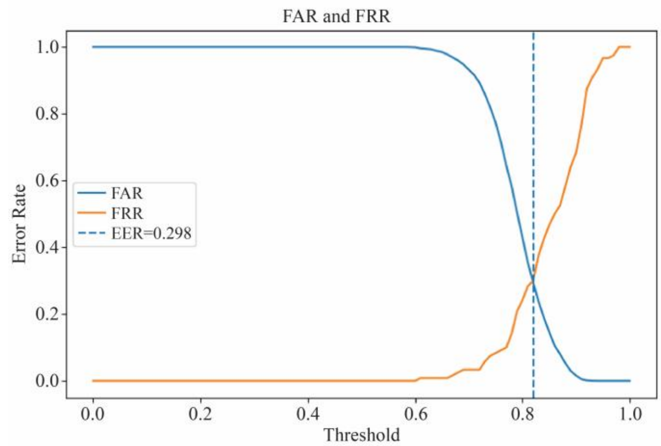

Fig. 10 (a) FAR–FRR of the authentication framework.

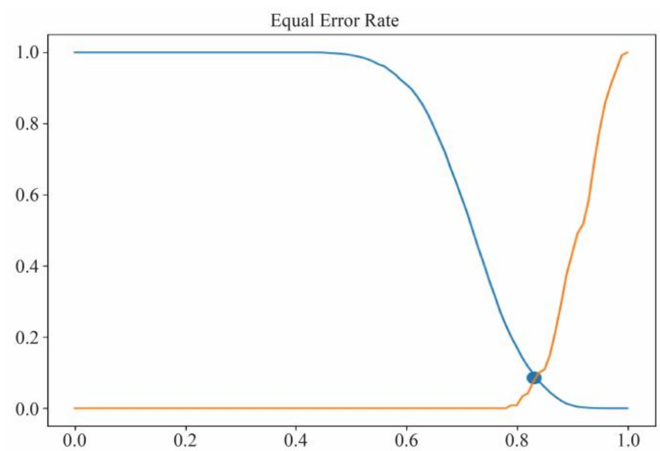

Fig. 10 (b) Equal Error Rate (EER) of the authentication framework.

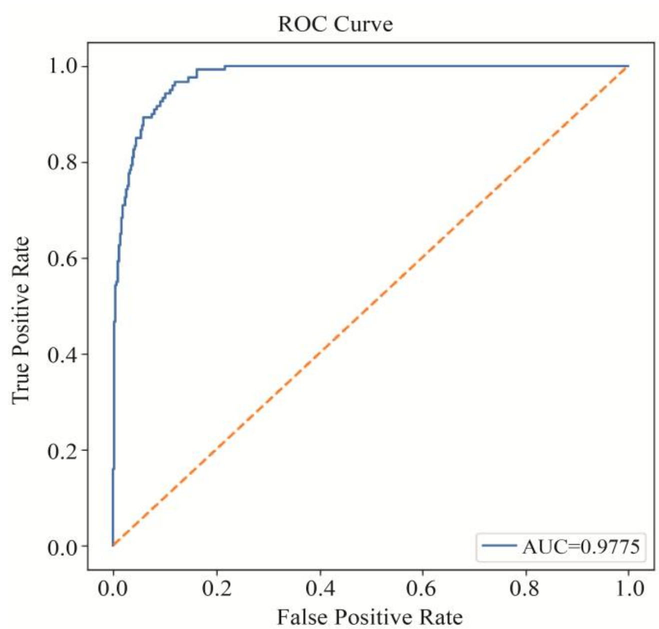

Fig. 10 (c) ROC analysis of the proposed authentication framework.

Therefore, the experiments prove the proposed framework can perform accurate, secure and reliable passwordless authentication and better pattern protection when compared to traditional Iris based systems (Daugman IrisCode-Based Authentication System).

6.4. Comparative analysis with the CONVENTIONAL DAUGMAN IRISCODE Framework

In order to examine the validity of the proposed system, a comparison analysis was conducted with standard Daugman IrisCode authentication. Standard framework uses hand-engineered features, and matching is done using Hamming distance, whereas proposed method uses MobileNetV2 to achieve deep feature learning, uses SHA-256 for creating the Dynamic Password IrisCode. Authentication accuracy, Feature representation power, computational efficiency, Security and Credentials generation features were used for comparison. Further, the presented framework produces a small 128-dimensional embedding, which is transformed into protected Password IrisCodes with SHA-256. A new secure, non-invertible credential generation technique is introduced, unlike current biometric system which stores permanent static template. The framework provides greater protection to the template and facilitate a passwordless authentication. It leads to moderately increased processing time for deep feature extraction and hashing, but authentication accuracy, security and protection of the credential are of greater importance than processing time increase. Table 3 shows a comparison in terms of performance metrics between the traditional Daugman IrisCode authentication achieves an authentication accuracy of 67.09%, whereas the proposed framework obtains an authentication accuracy of 95.00%. Thus, the recognition performance shows a large improvement, the main reason of which is that the MobileNetV2 can effectively learn discriminating iris features directly from the image without relying on hand-crafted feature extractors.

The proposed framework outputs short 128-dimensional embeddings and converts these embeddings into the Password IrisCode with SHA-256 hashing. This is in contrast to the traditional method, where the biometric templates are stored directly as is, thus adding a safe and non-reversible way to generate the credential, which adds up to template protection and a possible passwordless authentication scheme. Though the average processing time is a bit higher due to deep feature extraction and hashing process, it can be outweighed by the advantages in terms of authentication accuracy, security and template protection.

6.5. Password IrisCode Generation and Security Analysis

The unique aspect of the proposed system is the utilization of the extracted deep iris embeddings to generate Dynamic Password IrisCodes. The conventional iris systems store the biometric templates for matching, while the proposed system translates these biometric templates into safe authentication credentials and also allows for passwordless authentication. The framework performs the extraction of iris features to generate secure authentication credentials through the embedding, quantization, and SHA-256 cryptographical hashing. The 128-bit iris embedding extracted from the MobileNetV2 network will consist of the salient feature information present in the iris template of the individual.

Table 3. Comparative analysis between the conventional daugman iriscode framework and the proposed MobileNetV2-based password iriscode framework

S.N	Metric	Daugman IrisCode Method	Proposed MobileNetV2
1	Dataset	CASIA-Iris-Thousand	CASIA-Iris-Thousand
2	Model	Traditional IrisCode	MobileNetV2
3	Learning Mechanism	Rule-Based	Deep Learning
4	Accuracy (%)	67.09	95.0
5	Success Rate (%)	67.09	95.0
6	Failure Rate (%)	32.91	5.0
7	Loss / Optimization Metric	Deterministic Feature Matching	0.2123
8	Template Length	256-bit IrisCode	128-D Embedding
9	Generated Credential	IrisCode Template	64 Hex Character Password IrisCode
10	Average Processing Time (s)	0.00088	0.4065
11	Feature Extraction	Handcrafted Iris Features	MobileNetV2 Deep Features
12	Authentication Method	Cosine Similarity Matching	SHA-256 + Cosine Similarity
13	Security Level	Medium	High

The extracted 128-bit iris embedding is then quantized to obtain the binary code, and then the SHA-256 cryptographical hashing is performed to achieve a fixed 64-hexadecimal character long Password IrisCode. It is computationally unfeasible to re-obtain the original iris template from the Password IrisCode, as the SHA-256 is a one-way function. During the enrollment and verification phase, the generated Password IrisCode will be stored as an authentication credential. If the stored credentials are stolen, the original iris template would remain uncompromised as the credentials can neither be reversed back into iris template, thus minimizing the theft of biometric template, credential duplication and unauthorized usage of biometric credentials.

Table 4. Security comparison between the conventional daugman IrisCode framework and the proposed password IrisCode authentication framework

Security Feature	Conventional Daugman IrisCode	Proposed Password IrisCode
Template Storage	Static Iris Template	SHA-256 Protected Credential
Reversibility	Possible Template Exposure	Non-Reversible
Deep Feature Learning	No	Yes
Password Generation	Not Supported	Supported
Template Protection	Limited	High
Passwordless Authentication	No	Yes

The comparison results in Table 4 verify the benefits of the proposed MobileNetV2-based Password IrisCode authentication framework over the Daugman IrisCode one. Its integration of deep feature learning helps the framework to adapt to strong, discriminative iris patterns and leads to an authentication accuracy enhancement from 67.09% to 95.00%. Moreover, the proposed system performs the Dynamic Password IrisCode generation by hashing with SHA-256, which offers secure protection for template data. Passwordless authentication is facilitated. While it has a slightly increased calculation process time for deep learning and cryptography algorithms, the improvements achieved in terms of recognition accuracy, credential security and biometric template security can overcome it.

7. Conclusion and Future Work

In the era of increasing dependency on digital services and secure access control systems, accurate authentication systems are being constantly demanded that also protects users' privacy and biometric template. Among all biometric modalities, iris recognition is one of the most reliable biometrics; however, the traditional iris authentication systems were using hand-crafted feature extraction techniques and static biometric templates that might lower the recognition performance and make the biometric templates prone to various security threats. The issues addressed have driven us to devise a novel authentication framework which is secure, intelligent, and privacy-preserving.

This research finding proposed a MobileNetV2-based Password IrisCode authentication framework that combine the use of deep feature learning with cryptograph credentials to allow secure and passwordless authentication.

The system utilizes MobileNetV2 to generate highly discriminating iris features in the form of 128-dimensional iris embeddings from the preprocessed iris images and then transform it to the Dynamic Password IrisCodes by performing quantization and SHA-256 hashing. The proposed method uses deep feature extraction coupled with cryptographic protection to boost both authentication performance and template security.

The framework has been implemented and evaluated on CASIA-Iris-Thousand dataset, the experimental results showed promising authentication accuracy and performance in the security domain. The implemented system achieved an authentication accuracy of 95.0%, an authentication success rate of 95.0%, and AUC of 0.9775, final loss of 0.2123, respectively, which indicates good security performance for biometric authentication. While generating the Password IrisCodes that could secure the biometric templates without revealing them directly, and still support efficient passwordless authentication.

In conclusion, all these achievements show that the presented framework has addressed the accuracy issues, template security issues and authentication security issues properly. The combination of MobileNetV2-based deep feature extraction and the Dynamic Password IrisCode generation presents a useful, extendable and feasible approach for the contemporary access control system.

Future work could incorporate multimodal biometrics traits, such as Iris and face recognition, in the system for higher accuracy. Additional research will focus on the optimization on the framework by exploring the edge implementation architecture, and adaptive authentication threshold, federated learning, or blockchain-enabled credentials management.

Conflicts of Interest

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

Funding Statement

Not Applicable

References

[1] Abhishek Gangwar et al., "DeepIrisNet2: Learning Deep-IrisCodes from Scratch for Segmentation-Robust Visible Wavelength and Near Infrared Iris Recognition," *arXiv preprint*, pp. 1-10, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[2] A. Alsubari et al., "Composite Feature Extraction and Classification for Fusion of Palm-Print and Iris Biometric Traits," *Engineering, Technology & Applied Science Research*, vol. 9, no. 1, pp. 3807-3813, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[3] Dingding Jia, and Wenzhong Shen, "Is Normalized Iris Optimal for Iris Recognition Based on Deep Learning?," *Journal of Electronic Imaging*, vol. 30, no. 5, pp. 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Reihan Alinia Lat et al., "Boosting Iris Recognition by Margin-Based Loss Functions," *Algorithms*, vol. 15, no. 4, pp. 1-13, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Qinhong Zou et al., "Toward More Efficient Iris Recognition Using a Lightweight CNN Framework with Attention Mechanism," *Proceedings of the International Conference on Computer Network Security and Software Engineering (CNSSE 2022)*, vol. 12290, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Mohammad Yamin et al., "Biometric Verification System Using Hyperparameter Tuned Deep Learning Model," *Computer Systems Science and Engineering*, vol. 46, no. 1, pp. 321-336, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Lijun Zhou et al., "Iris Recognition Based on Convolutional Neural Network and Active Iterative Optimization," *2023 International Conference on Advances in Electrical Engineering and Computer Applications (AEECA)*, Dalian, China, pp. 523-528, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Dongdong Zhao et al., "Cancelable Iris Biometrics Based on Transformation Network," *2023 IEEE 23rd International Conference on Software Quality, Reliability, and Security (QRS)*, Chiang Mai, Thailand, pp. 507-516, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Shailendra W. Shende, Jitendra V. Tembhurne, and Nishat Afshan Ansari, "Deep Learning based Authentication Schemes for Smart Devices in Different Modalities: Progress, Challenges, Performance, Datasets and Future Directions," *Multimedia Tools and Applications*, vol. 83, no. 28, pp. 71451-71493, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Serkan Salturk, and Nihan Kahraman, "Deep Learning-Powered Multimodal Biometric Authentication: Integrating Dynamic Signatures and Facial Data for Enhanced Online Security," *Neural Computing and Applications*, vol. 36, no. 19, pp. 11311-11322, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Kien Nguyen et al., "Deep Learning for Iris Recognition: A Survey," *ACM Computing Surveys*, vol. 56, no. 9, pp. 1-35, 2024. [CrossRef] [Publisher Link]

[12] Yimin Yin et al., "Deep Learning for Iris Recognition: A Review," *Neural Computing and Applications*, vol. 37, no. 17, pp. 11125-11173, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[13] K. Sivasankari, and D. Kerana Hanirex, *Advancing Security on Harnessing Deep Learning for Iris Recognition and Classification*, Optimizing Patient Outcomes Through Multi-Source Data Analysis in Healthcare, IGI Global Scientific Publishing, pp. 1-18, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[14] Abdelnasser Mohammed et al., "Enhancing Network Access Control using Multi-Modal Biometric Authentication Framework," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 20144-20150, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[15] Neama Abdulaziz Dahan, and Emad Sami Jaha, "IRIS-QResNet: A Quantum-Inspired Deep Model for Efficient Iris Biometric Identification and Authentication," *Sensors*, vol. 25, no. 1, pp. 1-44, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[16] Saif Mohanad Kadhim et al., "Deep Learning for Robust Iris Recognition: Introducing Synchronized Spatiotemporal Linear Discriminant Model-Iris," *Advances in Artificial Intelligence and Machine Learning*, vol. 5, no. 1, pp. 3446-3464, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] Azizur Rahman et al., "Distant Iris Recognition Through Machine Learning Models with Deep Features Transfer for Human Identification," *Journal of Innovative Image Processing*, vol. 7, no. 3, pp. 840-860, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] J. Chethana, and J. Ravi, "Deep Segmentation Assisted Residual Spatio-Textural Ensemble Feature Learning Framework for Multimodal Person Authentication System," *International Journal of Advances in Signal and Image Sciences*, vol. 12, no. 1, pp. 1011-1053, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[19] S. Alangaram et al., "AI Powered Secure Payment with Eye Recognition in Wallet Platform," *International Journal of Computer Technology and Electronics Communication*, vol. 9, no. 3, pp. 1018-1025, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[20] S.V. Sheela, and K.R. Radhika, "Deep Learning Driven Fusion of Iris Biometrics for Optimised Multimodal Authentication Informative Security," *International Journal of Information and Computer Security*, vol. 29, no. 4, pp. 397-435, 2026. [CrossRef] [Google Scholar] [Publisher Link]