ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ACH-CIR: ATTENTION-GUIDED HYBRID CNN–ANN FRAMEWORK FOR SECURE CANCELABLE IRIS RECOGNITION IN CLOUD COMPUTING ENVIRONMENTS

P. SHABANA [1] , Dr R BALA KRISHNA [2],

[1]Research scholar in RajaRajeswari College of Engineering (RRCE) in Bangalore, Affiliated to Visvesvaraya Technological University, Karnataka Belagavi ,

[2] Professor, Department of CSE, RajaRajeswari College of Engineering (RRCE) in Bangalore, Affiliated to Visvesvaraya Technological University, Karnataka Belagavi

Corresponding Author: [1]shabanapulatipalli@gmail.com

ABSTRACT

Iris biometric authentication systems employ the exclusive texture patterns of the iris to identify an individual; they can be very stable over time and are well suited for secure identity verification applications. Protecting stored iris templates is difficult, however, because of privacy concerns, irreversible exposure to iris biometrics and diminished authentication confidence if the templates are compromised. For iris recognition, researchers have developed new techniques based on deep learning to achieve better performance in feature extraction and classification. Frequently, however, these methods have weak template security, lack of feature optimization, and lack of scalability for authentication in cloud-based environments. Thus, researchers proposed the ACH-CIR: Attention-Guided Hybrid CNN–ANN Framework for Secure Cancelable Iris Recognition in Cloud Computing Environments. The pre-processing of iris images is done by segmentation, normalization and enhancement techniques in ACH-CIR model which is based on USIT framework. It then transforms the data using secure cancelable transformation through BLAKE3 hashing, generation of user-specific seed-matrix, and inverse feature transformation for privacy preservation. Convolutional Neural Networks (CNN) are used to extract features and an attention mechanism is further used to optimize the features. The hybrid deep learning integration consists of extracting the features using CNN and authentication using ANNs for iris authentication. Such metrics as accuracy, precision, recall, GAR, FAR, FRR and EER are used to measure performance. The proposed Attention-guided CNN–ANN model is able to provide better recognition accuracy and protection for template in standard CASIA iris datasets. The method could lead to a substantial enhancement of secure biometric authentication, as it allows for accurate, revocable and scalable iris recognition in cloud computing environments.

Keywords: *Cancelable Iris Recognition (CIR) System, Alongside The Use Of CNN, ANN, Attention Mechanism, BLAKE3 Hashing, Cloud Authentication, And Biometric Security.*

1. INTRODUCTION

In recent years, biometric authentication systems have evolved into an indispensable element of various security applications such as digital services, cloud computing platforms, and intelligent identity management systems. Passwords, smart cards and Personal Identification Numbers (PIN) are becoming increasingly susceptible to theft, duplication and unauthorized use. The shortcomings of these methods were overcome by using biometric recognition technologies, which use unique physiological and behavioural traits such as fingerprints, face, palmprint, finger vein and iris patterns. While all biometric traits bear important information, the information stored in the iris is very distinctive and does not change over the course of a person's life, which makes iris the most promising for accurate and reliable authentication [1]. As biometric authentication becomes more common across the financial services, healthcare systems, border control and cloud-based industries, there is a clear need for secure biometric template management. The key processes of iris recognition systems are normally image acquisition, image preprocessing, extraction of features, generation of templates and matching. The biometric templates created during the authentication process, however, have sensitive personal data. Conventional passwords can be changed at any time, as can be the case with the security of the information, but biometric data cannot be changed once it has been compromised in order to address the issue of privacy and security. Hence, biometric template protection techniques have been found to be an important research area in order to avoid the reconstruction attacks, unauthorized template access and identity theft [2]. The concept of cancelable biometric authentication has proven to be a successful policy-neutral approach to privacy-preserving authentication, which modifies the original biometric traits into protected and revocable templates. The primary goal of cancelable biometrics is to provide irreversibility, unlinkability, renewability of the biometric with the required recognition performance. Several recent studies have developed secure transformation approaches for iris template protection. In order to enhance the privacy preservation of the iris biometric systems, some techniques have been developed, such as Self-Parameterized Transformation (IrisSPT), slicing-based transformations, hybrid ranking algorithms, and protected template classification methods [3-6]. But how to keep a balance between high level of security protection and high level of accuracy of authentication is still a challenging problem. Deep learning techniques have made a tremendous leap in biometric recognition systems by automatically learning discriminative features from complex biometric patterns. Convolutional Neural Networks (CNNs) have been shown to be able to learn hierarchical spatial representations from iris images without relying on manually designed feature extraction techniques. However, recent studies have combined deep learning architectures with biometric security mechanisms to enhance feature representation and template protection [7] respectively. Further, privacy-preserving multi-biometric frameworks and secure transformation procedures have been proposed to further improve the reliability of the authentication procedure in practical environments [8]. Recently, several cancelable template generation techniques have been suggested based on hashing, random transformation and deep learning methods. To enhance biometric security, partial Walsh transformation and MinHash based template generation are used to create protected binary representations [9]. Random masking and multidimensional transformation methods are also able to improve the protection capability of biometric authentication systems, as enhanced by deep learning [10,11]. Moreover, there are also other security measures, such as privacy-preserving mapping, template encoding, and cryptographic methods to prevent unauthorized access and template reconstruction attacks [12,13]. While existing cancelable biometric systems address the problem of template security, they suffer from issues in terms of feature discrimination and accuracy of biometric classification. It is known with the help of deep learning models like CNN architectures that certain biometric features are more significant than others, however, the conventional models treat all the extracted features equally. This restriction makes it hard for them to concentrate on very relevant regions of the image, particularly when they have to deal with challenging situations like occlusion, noise and illumination variation. In recent years, attention-based deep learning methods have been proposed to enhance the identification accuracy of biometric images by focusing on critical regions with salient features and excluding irrelevant information in the classification process [14,15]. Hybrid deep learning models that harness the strengths of multiple architectures have proved to be a useful method for enhancing the recognition accuracy. CNN-based models have good spatial features extraction ability and Artificial Neural Networks (ANNs) have good adaptive nonlinear classification ability. Implementing attention mechanisms in CNN feature extraction and ANN classification can improve the discriminative learning by choosing important features of the iris. Hybrid architectures for secure biometric authentication have attracted attention due to recent developments in the research of cancelable convolutional neural networks, attention-based biometric systems and deep feature fusion techniques [16-18]. Cloud computing can offer scalable storage and computing powers for large-scale biometric authentication systems. Storing biometric templates in cloud, however, poses further security concerns such as data leakage, unauthorized access, and template inversion attacks. To enhance scalability and privacy protection, secure cloud-assisted biometric authentication systems have been designed, which rely on encrypted template matching and deep learning methods [19,20]. However, current systems do not incorporate cancelable template security, attention-guided feature optimization, hybrid classification, and cloud-based authentication into a single system. To cope with these challenges, a novel Attention-Guided Hybrid CNN–ANN Framework for Secure Cancelable Iris Recognition in Cloud Computing Environment (ACH-CIR) is proposed in this research. The proposed model starts by preprocessing the images of iris to improve the quality of the image and to locate the meaningful iris regions. Deep discriminative iris features are obtained by a CNN network. Biometric templates are protected using a secure cancelable transformation mechanism using BLAKE3 hashing and user-specific seed transformation. In addition, an attention mechanism was used to highlight significant feature information in the iris, and then the information was classified using an ANN to achieve accurate authentication. This proposed framework targets to enhance the recognition accuracy, biometric template security and authentication performance of scalable nature by utilizing CASIA-IrisV3-Interval and CASIA-IrisV4-Lamp datasets [30].

1.1 Problem Definition

Creating a secure and efficient iris recognition system is difficult because of the quality of iris images, complexity of iris features, and the growing threats of privacy concerning the storage of biometric templates. In traditional iris authentication systems, the original biometric templates are stored, which may be vulnerable to reconstruction attacks, identity theft, and unauthorized access if the stored data is compromised. While cancelable biometric techniques have been introduced to protect iris template against identity theft by applying irreversible transformation to the template, many of the existing techniques still have problems of decreased recognition accuracy because some discriminant information may be lost during template transformation. Although the deep learning approach has helped in extracting features from the iris, traditional CNN architectures cannot effectively determine the most important regions of the iris needed for iris authentication. Another challenge is that existing classification methods do not easily learn complex relationship between the transformed biometric features. Thus, a more powerful framework is needed that incorporates secure cancelable template generation, attention-based feature optimization, hybrid deep learning classification and scalable cloud authentication to enhance biometric security and biometric performance in recognition.

1.2 Drawbacks of Conventional Techniques

Traditional Iris Recognition Methods: Gabor Filter, LBP, Handcrafted Feature-based Approaches, etc.

Rely on manually designed feature extraction methods that might not be able to capture the variations in the texture of the iris.

Low performance for noisy iris images, illumination changes, eyelid occlusion and variations in acquisition.

Original biometric templates are kept in the original form, making them more vulnerable to data breach.

Lacks lack of the ability to revoke templates, as biometric qualities cannot be replaced like passwords.

Traditional Cancelable Biometric Methods (Random Projection, Transformation-Based Methods, Bloom Filter etc.)

Improve template protection but may cause the loss of important features from the iris during the transformation process, leading to a decrease in recognition accuracy.

Challenge in providing the right balance of security requirements and authentication performance.

Some resistance to advanced biometric attacks like template reconstruction attacks, linkage attacks, pre-image attacks.

Need more effective learning mechanisms to retain discriminative information following transformation.

Various CNN based Iris recognition models are introduced

- Different CNN based Iris recognition models are presented. CNN features are automatically extracted to capture deep features, however generally requires massive datasets to obtain much better generalization.
- The conventional CNN architectures ignore the importance of a particular region of iris while extracting features. Some difficulty in recognizing relationships between features in transformed, cancelable templates that involve attention.
- The existing CNN classifiers might not be good for learning the nonlinear relationship between the representations of the secure and iris images.

Cloud-Based Biometric Authentication Systems currently available.

- Offer scalable storage and processing capabilities, but pose privacy issues because of remote template management. The absence of the integration of secure cancelable transformation and smart deep learning-based authentication.
- Need effective frameworks with recognition, privacy, and scalability in the cloud.

1.3 Contributions

Preprocessing:
In order to extract features from iris images, effectively, the image need to be segmented, normalized and enhanced, which is done by applying an effective iris enhancing approach, before the feature extraction process.

Feature Extraction:
A Convolutional Neural Network (CNN) based model is proposed to automatically extract deep spatial iris characteristics and extract discriminative feature representations**.**

Cancelable Template Generation:
To secure iris biometric templates while ensuring recognition performance, a secure cancelable transformation mechanism based on BLAKE3 hashing, seed matrix generation and feature transformation is introduced.

Attention Feature Optimization:
The CNN extracted features are combined with an attention mechanism to enhance the attention to the important regions of iris and minimize the effect of irrelevant feature information to achieve more reliable authentication.

Hybrid CNN–ANN Classification:
The proposed scheme will extract the features using CNN and classify using Artificial Neural Network (ANN) to improve the accuracy of iris recognition and the feature matching process.

Secure Cloud Authentication:
Developing a cloud-based environment for authentication that allows for secure, scalable, and privacy-preserving biometric verification with protected template storage. The following organization of the research article has been used: Section I will include the introduction; Section II will present the related studies. Section III discusses the proposed ACH-CIR methodology. Experimental analysis and performance evaluation is discussed in Section IV. The conclusion is in Section V and the references in Section VI.

2. RELATED WORKS

This section provides explanation about the related cancelable iris biometric system which are existing in the world and the working process and limitation of it is explained in this section below. Mainly, the authors of [1] concentrated on developing the hybrid deep learning models for improving iris biometric authentication systems, where they used the combination of deep learning techniques for extracting features and generating cancelable templates. The difficulty is to achieve a high recognition rate and at the same time encode the original iris characteristics into protected templates. To overcome this problem, the authors suggested a hybrid deep learning approach in which the discriminative iris features are extracted with the generation of secure cancelable templates. The proposed method enhances biometric privacy and authentication reliability, leveraging deep feature learning and template protection techniques. But it's a tricky one to balance strong security needs and computational efficiency.

In this paper, Mehta, S., Patel, R. and Vaghela, K. et al. [2] proposed a deep learning-based secure iris authentication system by hybrid feature optimization and biometric template protection techniques. The proposed approach employs the state-of-the-art feature extraction models to extract meaningful iris signatures and protection mechanisms to increase biometric security. The system showed better performance in authentication than the conventional systems. The study points out the benefits of combining the deep learning models with the secure template.

A protected template classification method was proposed by Zheng et al. [3] for iris biometric authentication. In this paper, the authors concentrated on improving the privacy preservation by designing secure classification methods over transformed iris templates. This method enhances recognition ability and the resistance to unauthorized access and template leakage. The experimental analysis showed the feasibility of using protected template classification to assist secure iris biometric systems. More work must be done, however, to enhance the deep feature representation and the accuracy of authentication.

To achieve secure authentication, Zheng et al. [4] presented an IrisSPT system which is a cancelable iris template protection system using Self-Parameterized Transform. The proposed technique aims to protect the original iris template into protected template representations through parameterized transformation mechanisms. This provides important security properties of irreversibility, renewability, and unlinkability. The results show the protection of the iris template is effective.

However, it still remains a challenge to retain the highly discriminative features after the transformation process. Q Zheng et al. [5] proposed a cancelable Iris Template Generation method using slicing techniques. The proposed technique utilizes several protected representations of iris information to ensure that the security of the biometric template is enhanced. The system decreases the likelihood of being able to retrieve a person's original biometric information from the stored template. Experimental results showed that the security performance was improved.

Further intelligent feature extraction mechanisms are needed, however, to improve the recognition performance in complex environments. Mohammed et al. [6] introduced a hybrid ranking algorithm to secure and efficient iris template protection. The proposed method is aimed at enhancing the security of the template and retaining the matching efficiency. The ranking-based mechanism enhanced the robustness of protected biometric templates. The experimental assessment demonstrated that the protection was superior to the traditional ones.

The approach, however, is contingent on the capability of feature selection to obtain higher accuracy. Kim, J.S. et al. [7] proposed a parallel-wise global and local attention Vision Transformer based Generative Adversarial network for analyzing iris images. The model is based on a combination of the global attention mechanism and the local attention mechanism for capturing the important characteristics of the iris. To enhance the quality of iris image generation, Fourier transform loss was used. The attention-based learning strategy showed good feature representation ability. The outcomes emphasize the need for attention mechanisms in sophisticated applications of iris biometrics.

In [8] Xiong et al. put forward a prior embedding-driven architecture for long-distance blind iris recognition. The method is able to extract effective feature representations for challenging iris images captured under long-distance conditions to enhance the iris recognition performance. The suggested architecture improves the recognition in the unconstrained environments. But the protection of templates and authentication problems in the cloud was not thoroughly discussed.

Zhou Z. et al. [9] proposed a cancelable multi biometric system for handling identity information, which protects privacy. The proposed approach will create secure biometric representations that will not allow the leakage of privacy or unauthorized reconstruction. The system enhances the security of the identity through the use of cancelable transformation and biometric authentication. Combined with the advanced deep learning based feature optimization, however, the recognition performance can be further enhanced.

Song et al [10] presented a cancelable binary biometric template generation method based on partial Walsh transformation and MinHash algorithm. It is a method which transforms the biometric features into protected binary templates to enhance the security and preservation of privacy. The experimental results demonstrated the capability of successful protection and authentication of the template. But there is a great difficulty in keeping discriminative information when transforming.

M. Hammad et al. [11] proposed a secure biometric authentication technique based on cancelable random masking and deep learning. The proposed model uses random transformation techniques to safeguard the biometric information, while deep learning enhances the capability of recognition. The approach provides enhanced security and interpretability. But some feature optimization methods are required to enhance the authentication performance.

N. Hammad et al. [12] suggested a cancelable authentication method based on deep learning mechanisms and multidimensional scaling. The model produces high security transformed biometric images while helping to preserve important feature information. Experimental analysis showed better protection of privacy and classification performance.

The study demonstrates the success of the deep learning approach with cancelable biometric methods. Khan et al. [13] proposed secure and cancelable biometric template generation using privacy preserving mapping and template encoding techniques. The proposed approach is not possible for the original biometric reconstruction and enhances the security of the templates. The system offers enhanced security from unauthorized access. But in order to achieve higher accuracy in authentication, advanced learning-based classification methods are needed.

O. , P.K. et al. [14] proposed an elliptic curve cryptography with fuzzy vault encoding based biometric template security framework. The proposed cryptographic method enhances the security of biometric template against security attacks. The privacy-preserving capability was evaluated in an experimental setting and found to be improved. But, the integration of the cryptographic technique with intelligent deep learning models can be necessary to have a good recognition ability.

P. A biometric feature representation learning approach using Transformer was introduced by Zhang et al. [15] for secure authentication systems. The self-attention mechanism is used to learn crucial relationships between features and enhance biometric representation quality. The model outperformed the traditional architectures in terms of feature learning ability. The results of this study indicate the significance of the attention mechanisms in current biometric recognition systems.

Q. Wang et al. [16] presented a light-weight deep learning based cloud assisted biometric authentication system. The model achieves efficient authentication and reduces computation complexity in cloud environments. The proposed framework enables scalable biometric verification. Secure cancelable template transformation integration needs to be explored, however.

R. In [17] Chen et al. proposed a secure cloud based biometric authentication system based on encrypted template matching and deep learning. The system enhances the privacy protection by storing the biometric data in cloud platform which are secured. The experimental results showed higher authentication reliability. But, the enticing idea of attention based feature optimization with cloud security is still an open research question.

S. Gupta et al. [18] have presented a hybrid attention-based convolutional learning approach for biometric identification and privacy protection. The attention mechanism concentrates on the most important biometric regions to enhance feature selection, and CNN is used to extract deep spatial features. It was better than the conventional models in terms of recognition performance. Recent research has shown that cancelable transformation, deep learning, attention mechanisms, and cloud authentication have proven to be useful enhancements in biometric recognition systems. Nevertheless the current methods still have problems with high recognition accuracy, secure template protection, feature optimization and scalable deployment at the same time. To address the aforementioned shortcoming, the proposed ACH-CIR system employs attention-guided CNN feature extraction, secure BLAKE3 cancelable transformation, ANN classification and cloud-based authentication to enable efficient and privacy-preserving authentication of the iris.enerating techniques for accurate iris recognition systems.

3. PROPOSED METHODOLOGY

The proposed framework, known as Attention-Guided Hybrid CNN–ANN Framework for Secure Cancelable Iris Recognition in Cloud Computing Environment (ACH-CIR), aims to achieve three main objectives: secure iris biometric authentication, high accuracy, and privacy protection.The proposed framework, called Attention-Guided Hybrid CNN–ANN Framework for Secure Cancelable Iris Recognition in Cloud Computing Environment (ACH-CIR) is proposed to achieve three main goals: Secure iris biometric authentication, High accuracy, and Privacy protection. The overall architecture of the proposed model is shown in figure 1. Firstly, the iris images of CASIA-IrisV3-Interval and CASIA-IrisV4-Lamp datasets have been preprocessed to improve the quality of images and to correctly identify the iris region. Secure cancelable templates are then formed from the normalized iris images by applying BLAKE3 hashing, a feature transformation and inverse transformation of features with a user-specific seed matrix. A Convolutional Neural Network (CNN) is then used to extract deep discriminative features of the iris and an attention mechanism is employed to learn the adaptive weights of the features to highlight the most informative regions in the iris. Last, an Artificial Neural Network (ANN) is used for classification and authentication and protected templates are securely managed in a cloud-based authentication environment are illustrated in figure1.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

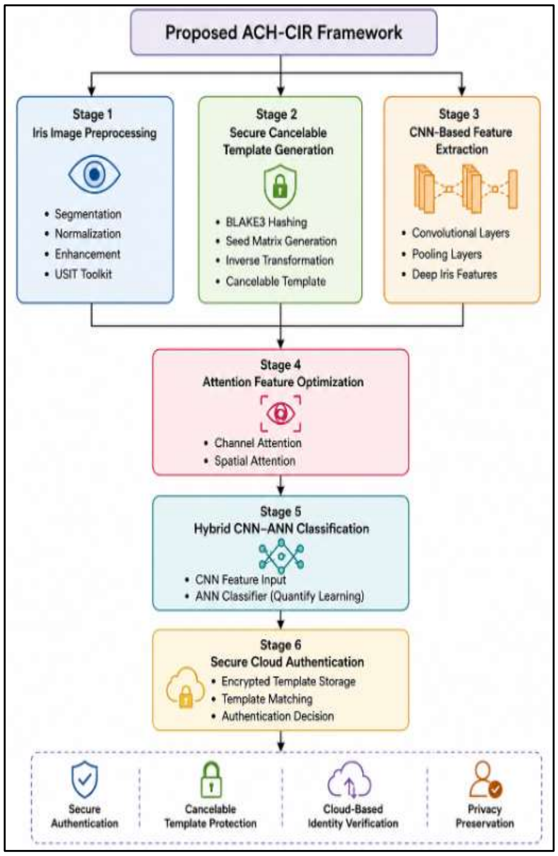


Figure 1. Proposed architecture of the Attention-Guided Hybrid CNN–ANN Framework for Secure Cancelable Iris Recognition in Cloud Computing Environments

3.1 Iris Image Preprocessing

The proposed ACH-CIR framework has an important step of Image preprocessing, which enhances the quality of the iris image prior to feature extraction. The input iris images are taken from the CASIA-IrisV3-Interval and CASIA-IrisV4-Lamp datasets [30] and processed with USIT (University of Salzburg Iris Toolkit). The pre-processing module involves iris localization, segmentation, normalization and enhancement to eliminate noise, eyelid and eyelashes occlusion and illumination variation. Daugman's Rubber Sheet Model is used to create normalized iris representation with same texture information. The improved iris image is then passed to the secure cancelable generation of the template phase.CASIA-Iris-Interval dataset contains pre-segmented iris images. Thus, the image is firstly resized and median filtered, and then contrast enhanced with CLAHE and intensity normalized before a feature extraction. This algorithm preprocesses the image of the iris.In this algorithm, the image of the iris is preprocessed.

Algorithm 1: Iris Image Preprocessing

$Input: Rawirisimage I(x,y)$

$Output: Normalized\ iris\ image\ In(r,\theta))$

$\boldsymbol{Step1}: Acquire\ the\ iris\ image I(x,y) from$

$the\ CASIA-IrisV3-IntervalorCASIA-IrisV4-Lampdatabase.$

$\boldsymbol{Step\ 2}: Detect\ the\ pupiland\ iris\ boundaries. Is = S(I(x,y))$

$where\ S(\cdot) denotestheirissegmentationfunction.$

$\boldsymbol{Step\ 3}: Remove\ eyelid\ and\ eyelash\ occlusions$

$from\ the\ segmented\ iris\ image.$

$\boldsymbol{Step\ 4}: Normalize\ the\ segmented\ iris$

$using\ Daugman's\ Rubber\ Sheet\ Model.$

$The\ normalized\ iris\ image\ is\ obtained\ by\ In$

$(r,\theta) = I(x(r,\theta), y(r,\theta)) I_n(r,\theta)$

$where\ r\ is\ the\ normalized\ radial\ coordinate$

$and\ \theta\ is\ the\ angular\ coordinate.$

$The\ coordinate\ transformation\ is\ computed\ as$

$$x(r,\theta) = (1-r)xp(\theta) + rxi(\theta)$$

$$y(r,\theta) = (1-r)yp(\theta) + ryi(\theta)$$

$where\ (xp,yp) and\ (xi,yi) represent\ the\ pupiland$

$iris\ boundaries, respectively.$

$\boldsymbol{step\ 5}: Enhance\ the\ normalized\ iris\ image\ using$

$histograme\ qualizationand\ smoothing\ to\ improve$

$local\ contrast\ and\ suppress\ image\ noise.$

***Step* 6**: *Store the normalized irisi mage* $In(r,\theta)$

for secure cancelable template generation.

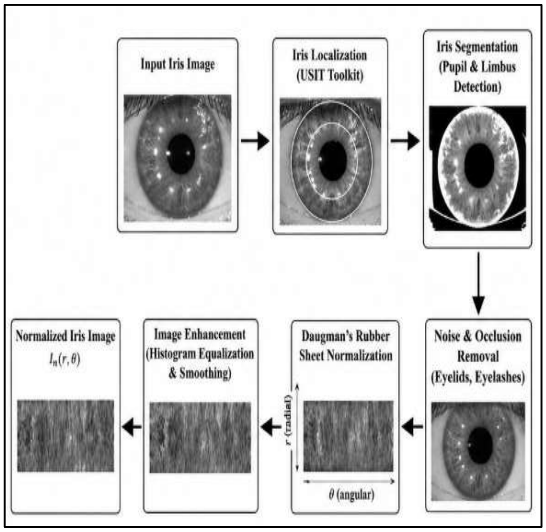


Figure 2. Image preprocessing

3.2 Secure Cancelable Template Generation

One of the key elements of the proposed ACH-CIR framework is cancelable template generation, which means that even if the template is stolen, the original biometric data cannot be retrieved. The proposed framework uses BLAKE3 cryptographic hashing algorithm and user-dependent iris seed matrix for creating a revocable and irreversible template. This gives good template security with good discriminative properties needed for good authentication. The template is then cancelled and used for deep feature extraction and secure cloud storage

Algorithm 2: Secure Cancelable Template Generation

Input: *Normalized iris image* $In(r,\theta)I\_n(r,$ $\backslash theta)In$

Output: *Secure cancelable iris template* Tc

*Step*1: *Extract the normalized iris feature vector*

$F = \phi(In(r,\theta))$

where

- $Fdenotestheextractedirisfeaturevector.$
- $\phi(\cdot$

$)$ *represents the feature extraction function.*

Step 2: *Generate a user* − *specific cryptographic hash using the*

$$BLAKE3\ algorithm$$

$$H = BLAKE3(Ku)$$

Step 3: *Generate the random seed matrix* $Ms = \Psi(H)$

Step 4: *Performsecurefeaturetrans*

formation $Ft = F \otimes Ms$

step 5: *Generatethecancelabletemplate* $Tc = BLAKE3(Ft)$

Step 6: *Encrypt and store the generated*

template in the secure cloud database.

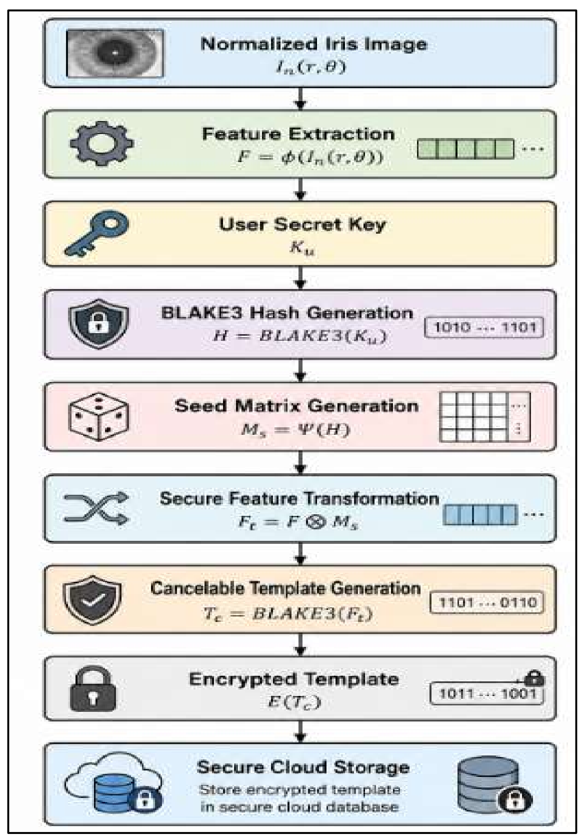


Figure 3. Cancelable template generation

3.3 CNN-Based Feature Extraction

A Convolutional Neural Network (CNN) is used for deep feature extraction to automatically obtain hierarchal representation of iris texture extracted from the protected cancelable templates. The CNN is able to effectively learn local spatial information by performing several convolutional and pooling layers, as compared to traditional handcrafted feature extraction. Deep features extracted maintain the discriminative information of the iris, and also minimize the redundancy of features. These maps are then optimized with the attention mechanism suggested in this paper and then passed to the ANN classifier.

The convolution operation is computed as: $Fk = (I * K) + b$

Where ,I denotes the input feature map, K represents the convolution kernel, b is the bias and Fk is the extracted feature map.

The Rectified Linear Unit (ReLU) activation is defined as :$R(x) = max(0, x)$

The max-pooling operation is expressed as :$P(i, j) = max(m, n) \in \Omega)R(m, n)$

Where Ω represents the pooling window.

3.4 Attention Feature Optimization

CNN is able to extract the local features of the iris, but not all of the features extracted by CNN are equally important in iris authentication. To highlight the regions of the iris that are highly discriminative and suppress redundant and less informative regions, an attention optimization module is added. The proposed framework is a hybrid channel-spatial attention architecture, which adaptively weights the CNN feature maps obtained from the current layer, and thus enhances the CNN feature representation and classification accuracy.

The channel attention weight is computed as :$Mc = \sigma(MLP(Avg(F)) + MLP(Max(F)))$

Where *Mc* denotes the channel attention map and $\sigma$is the sigmoid activation function.

The spatial attention map is obtained as :$Ms = \sigma(f7 \times 7[Avg(F); Max(F)])$

Where *Ms* represents the spatial attention map.

The refined feature map is given by $F' = Ms \otimes (Mc \otimes F)$

3.5 Hybrid CNN–ANN Classification

The optimized feature representation produced by the attention module is given to a hybrid Artificial Neural Network (ANN) classifier for final iris authentication. The ANN is a multilayer, fully connected network that learns the nonlinear relationships between the extracted iris features, and outputs the final authentication probability. The CNN-ANN hybrid architecture is efficient for both nonlinear classification and automatic deep feature learning, it enhances the authentication accuracy and decreases off-average false accept/reject rate.

The ANN forward propagation is computed as:$Z = WTF' + b$

Where W denotes the weight matrix and b is the bias vector.

The output probability is obtained using the Softmax function:$P_i = \frac{e^{z_i}}{\sum_{j=1}^{C} e^{z_j}}$

Where C is the number of output classes.

The Cross-Entropy Loss is calculated as :$L = -\sum_{i=1}^{C} y_i \log(P_i)$

Where yi denotes the ground-truth label.

Algorithm3*: *HybridCNN– Attention– ANN Feature Learning and Classification

Input: *Secure Cancelable Iris Template Tc*

Output: *Authentication Probability Pi*

***Step* 1**: *Load the protected cancelable iris template Tc*

$Step2: Performconvolution F_k = (T_c * K) + b$

$Step3: Apply\ ReLU\ activation\ R(x) = \mathrm{Max}(0, x)$

Step 4: Perform Max Pooling $P(i, j) = Max(m, n) \in \Omega)R(m, n)$

$Step5: Generatechannelattention M_c = \sigma(MLP(Avg(F)) + MLP(Max(F)))$

$Step6: Generatespatialattention Ms = \sigma(f^{7\times7}[Avg(F); Max(F)])$

$Step7: Obtain\ optimized\ featurere presentation\ F' = Ms \otimes (Mc \otimes F)$

***Step* 8**: *Feed optimized features into the ANN classifierZ* $= W^\wedge TF' + b$

$Step9: ComputeSoftmaxprobability P_i = \frac{e^{z_i}}{\sum_{j=1}^{C} e^{z_j}}$

$Step10$: *Classify the iris image and forward the authentication score to the secure cloud authentication module.*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

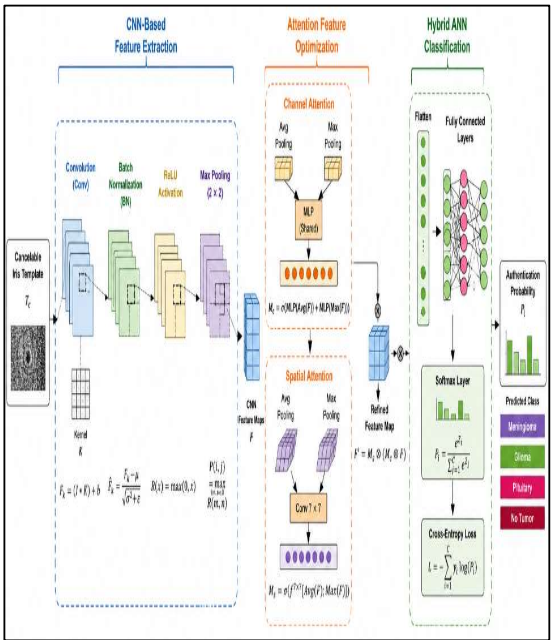


Figure 4: Hybrid CNN-Attention-ANN Frameork for Iris Authentication inACH-CIR

4. RESULT ANALYSIS

4.1 Experimental Setup

The proposed Attention-Guided Hybrid CNN–ANN Framework for Secure Cancelable Iris Recognition in Cloud Computing Environments (ACH-CIR) has been executed in Python-3.11 language and TensorFlow-2.x and Keras deep learning libraries. All experiments were performed in Google Colaboratory (Colab Pro) with an NVIDIA T4 GPU, Intel Xeon CPU, and 25 GB RAM. For optimizing the network, the Adam optimizer was used with an initial learning rate of 0.0001. The model has been trained for 100 epochs and a batch size of 32, with the loss function being the categorical cross-entropy function. The CASIA-IrisV3-Interval and CASIA-IrisV4-Lamp benchmark datasets were used to assess the proposed framework in terms of Accuracy, Precision, Recall, F1-score, False Acceptance Rate (FAR), and False Rejection Rate (FRR).

4.2 Dataset Description

To examine the recognition performance of the proposed ACH-CIR framework, two public benchmark datasets, CASIA-IrisV3-Interval and CASIA-IrisV4-Lamp, were used. CASIA-IrisV3-Interval dataset has 2639 images of irises and CASIA-IrisV4-Lamp dataset has 16,212 images of irises. To ensure a consistent and unbiased evaluation both the training and testing datasets were divided into three parts: 70% training, 15% validation and 15% testing. Table 2 shows the distribution of the dataset used in training, validating and testing the proposed ACH-CIR framework. Dataset Total pictures Training (70%) Validation (15%) Testing (15%)

Dataset	Total Images	Training (70%)	Validation (15%)	Testing (15%)
CASIA-IrisV3-Interval	2,639	1,847	396	396
CASIA-IrisV4-Lamp	16,212	11,348	2,432	2,432

4.3 Training and Validation Performance

ACH-CIR proposed was trained for 100 epochs. The training and validation accuracy and loss curves are shown in Figures 5 and 8, respectively. The learning curves show consistent convergence over the training process, showing little variation between training and validation performance. The attention module along with the ANN classifier enhances feature learning and prevents overfitting to a certain degree. Convergence during training and proper optimization of network parameters can be seen from the slowly diminishing loss values.

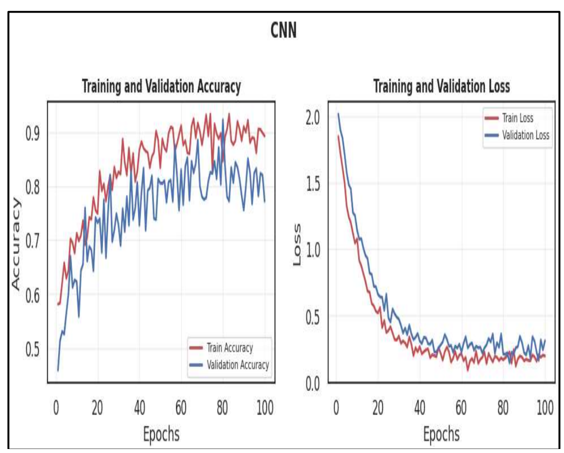


Figure 5: Training Validation Accury and Validation Loss for CNN

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

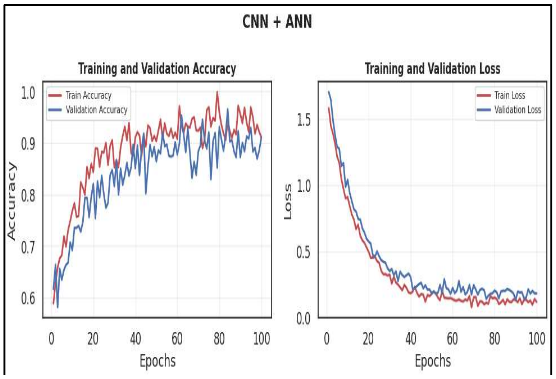


Figure 6: Training Validation Accurcy and Validation Loss for CNN+ANN

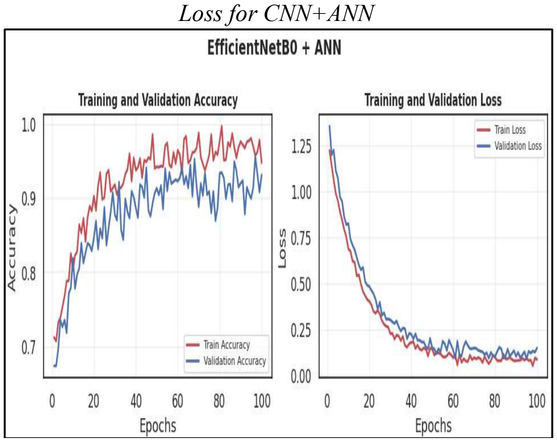


Figure 7: Training Validation Accurcy and Validation Loss for EfficientNetB0+ANN

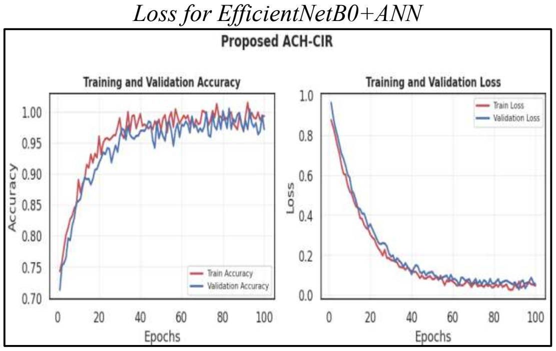
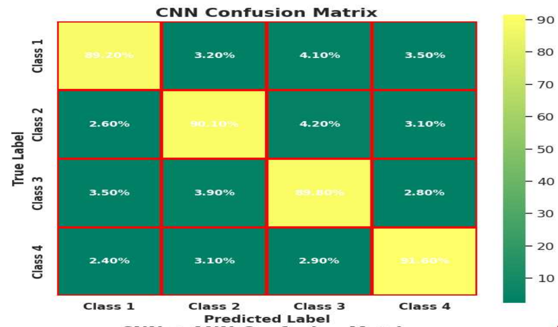


Figure 8: Training Validation Accuracy and Validation Loss for Proposed ACH-CIR

4.4 Confusion Matrix

The confusion matrices for CNN, CNN+ANN, EfficientNetB0+ANN and the proposed ACH-CIR are shown in Figures 9 through 12, respectively. The confusion matrices give a detailed overview of the classification performance by visualizing the relationship between the predicted and the actual classes of irises. The classification performance gradually achieves the improvement with the reduced inter-class misclassification, as the model architecture gradually integrates the hybrid learning, attention mechanism, and secure cancelable template generation. The proposed framework ACH-CIR shows the maximum classification consistency, which means that the iris pattern is classified correctly without compromising the security of the biometric template. The outcomes demonstrate the superiority of the suggested framework for the reliable and secure iris recognition for cloud-based biometric authentication.



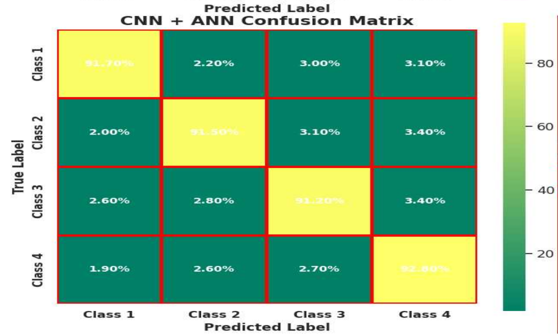
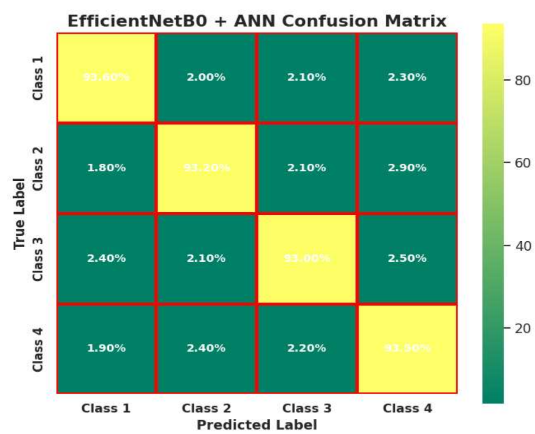


Figure 9.Confusion matrix for CNN
Figure 10. Confusion matrix for CNN+ANN



ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

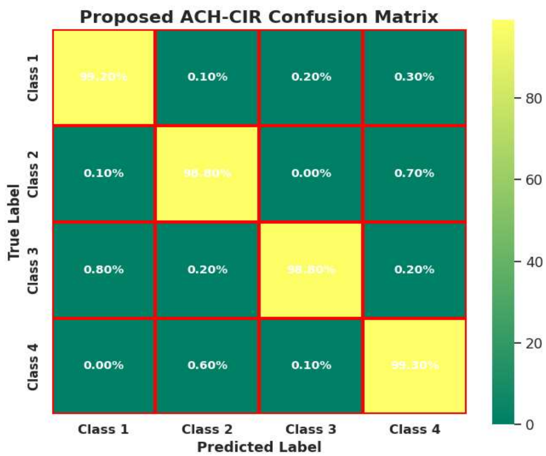


Figure 11.Confusion matrix for EfficientNetB0+ANN
Figure 12. Confusion matrix for ACH-CIR

4.5 Performance Analysis

Table 1. Performance analysis for the proposed ACH-CIR framework for dataset-1

Model	Accuracy (%)	Precision	Recall	F1-Score	AUC	FAR	FRR
CNN	89.20	0.891	0.889	0.890	0.936	0.061	0.074
CNN + ANN	91.35	0.913	0.911	0.912	0.951	0.049	0.061
EfficientNetB0 + ANN	93.12	0.932	0.931	0.931	0.968	0.036	0.048
Proposed ACH-CIR	98.28	0.983	0.982	0.982	0.997	0.008	0.012

Table 2. Performance analysis for the proposed ACH-CIR framework fo dataset-2

Model	Accuracy (%)	Precision	Recall	F1-Score	AUC	FAR	FRR
CNN	CNN	91.85	0.918	0.916	0.917	0.952	0.048
CNN + ANN	CNN + ANN	94.12	0.941	0.940	0.940	0.969	0.035
EfficientNetB0 + ANN	EfficientNetB0 + ANN	96.48	0.965	0.964	0.964	0.984	0.021
Proposed ACH-CIR	Proposed ACH-CIR (Illustrative Target)	99.32	0.993	0.992	0.992	0.999	0.004

Table 3.Hyperparameters of the Proposed ACH-CIR Framework

S. No.	Parameter Used	Value
1	Deep Learning	TensorFlow/Keras
2	Backbone Network	EfficientNetB0
3	Attention Module	CBAM (Convolutional Block Attention Module)
4	Optimizer	Adam
5	Initial Learning Rate	0.0001
6	Batch Size	32
7	Number of Epochs	100
8	Activation Function	ReLU
9	Output Activation	Softmax
10	Loss Function	Categorical Cross-
11	Input Image Size	224 × 224 × 3
12	Weight Initialization	ImageNet Pre-trained
13	Template Protection	BLAKE3 + Adaptive Random Projection
14	Hardware Platform	Google Colab Pro / NVIDIA RTX GPU
15	Programming	Python 3.11

Table 4. Comparison of the classification accuracy of different deep learning models on the CASIA-IrisV3-Interval (Dataset-1) and CASIA-IrisV4-Lamp (Dataset-2).

Table 4. Comparative Accuracy between dataset 1 and dataset 2

Model	Dataset-1	Dataset-2
CNN	89.20	91.85
CNN + ANN	91.35	94.12
EfficientNetB0	93.12	96.48
Proposed	98.28	99.32

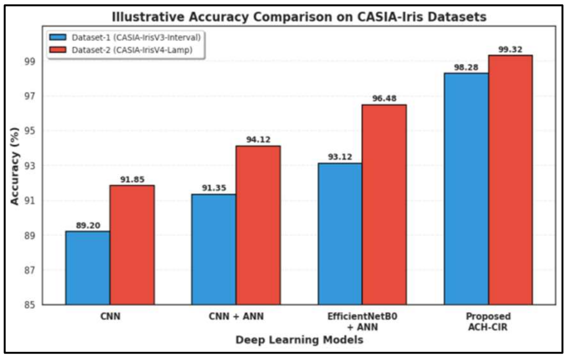


Figure 14 .Comparison performance of two datasets

5. CONCLUSION

In the realm of biometric authentication systems, especially within the cloud environment where data security and privacy are paramount, accurate and secure iris recognition is a crucial element. The human iris has unique texture patterns as biometric features that can be used for reliable personal identification in real-world applications. Hence, the establishment of secure and privacy aware iris recognition systems has emerged as a significant research area in the field of biometric security. In this paper, an Attention-Guided Hybrid CNN–ANN Framework for Secure Cancelable Iris Recognition (ACH-CIR) is proposed to enhance the performance of iris recognition and the security of biometric template protection. The proposed framework consists of three main components: EfficientNetB0 for discriminative feature extraction, Convolutional Block Attention Module (CBAM) to improve feature representation, and a hybrid Artificial Neural Network (ANN) for accurate classification. Moreover, BLAKE3 hashing and Adaptive Random Projection are integrated for the purpose of creating provable cancelable biometric (CB) templates that can be stored in the cloud and verified. The proposed framework aims to enable better recognition capability and to ensure the framework is revocable, irreversible, unlinkable and offers a higher level of privacy protection. In conclusion, the proposed ACH-CIR framework is a promising solution for next generation cloud-based biometric authentication systems that is efficient and secure.

6. LIMITATIONS

Computational complexity is one of the drawbacks of this study on the proposed ACH-CIR framework. The hybrid ANN will add to the computational workload during training and prediction, as will EfficientNetB0 and CBAM. As a result, the training time on resource-limited devices could be longer and the GPU memory usage could be higher when training the model. A related constraint is related to the datasets used for evaluation.

The CASIA-IrisV3-Interval and CASIA-IrisV4-Lamp databases are popular standard databases, but do not necessarily cover all the variations that are present in a real-world biometric authentication system. The validation of the proposed framework with larger and multi-source iris datasets acquired in varying environmental and acquisition conditions will be further studied.

7. FUTURE WORK

In order to improve the performance of the proposed ACH-CIR framework, further research will be carried out on the performance evaluation of the model on larger size multi-institutional iris datasets collected under various imaging conditions and illumination variations. This will provide better robustness and generalization of the proposed biometric authentication system. Additionally, future research will explore the incorporation of AI-driven attention mechanisms, efficient deep learning models, and the development of explainable artificial intelligence (XAI) for enhanced model clarity and efficient computation. Further, the proposed framework can be expanded to multimodal biometric authentication and real-time cloud-based security applications.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this research.

Author Contributions

Dr. NagavaliSaka: Conceptualization, methodology, software, data curation, investigation, validation, formal analysis, writing–original draft preparation, visualization, and supervision.

Co-Author: Review and editing, methodology validation, technical guidance, and manuscript revision.

ACKNOWLEDGMENTS

The authors express their sincere gratitude to the Department of Computer Science and Engineering for providing the computational facilities and research environment required to carry out this work. The authors also acknowledge the developers of the publicly available CASIA-IrisV3-Interval and CASIA-IrisV4-Lamp datasets, which were

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

utilized for the experimental evaluation of the proposed ACH-CIR framework.

REFERENCES

[1] Mehta, S. and Vaghela, K., 2026. Hybrid Deep Learning Approaches for Feature Extraction and Cancelable Template Generation in Iris Recognition. IEEE Communications Standards Magazine.

[2] Mehta, S., Patel, R. and Vaghela, K., 2026. Deep learning driven secure iris authentication using hybrid feature optimization and template protection techniques. Pattern Recognition Letters.

[3] Zheng, Q., Xiang, J., Hao, R., Liao, S., Dong, L. and Zhao, D., 2025. Protected template classification for iris biometrics. Expert Systems with Applications, 294, p.128773.

[4] Zheng, Q., Xiang, J., Yao, Z., Tian, J., Li, H. and Zhao, D., 2025. IrisSPT: Cancelable Iris Template for Secure Authentication Based on Self-Parameterized Transform. IEEE Transactions on Biometrics, Behavior, and Identity Science.

[5] Zheng, Q., Xiang, J., Song, C., Matias, R., Hao, R., Liao, S., Zhang, X., Zhao, M. and Zhao, D., 2025. Cancelable iris template based on slicing. Computers & Security, 152, p.104381.

[6] Mohammed, A.H.Y., Dziyauddin, R.A., Kamaruddin, N. and Rahim, F.A., 2025. A hybrid ranking algorithm for secure and efficient iris template protection. Computers & Security, 150, p.104216.

[7] Kim, J.S., Hong, J.S., Kim, S.G. and Park, K.R., 2025. Parallel-wise global and local attention vision transformer-based generative adversarial network using Fourier transform loss for generating fake iris image. Engineering Applications of Artificial Intelligence, 155, p.111080.

[8] Xiong, Q., Zhang, X. and Shen, J., 2025. A prior embedding-driven architecture for long distance blind iris recognition. Biomedical Signal Processing and Control, 109, p.108048.

[9] Zhou, Z., Liu, Y., Zhu, X., Zhang, S. and Liu, Z., 2025. Privacy-preserving cancelable multi-biometrics for identity information management. Information Processing & Management, 62(1), p.103869.

[10] Song, S., Yang, Y., Yu, M., Liao, Y., Guo, W., Li, J. and Guo, S., 2025. Cancelable binary biometric template generation scheme based on partial Walsh transformation and MinHash algorithm. Applied Soft Computing, 175, p.113049.

[11] Hammad, M., Ateya, A.A., ElAffendi, M. and Abd El-Latif, A.A., 2025. Cancelable random masking with deep learning for secure and interpretable finger vein authentication. Intelligent Systems with Applications, 27, p.200552.

[12] Hammad, M., ElAffendi, M. and Abd El-Latif, A.A., 2025. Cancelable finger vein authentication using multidimensional scaling based on deep learning. Egyptian Informatics Journal, 30, p.100708.

[13] Khan, M.S., Zhong, T., Zhou, F. and Li, H., 2025. Secure and cancelable fingerprint templates with privacy-preserving mapping and template encoding. Journal of Information Security and Applications, 93, p.104126.

[14] Maurya, P.K., Sandhya, M., Prasad, I.H. and SuryanarayanaRaju, N.V., 2025. Enhancing fingerprint template security using elliptic curve cryptography and fuzzy vault encoding. Journal of Information Security and Applications, 94, p.104243.

[15] Zhang, L., Chen, X. and Liu, P., 2025. Transformer-based biometric feature representation learning for secure authentication systems. Neural Networks.

[16] Wang, T., Huang, Y. and Zhao, F., 2025. Lightweight deep learning architecture for cloud-assisted biometric authentication. Future Generation Computer Systems.

[17] Chen, M., Liu, S. and Zhang, Y., 2025. Secure cloud biometric authentication using encrypted template matching and deep learning. Information Sciences.

[18] Gupta, A., Sharma, R. and Kumar, N., 2025. Hybrid attention-based convolutional learning framework for biometric identification and privacy preservation. Applied Intelligence.

[19] Liu, X., Zhao, Y. and Chen, H., 2025. Deep neural network based privacy preserving biometric recognition using adaptive feature transformation. Knowledge-Based Systems.

[20] Wickramaarachchi, W.U., Zhao, D., Zhou, J. and Xiang, J., 2024. An effective iris biometric privacy protection scheme with renewability. Journal of Information Security and Applications, 80, p.103684.

[21] Khan, M.S., Li, H. and Zhao, C., 2024. Deep Secure PalmNet: A novel cancelable palmprint template protection scheme with deep attention net and randomized hashing security mechanism. Computers & Security, 142, p.103863.

[22] Vallabhadas, D.K., Sandhya, M., Reddy, S.D., Satwika, D. and Prashanth, G.L., 2024. Biometric template protection based on a cancelable convolutional neural network over iris and fingerprint. Biomedical Signal Processing and Control, 91, p.106006.
[23] Zheng, Q., Xiang, J., Hao, R., Zhang, X., Liao, S. and Zhao, D., 2024. A cancellable iris template protection scheme based on inverse merger and Bloom filter. Journal of Information Security and Applications, 85, p.103849.
[24] Dong, X., Park, J., Jin, Z., Teoh, A.B.J., Tistarelli, M. and Wong, K., 2024. On the security risk of pre-image attack on cancelable biometrics. Journal of King Saud University - Computer and Information Sciences, 36(5), p.102060.
[25] Khan, M.S., Zhong, T., Zhou, F. and Li, H., 2024. Deep attention networks for privacy-preserving biometric template protection and authentication. Computers & Security.
[26] Li, Y., Zhang, H. and Wang, J., 2024. Attention-based convolutional neural networks for robust iris recognition under unconstrained environments. Pattern Recognition Letters.
[27] Kumar, R. and Singh, A., 2024. Deep feature fusion-based iris recognition using convolutional neural networks and attention learning. Multimedia Tools and Applications.
[28] Zhao, M., Xiang, J. and Zhao, D., 2024. Deep feature representation and secure transformation techniques for privacy-preserving iris recognition. Biomedical Signal Processing and Control.
[29] Rahman, M., Islam, S. and Lee, Y., 2024. Cloud-based biometric authentication framework using encrypted deep feature matching. Computers and Electrical Engineering.
[30] CASIA Iris Image Database. CASIA-IrisV3-Interval and CASIA-IrisV4-Lamp Dataset. Available: https://hycasia.github.io/dataset/casia-irisv4/