INTERNATIONAL JOURNAL OF Telecommunications
AIR DEFENSE COLLEGE

Advanced Iris Recognition Framework using Efficient Net And Fully Homomorphic Encryption with Bloom Filters

Citation: Fouda , E.; Elsaid , S.; Abdelhay , E.; Mohamed,M.
Inter. Jour. of Telecommunications, ***IJT'2025****, Vol. 05, Issue 02, pp. 1-22, 2025.*
Doi: 10.21608/ijt.2025.393351.1116
Editor-in-Chief: Youssef Fayed.
Received: 11/06/2025.
Accepted date: 10/08/2025.
Published date: 10/08/2025.

Eslam Mahmoud Fouda[1,*], Shaimaa Ahmed Elsaid [2], Ehab H. Abdelhay[3], and Mohamed Abdel-Azim Mohamed[5].

[1] Electronics and Communications Department, Faculty of Engineering, Mansoura University, Mansoura, Egypt, eslamfouda138@gmail.com.
[2] Department of Computer Engineering, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj, Saudi Arabia. 3 Electronics and Comm. Dep., Faculty of Engineering, Zagazig University, Egypt. sh.ahmed@psau.edu.sa.
[3] Department, Faculty of Engineering, Mansoura University, Mansoura, Egypt. Faculty of Engineering, Mansoura National University, Egypt. ehababdelhay@mans.edu.eg.
[4] Electronics and Communications Department, Faculty of Engineering, Mansoura University, Mansoura, Egypt. mazim@mans.edu.eg.

* Correspondence: eslamfouda138@gmail.com.

Abstract: Iris recognition systems have emerged as a pivotal biometric technology, providing high reliability for secure authentication systems, especially in the post-pandemic era where contactless and hygienic identification is critical (e.g., during COVID-19). The system uses EfficientNet-B7 to accurately extract features and encrypts them using Fully Homomorphic Encryption (CKKS) enabling secure matching without decrypting sensitive data. To store templates quickly and privately, the encrypted features are indexed via an enhanced Bloom filter with Homomorphic hashing, ensuring secure membership Verification. This framework was evaluated using CASIA-Iris-Syn and IITD-Iris-V1, achieving an accuracy of 99.98% (EER of 0.001) and 98.98% (EER= 0.024), respectively, outperforming existing methods in terms of performance and security. By combining EfficientNet-B7 indexing, FHE, and Bloom Filter, this work bridges the gap between high-performance biometrics and strict data protection, making it suitable for use in healthcare, financial, and national identity systems.

Keywords: Iris Recognition, Data Security, Authentication System, Convolutional Neural Network (CNN), EfficientNet-B7، Fully Homomorphic Encryption (FHE), Bloom Filter (BF).

1. Introduction

Biometric identification technology is a critical field in computing and security sciences, enabling the verification of individuals' identities based on unique biological and physiological characteristics, particularly iris patterns. These systems are now widely integrated into various applications, including banking, smartphones, and airport security [1]. However, despite their increasing adoption, improving the accuracy and security of biometric data remains a major concern. Unlike traditional credentials, biometric information cannot be easily revoked or modified once compromised. This poses ongoing security risks to users. A prominent example of this occurred in 2019, when the BioStar 2 system operated by Suprema, responsible for

managing biometric data such as fingerprints and facial recognition was compromised [2]. This breach exposed approximately 27.8 million records, compromising sensitive information, including fingerprints, facial images, unencrypted passwords, personal details, and access credentials.

1.1 Problem Statement

Traditional manual feature extraction methods have evolved significantly over the years. The integration of deep learning techniques has led to significant improvements. However, ensuring the security and privacy of biometric data templates remains a pressing challenge that requires continuous innovation.

- Deep learning methods, especially end-to-end approaches, require significant computing time and resources [3].
- Some security systems are becoming increasingly vulnerable, facilitating unauthorized access to sensitive biometric data. Conversely, while implementing robust security mechanisms enhances protection, it often poses challenges in maintaining an optimal balance between system performance and security complexity [4].

1.2 Our Contribution

To address these challenges, this study proposes a secure and efficient iris recognition framework that combines deep learning and advanced cryptographic techniques. Specifically, we use the EfficientNet-B7 architecture a non-end-to-end approach to extract features accurately [5]. The extracted features are then protected using FHE [6] and efficiently regularized via BF [7], before being stored in a database. This approach enhances the accuracy and security of the system while reducing computational costs.

The rest of this paper is organized as follows: Section 2 provides an in-depth review of the relevant literature, highlighting existing approaches and identifying key research gaps. Section 3 provides a detailed explanation of the proposed secure iris recognition framework, including its structural components and the methodologies it relies on. Section 4 outlines the experimental setup, datasets, and evaluation metrics, followed by a comprehensive performance analysis and comparison with state-of-the-art systems. Finally, Section 5 concludes the paper by summarizing the key contributions and discussing potential directions for future research.

2.Related Work

Numerous studies have pioneered innovative methodologies to authenticate and safeguard biometric data against threats such as template reversal, theft, and unauthorized access. These approaches have integrated deep neural networks, cryptographic techniques, and hybrid frameworks to ensure robust security while maintaining high recognition accuracy.

Soliman et al. (2018) [8] engineered a chaos-based iris recognition system using Comb Filters on CASIA-Iris-V3-Interval, achieving 99.08% accuracy through linear transformations that ensured irreversibility and renewability. However, its security model was fundamentally undermined by PIN dependencies, creating critical revocability weaknesses despite its lightweight architecture.

Chen et al. (2018) [9] pioneered the Deep Secure Quantization (DSQ) framework on CASIA-v4-Interval, merging CNN feature extraction with secure binarization to achieve 98.7% accuracy while preserving inter-class separability. The approach's prohibitive computational demands and mandatory retraining requirements for new enrollments severely constrained practical scalability.

Wickramaarachchi et al. (2020) [10] devised a cancelable system using 1D Log-Gabor wavelets and block-wise transformations on CASIA-Iris-V1/V4, attaining 0.18% EER through XOR-based distortion. Methodological fragility emerged from block-size sensitivity, irreversible information loss during thresholding, and significant computational latency in key operations.

Sudhakar et al. (2020) [11] formulated a cloud-based revocable framework for multi-modal biometrics (IITD/MMU), achieving 0.04% EER through two-stage transformations. Operational viability was compromised by excessive cloud dependency costs, inherent key management vulnerabilities, and computational complexity.

Sandhya et al. (2024) [12] implemented IFO hashing with Partial Sort on CASIA-v3, demonstrating 97.3% recognition via P-rank Hadamard products. The system exhibited unvalidated renewability capabilities and impractical quadratic computational overhead during modulo threshold operations.

Punithavathi et al. (2022) [13] enhanced LDA with random permutations across UBIRIS/IITD datasets, maintaining recognition efficacy under quality variations. Security relied on vulnerable PIN-based mechanisms while demonstrating environmental fragility through unrecoverable accuracy degradation (EER >5.43%) under suboptimal conditions.

Salama et al. (2022) [14] architected a multi-layer encryption framework (DRPE/Bakerian maps) on ORL, achieving 0.0035 EER through watermarking and SVD. Deployment feasibility was restricted by foreign-key management risks and prohibitive computational costs for chaotic operations.

Farooq et al. (2022) [15] developed an optimized CNN pipeline with variance-aware loss on CASIA-Iris-Interval V4/MMU, reducing storage by 40% while maintaining 99.1% accuracy. Resource efficiency claims were contradicted by exponential computational requirements and noise amplification vulnerabilities during embedded transformations.

Abdellatef et al. (2023) [16] created a CNN-based system with bio-convolutional layers across four datasets, sustaining >95.48% accuracy during revocation. Implementation complexity escalated system integration challenges, increasing attack surfaces without compensating security enhancements.

Singh et al. (2023) [17] proposed a hybrid CNN with embedded non-invertible transformations (IITD/MMU1), achieving 98.9% accuracy. Generalizability concerns persisted due to environmental context sensitivity and narrow validation across heterogeneous datasets.

Wu et al. (2025) [18] established a three-party FHE model using enhanced CS-LBP on CASIA-IrisV4, attaining 0.990 AUC through BGV-encrypted comparisons. Distributed architecture introduced critical latency from homomorphic computation overhead and mandatory cloud infrastructure dependencies.

2.1 Literature Gap

Despite significant progress, current biometric template protection systems face several limitations. Many approaches suffer from significant computational complexity, making them unsuitable for immediate or large-scale deployment. Systems that rely on secret keys introduce single points of failure a key leak compromises the entire system. Additionally, some encryption methods based on randomness or chaos may be vulnerable to brute force or dictionary attacks due to limited key space. Furthermore, some frameworks require significant computational resources, increasing operational costs and limiting endpoint compatibility.

Table 1 provides a comparative summary of existing approaches, including their strengths, weaknesses, and performance on benchmark datasets.

Table 1. An overview of the most recent biometrics authentication and template protections approaches.

Ref. NO	Year	Authors	Methodology	Iris Dataset	Performance Metrics	Limitations
[8]	2018	Soliman et al.	Gabor Filters + Chaotic Map Encryption	CASIA-Iris-V3-Interval	Accuracy: 99.08% EER: 1.17%	Dependence on PIN weakens security and revocability.
[9]	2018	Chen et al.	Deep Secure Quantization (DSQ) + CNN Features	CASIA-v4-Interval	Accuracy: 98.7% EER ≤1%	High computational cost, retraining needed for new users.
[10]	2020	Wickramarachchi et al.	Block-wise Feature Transformation + 1D Log-Gabor + XOR Key Operation	CASIA-Iris-V1	GAR:99.43% FAR=0.01% EER: 0.18%	Block-size sensitivity, key management, information loss and computational latency.
[11]	2020	Sudhakar et al.	Revocable Biometric Framework (Deep Learning)	MMU& IITD and FV-USM	MMU: AUC=0.92, EER=0.14 IITD: AUC=0.98, EER=0.04 ،FV-USM: AUC=1.00,EER=0.01	High cost of cloud services. High computational complexity, cloud dependency, key management challenges.
[12]	2021	M. Sandhya et al	the Indexing-First-One (IFO) hashing technique	CASIA-v3	Recognition Rate: 97.3%	no renewability tests, high computational overhead.
[13]	2022	Punithavathi et al	Linear Discriminant Analysis (LDA)-with random permutation	ORL, UBIRIS and IITD	EER =4.21% on ORL, 5.43% on UBIRIS, and 6.52% on IITD	PIN-based, no multi-cancel testing, sensitive to image quality.
[14]	2022	GM Salama et al	Double Random Phase Encoding (DRPE) and chaotic Baker Map with watermarking	ORL and MIT	EER 0.0035, FAR 0.0011, FRR 0.0017	high computational costs, reliance on a foreign key

[15]	(2022)	Farooq et al.	Optimized CNN Architecture + Variance-Aware Loss Function	CASIA-Iris-Interval V4 & MMU	Accuracy: 99.1% Storage Reduction: 40%	High computational costs, sensitivity to noise.
[16]	(2022)	E. Abdellatef et al	a (CNN) with a bio-convolution layer	(LFW, FERET, IITD, and CASIA-IrisV3)	recognition rates of 99.15%, 98.35%, 97.89%, and 95.48%	Complex system integration
[17]	(2023)	Singh et al.	Hybrid CNN with Integrated Secure Transformation Layers	IITD & MMU1	Accuracy: 98.9% EER: 0.8%	Based on limited data, and sensitivity to environmental context.
[18]	(2025)	Wu et al.	FHE-Enabled Processing + Enhanced CS-LBP Features	CASIA-IrisV4	accuracy of 97.0%, recall of 96.5%, F1-score of 96.7%, and an AUC of 0.990	High computational costs and Requires cloud computation

Unlike previous methods that rely on secret keys or computationally expensive encryption, the proposed framework leverages FHE and Bloom filters to provide secure, scalable, and reversible iris recognition with minimal compromise to speed or accuracy.

3. The proposed system

This section outlines the proposed methodology, which is systematically structured into two principal stages: preprocessing and feature extraction, data security during the enrollment phase, and the verification phase as shown in Fig. 1. Each stage incorporates meticulously designed procedures aimed at ensuring the secure processing and reliable verification of biometric information. The following subsections provide a detailed overview of each stage along with their constituent components.

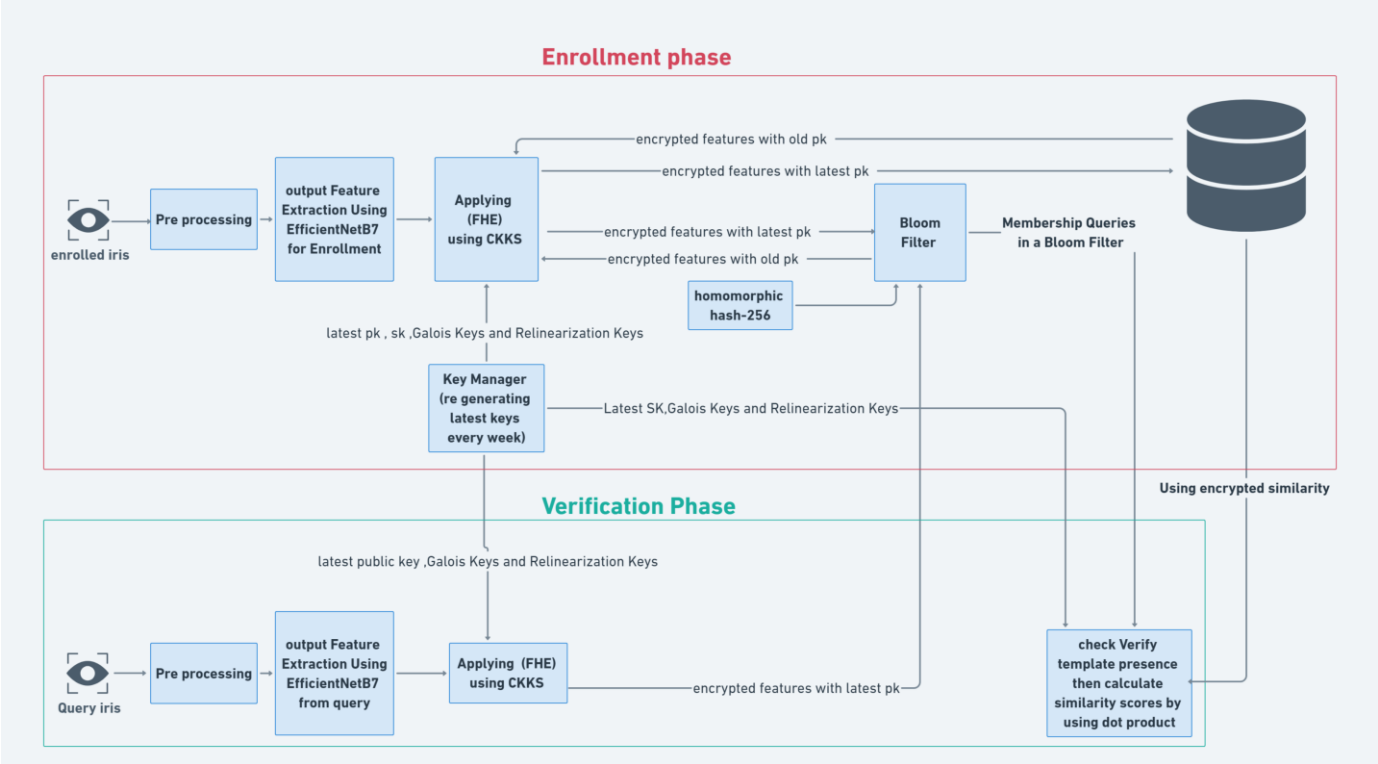

Fig. 1 Enrollment and verification phases Block diagram

3.1 ENROLLMENT PHASE

3.1.1 preprocessing and feature extraction

To improve image quality before feature extraction, an effective image preprocessing pipeline has been created, as shown in Fig. 2. This pipeline is a series of linked operations designed to improve edge clarity, reduce noise, optimize contrast, and fine-tune texture details, all of which contribute to a more accurate and efficient extraction of iris characteristics. Each preprocessing step and its significance are explained in depth in the section that follows.

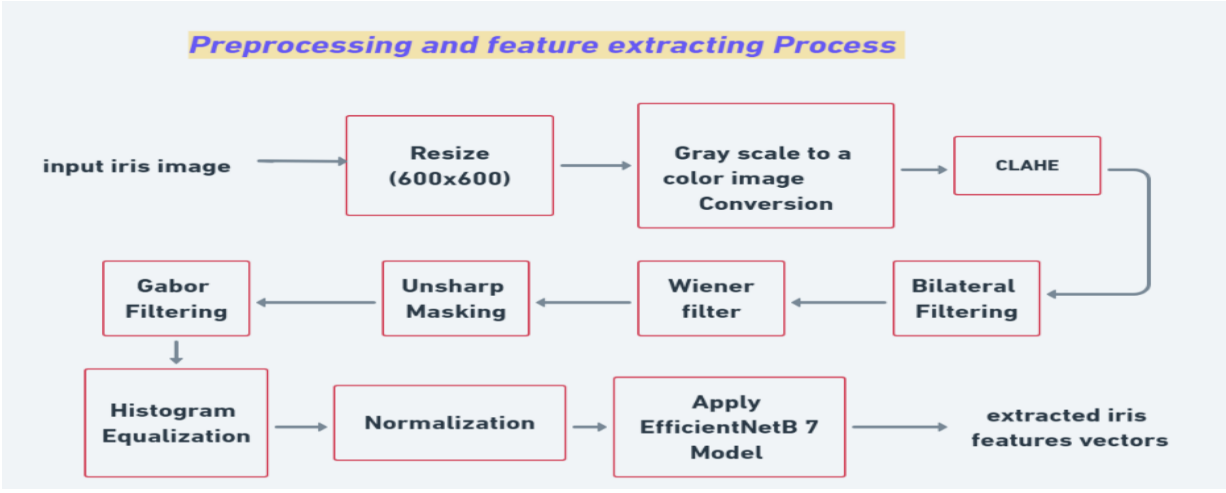

Fig. 2 Preprocessing and feature extraction diagram

a. The input image is resized to a standardized resolution of 600×600 pixels, aligning with the input size requirements of most deep learning architectures. This normalization step ensures consistency across all samples and compatibility with fixed-dimension model inputs.

b. Generate a color image with three color channels (RGB) from grayscale. We reject any additional channels, including alpha channels, from the image and convert it to RGB with just three channels. This ensures that the image is prepared for use with procedures that call for three color channels.

c. To improve contrast, particularly in images with poor lighting, apply CLAHE (Contrast Limited Adaptive Histogram Equalization) [19] to the image's luminance channel (L). This technique enhances contrast in low-contrast areas while reducing the amplification of noise in uniform zones.

d. Use a bilateral filter [20] with precise settings for density and spatial smoothing. This filter is perfect for maintaining small details in texture-rich images since it reduces noise but retains edge integrity.

e. To minimize salt and pepper noise while maintaining edge sharpness, smooth the image with a Wiener filter with a kernel size of 5 [21].

f. To improve edges and highlight parts important to analysis, including borders in iris patterns, use unsharp masking [22], which involves removing a blurred version of the picture from the original and combining the results.

g. Use Gabor filters [23] with particular frequencies and directions to extract texture information. This is done in order to capture structures and patterns that are crucial for extracting biometric features, including ridges or circular textures in the iris.

h. The global histogram equation [24] can be utilized to enhance the overall contrast.

i. Adjust the values of pixels to correspond with the model's expected range (for example, scaling values to [0, 1] or [-1, 1]).

After enhancing the input images through the proposed preprocessing pipeline, it becomes well-prepared for feature extraction using the EfficientNet-B7 architecture.

3.1.2 Feature extractions using EfficientNet-B7

EfficientNet-B7 is an advanced convolutional neural network (CNN) architecture designed to strike an optimal balance between computational efficiency and recognition accuracy. It is particularly well-suited for visual recognition tasks such as image classification and biometric feature extraction [5]. The network employs a compound scaling method that adjusts depth, width, and input resolution, providing high performance with fewer parameters and reduced computational cost.

The architecture consists of seven key blocks (illustrated in Fig. 3), each incorporating Mobile Inverted Bottleneck Convolutions (MBConv) and Squeeze-and-Excitation (SE) modules. These features enable EfficientNet-B7 to extract hierarchical and discriminative features while minimizing memory usage, making it ideal for deployment in resource-constrained environments such as embedded and mobile systems.

For feature extraction, the classification head is removed, and a Global Average Pooling (GAP) layer is added after the final convolutional block [25]. This configuration produces a compact, high-dimensional feature vector that captures the crucial spatial and textural details of the iris image.

Given a preprocessed iris image $I \in \mathrm{R}^{600\times600\times3}$, the model generates a feature vector $V \in \mathrm{R}^{2560}$ using the following operation:

$$V = \text{GAP}\big(\text{EfficientNet} - \text{B7(I)}\big) \qquad (1)$$

Where, v represents the extracted feature vector, which is both compact and discriminative. This vector is then normalized and utilized as the biometric template for secure enrollment and authentication [5].

Additionally, fine-tuning the model on iris-specific datasets can further improve the discriminative power of the features, enhancing the model's ability to distinguish between individuals as illustrated in Fig. 4.

This approach ensures the features are not only accurate but also maintains privacy, enabling secure storage and matching through encryption techniques like FHE and Bloom Filter indexing

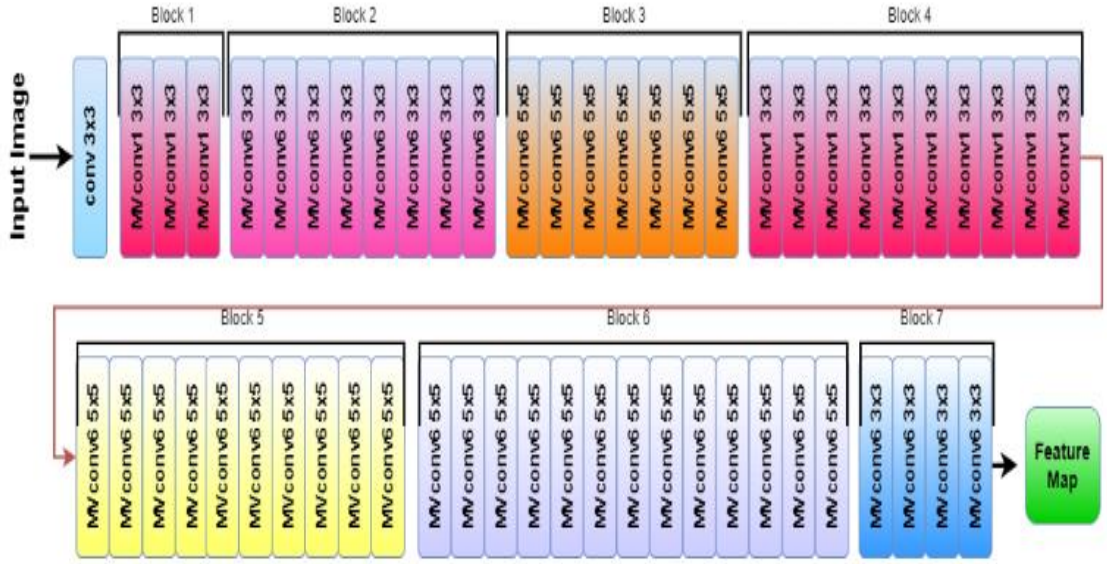

Fig. 3 Architecture of EfficientNet-B7 (Cited by [26])

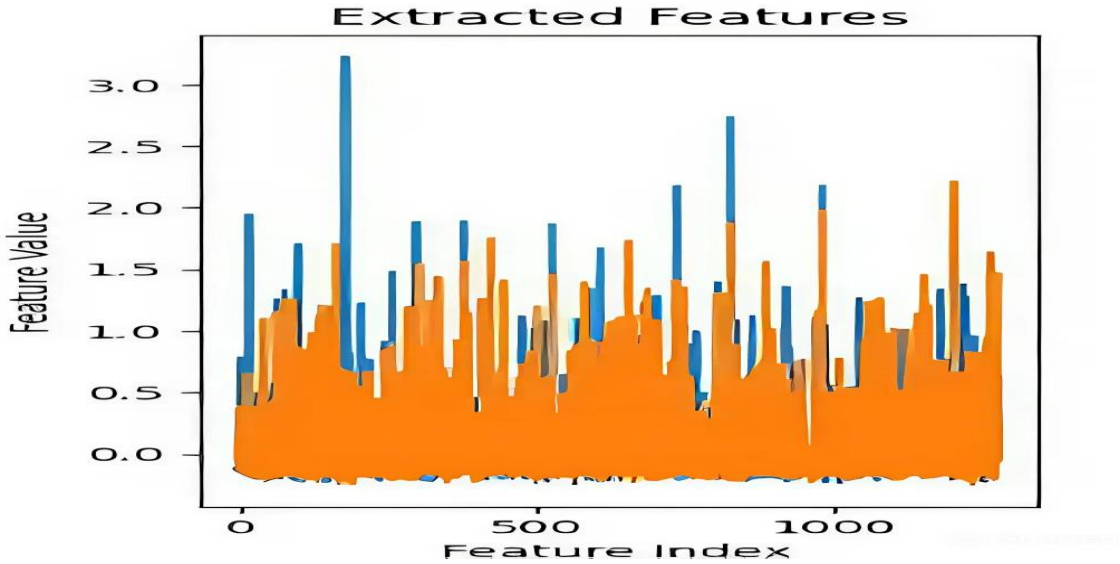

Fig. 4 Comparison of Extracted Feature Values for Two Different Persons' Iris Datasets Without Applying a Security Phase

After completing feature extraction, it is time to implement the biometric template security phase. This phase aims to enhance the security of biometric data by applying advanced encryption methods, specifically the

CKKS algorithm, to the feature vectors extracted using EfficientNet-B7. The encryption is implemented using the Tensor Secure Encrypted Arithmetic Library (Tenseal), a specialized framework for integrating encryption with 2560 deep learning outputs. The resulting encrypted features are then securely stored in the Secure Biometric File (BF).

Applying CKKS

FHE is an encryption method that enables arithmetic operations on encrypted data without decryption. This innovative approach provides a robust privacy solution for machine learning and cloud computing environments, allowing secure processing of sensitive data while maintaining confidentiality. Among various FHE schemes, the Cheon-Kim-Kim-Song (CKKS) scheme, available through the TenSEAL library, is specifically designed for secure machine learning applications [28]. CKKS simplifies mathematical operations on plaintexts, distinguishing it from other asymmetric encryption methods limited to integer operations. It supports floating-point arithmetic and enables approximate operations like addition, multiplication, and scaling. This is achieved by encoding input floating-point numbers and scaling them using a predetermined scaling factor, effectively converting them to integers. The encryption environment was configured using the TenSEAL library as shown below:

3.1.3.1 Creating a Cryptographic Context:

The first step creates a cryptographic context using the CKKS algorithm, enabling the system to perform operations on encrypted data and generate necessary keys. This includes:

- Poly modulus degree: Specifies the polynomial degree (32768), chosen to balance computational accuracy with memory efficiency for complex mathematical operations.
- Coeff mod bit sizes: Determines coefficient precision (60 bits for first/last, 40 bits for middle coefficients) balancing speed and accuracy.
- Relinearization keys: Simplify encrypted data after multiplication operations.
- Galois keys: Enable advanced mathematical operations like rotation on encrypted data without decryption.
- Public/Private keys: Used for encryption and decryption [29].

3.1.3.2 Features encryption process:

- After performing iris feature extraction using EfficientNet-B7, the resulting vector represents the unique texture patterns of the iris and can be expressed mathematically as:

$$v = [v_1, v_2, \ldots, v_{2560}] \in \mathbb{R}^{2560} \qquad (2)$$

- Floating-Point to Integer Conversion Since the CKKS encryption scheme operates on integers (not floating-point numbers), the first step is to scale the real-valued features using a scaling factor Δ . This ensures compatibility with homomorphic operations while preserving numerical precision.

$$\mu(X) = \Delta \cdot v(X) \qquad (3)$$

Where:

$v(X)$: The original feature vector (e.g., from EfficientNet-B7).

Δ : 2^{20} is the scaling factor.

$\mu(X)$: The scaled integer version of the vector.

Example

$$v = [0.12, -0.45, 0.03, \ldots, 0.89] \in \mathbb{R}^{2560} \qquad (4)$$

after Scaling

$$\mu(X) = \Delta \cdot v = 2^{20} \cdot v = [125829, -471859, \ldots, 934560] \in \mathbb{Z}^{2560} \qquad (5)$$

- Encryption Using the CKKS

Once the feature vector has been converted into an integer polynomial form, it is encrypted using the CKKS algorithm. The encryption generates a ciphertext Ct consisting of two components: C_0andC_1 , calculated as:

$$C_t = C_0, C_1 \qquad (6)$$

$$C_0 = b \cdot r + \mu(X) + \text{e} \bmod q \qquad (7)$$

$$C_1 = -a \cdot r + e' mod\ q \qquad (8)$$

Where:

- a and b: Polynomials derived from the public key.
- r : A randomly generated polynomial used to blind the message and provide semantic security.
- q: The modulus, which defines the valid range of values in the ciphertext space.
- $\boldsymbol{C_t}$: ($\boldsymbol{C_0}$, $\boldsymbol{C_1}$): represents the ciphertext, which consists of two polynomials resulting from the encryption process.
- e , e′ : Noise/error terms added for semantic security.
- The final encrypted representation is:

This encrypted representation can only be decrypted using the corresponding secret key, ensuring that the biometric data remains secure throughout its lifecycle.

Size of 2 polynomials × 32,768 coefficients (C_t) ≈4MB total

After encryption, mathematical operations—including addition, multiplication, and rotation can be applied directly to the encrypted data using specialized keys, such as Galois keys for rotation and linear keys to streamline post-operation data (e.g., after multiplication). The encrypted features are then forwarded to two places BF for fast reply on query and the other to database further processing

3.1.4 Using BF

A **Bloom filter** is a probabilistic data structure used to test whether an element is a member of a set. It is a space-efficient technique that allows for fast membership tests, but it may produce false positives (indicating an element is in the set when it is not) but never false negatives (missing an element that is

actually in the set [30]. Figure 5 illustrates the workflow from a search item to a result via hash functions and the bit array.

- **Core Components:**
  - **Bit Array (BF):** A binary vector of size m, initialized to zero:$BF = [0,0,\dots,0](length\ m)$
  - **Hash Functions:** A set of k independent hash functions $\{h1, h2, \dots, hk\}$, where each hi maps an input element to a position in BF: $hi: Input \rightarrow \{0,1,\dots,m-1\}$

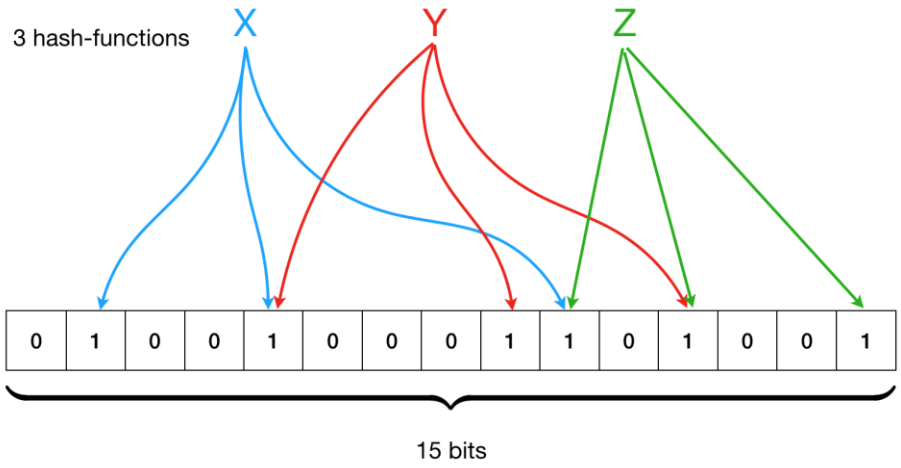

Fig. 5 An example for Bloom Filter Workflow

- **Key Characteristics of the Bloom Filter:**
  - **Space Efficiency:** Encodes set membership using $O(m)$ bits, significantly reducing storage overhead (e.g., 1 MB can represent ~1 million items).
  - **Constant-Time Operations:** Insertion and querying exhibit $O(k)$ complexity (effectively $O(1)$ for fixed k), ideal for latency-critical systems.
  - **Probabilistic Accuracy:**
    - **No false negatives:** If: $x \in Set,\ Query(x) = True$
    - **Controlled false positives:** $P(false\ positive) \approx \left(1 - e^{-\frac{kn}{m}}\right)^k$ (**9**)

Where:
m: total number of bits in the bit array.
n: number of inserted elements.
k: number of hash functions used.

  - **Privacy Preservation:** Stores only hashed indices; original data cannot be reconstructed from the BF.

- Integrating the Bloom Filter with CKKS Encryption

In the described biometric security system, the Bloom Filter is cleverly integrated with the CKKS (Cheon-Kim-Kim-Song) homomorphic encryption scheme. This combination leverages the privacy ensures of CKKS and the speed/efficiency of the Bloom Filter for an initial screening process.

- Workflow:
  - Recording Phase (Storing Encrypted Features):

To create a fingerprint suitable for the Bloom filter, a technique called homomorphic-256 hashing is applied to the ciphertext C_t. This type of hash is specifically chosen for its consistency with the encrypted data and, more importantly, because it tends to preserve the similarity between the original input vectors [31]. This means that similar cryptographic biometric features will produce a similar hash. Standard hashing algorithms such as SHA-256 do not have this property. Implementing Bloom filter hash functions, the output of the homomorphic hashing step is then passed through independent conventional hash functions $\{h1, h2, \dots, hk\}$

- For each hash function i (where i = 1 to k):
- Calculate index: $index_{\mathrm{i}} = h_{\mathrm{i}}(HomomorphicHash(C\_t))\ mod\ m$
- Where m is the size of the Bloom filter bit array
- Set corresponding bits in (BF) to 1:

$$BF[index_1] = 1, BF[index_2] = 1, \dots, BF[index_{\mathrm{k}}] = 1 \qquad (10)$$

This operation effectively stores a secure and concise representation of the encrypted biometric data in the BF.

To mitigate false positives while maintaining security ensures, a threshold-based verification approach is applied. For example, requiring 90% of the computed bit positions to be set strikes a balance between reducing false positives and maintaining acceptable false negative rates. The system uses a 10,000-bit BF with SHA-256 hash, designed to store 1,000 cryptographic blocks, achieving an improved false positive rate of approximately 1.74%. This configuration reduces the average verification time from 0.7 seconds (full similarity calculation) to 0.1 milliseconds (Bloom filter check), representing a 7,000-fold improvement in performance.

3.1.5 Keys Management:

Encryption keys are considered expired after one week. Using the old keys, the previously encrypted features are decrypted first to perform the update. The newly generated keys are then used to re-encrypt the features. Both the old encrypted features and the expired keys are deleted according to the renewal principle. To ensure synchronization with the updated keys during the registration process, new keys are securely sent to users during the request phase. Using the old keys to decrypt the previously encrypted feature, the equation for decryption is:

$$v = [(C_0 + C_1 \cdot sk + e) mod q]/\Delta \qquad (11)$$

This equation reconstructs an approximation of the original message v by combining the components of the ciphertext with the private key, reducing the result modulo q, and finally dividing by the scaling factor Δ to recover the plaintext in its expected numeric range‹ after decrypting the features, the system generates new keys and re-encrypts the features using them, as described in Sections 3.1.3.4 and 3.1.3.2. The encrypted item is then stored in the BF and DB.

3.2 *Verification Phase*

When a new biometric sample is entered for verification, the same steps as in the registration phase are performed: feature vectors are extracted, features are encrypted using the same CKKS parameters, and the output is fed into a Bloom filter. The verification phase consists of two verification processes: the first using a Membership Queries in a Bloom Filter and the second using encrypted similarity function to ensure fast and secure comparison.

3.2.1Membership Queries in a Bloom Filter:

To verify the presence of an encrypted feature in a Bloom filter, the same homomorphic hash transform is applied to the Bloom filter and the encrypted data in the query. This results in identifying the corresponding bit positions in the Bloom filter:

- Positive probability: When all or most of the bits in the computed positions are set to 1, this is considered a likely indication of the presence of the encrypted feature in the filter (with the possibility of false positives).
- Negative certainty: If less than 90% of the bits in the specified positions are set to 1, This confirms that the feature is not present (or enrolled) in the filter.

3.2.2Using encrypted similarity function:

The calculate encrypted similarity function provides a secure and confidential method for determining the similarity of two hashed feature vectors [32]. This function maintains data confidentiality throughout the calculation process using the encrypted data. This method, its mathematical basis, and its practical benefits will be explained in detail below.

3.2.3Mathematical Foundations of Cosine Similarity

In machine learning and data analysis, cosine similarity—a measurement of the cosine of the angle between two vectors in a dimensional space is frequently used to evaluate how similar two vectors are, despite their magnitude [33]. The following is the formula for the cosine similarity between encrypted vectors v_1 and v_2:

$$CosSim(v1, v2) = \frac{Enc(v_1 \cdot v_2)}{Enc(\| v_1 \|_2) \cdot Enc(\| v_2 \|_2)} \qquad (12)$$

Where:

- $\| v_1 \|_2 \; and \; \| v_2 \|_2$: represent the Euclidean norms (magnitudes) of vectors v_1 and v_2 , respectively.
- $v_1 \; and \; v_2$: denotes the dot product of the two vectors.

The encrypted features are kept secret during the computation since these operations (dot product and Euclidean norm) are applied directly to the encrypted features in homomorphic encryption, without the need for decryption.

3.2.4Steps of the Process

- **Step 1: Compute the Encrypted Dot Product**

TenSEAL's dot product function is used to immediately calculate the dot product between the two encrypted vectors from DB and query after proceeding Membership Queries in a Bloom Filter, v_1 and v_2 ($v_1 \cdot v_2$), on the encrypted feature. Similarly, the squared magnitudes of the vectors are computed by taking the dot product of each vector with itself ($v_1 \cdot v_1$ and $v_2 \cdot v_2$)

Because these computations are homomorphic, the data is encrypted during the entire process.

- **Step 2: Decrypt the Intermediate Results**

The private key is used to decrypt the encrypted results after the dot product has been calculated.$v_1 \cdot v_2$ (the product of the two vectors' dot values.) $v_1 \cdot v_1$ and $v_2 \cdot v_2$ (the vectors' squared magnitudes).

- **Step 3: Compute Cosine Similarity**

The square roots of the decrypted squared magnitudes ($v_1 \cdot v_1$ and $v_2 \cdot v_2$) are used to calculate the Euclidean norms $\|v_1\|$ and $\|v_2\|$. After that, cosine similarity is computed using the previously stated formula. This part will take place after the data has been decrypted since homomorphic operations like division and square roots are computationally costly.

- **Step 4: Decision Criteria**

A predetermined threshold (such as 0.9) is compared to the calculated cosine similarity score. Vectors are considered to belong to the same person if the similarity score is higher than the threshold, and vectors are considered to belong to two different people if the similarity score is lower.

4. Materials and Results

To implement the proposed iris recognition system, two widely recognized public databases were employed: CASIA-Iris-Syn [34] and IITD-Iris-V1 [35]. These datasets offer distinct characteristics that allow for comprehensive evaluation under both synthetic and real-world conditions. All experiments were conducted using the Kaggle platform [36], which provided a scalable and flexible computing environment suitable for deep learning and cryptographic operations.

4.1 Datasets and Implementation Details

For Dataset Description, Table 2 summarizes the key features of the selected databases:

Table 2. Characteristics of the Databases Used

Field	CASIA-Iris-Syn	IITD-Iris-V1
Number of Images	10,000	10,000
Individuals **Number**	1000	225
Dimensions (Pixels)	640 × 480	320 × 240
Type of Images	Synthetic (Generated by Computer)	Natural Near-Infrared (NIR)
Extension	.jpg	.jpg
Implementation Platform	Kaggle	

4.2 Data Partitioning Protocol

To ensure robustness and prevent data leakage during model training and testing, a subject-specific partitioning strategy was adopted:

- For CASIA-Iris-Syn, each subject contributed 10 images. Eight images per subject (80%) were used for fine-tuning, while the remaining two images (20%) formed the test set.
- For IITD-Iris-V1, where the number of images per subject varied, 80% of each subject's images were allocated for training/fine-tuning, with the remaining 20% reserved for testing.

4.3 Experimental Setup:

The implementation followed the configuration detailed in Table 3.

Table 3. Experimental Setup Details

Component	Configuration details
Image Standardization	Resized images 600×600 pixels
EfficientNet-B7	Pre-trained on ImageNet; fine-tuned for 50 epochs (Adam optimizer, LR=1e-4, batch size=32)
Encryption	CKKS via TenSEAL (poly modulus degree=32,768; scaling factor=2^{20}; coeff modulus bits=[60,40,60]).
Bloom Filter (BF)	Size=10,000 bits,k=4 homomorphic hash-256 hash functions, False Positive rate=1.74%.
Hardware/Software	Platform: Kaggle (Python 3.10, PyTorch 2.0, TenSEAL 0.3.12).

4.4 Evaluation Metrics

The evaluation metrics (FAR, FRR, EER, precision, specificity, recall, F1 score, and accuracy) were calculated by comparing the similarity scores between images of the same individual (positive scores) and images of different individuals (negative scores) using specific threshold (e.g., 0.9).

4.5 Computational Performance and Execution Time

Due to the integration of computationally intensive operations such as encryption and homogeneous operations, understanding execution time is essential for practical application. Table .4 shows Average Execution Times for Processing a Single Iris Image

Table 4. Average Execution Times for Processing a Single Iris Image

Loading the image	Preprocessing the images	Feature Extraction	Encrypting the features	Adding to BF	Check in BF	Calculating Encrypted Similarity	Total Execution Time
4.15 milliseconds	44.25 ms	57.75 ms	26.80 ms	0.2 ms	0.1ms	623.7 ms	756.95ms

The most time-consuming stage was the encrypted similarity calculation, primarily due to the complexity of homomorphic computations.

4.6 Evaluation of the proposed system performance on CASIA-Iris-Syn.

The proposed method performs extremely well with a very low rate of false classifications, as shown by the CASIA-Iris-Syn dataset, which has an impressively high accuracy of 0.9980 and a very low error rate of 0.001. With a specificity of 0.999, the method is effective at reducing false positives. With an F1-score of 0.9987, which indicates superior overall performance, the suggested system records a high recall of 0.9985, indicating that it rarely misses real matches. It achieves a good balance between recall and precision. Fig. 6, 7 displays the performance analysis of the suggested model on the CASIA-Iris-Syn dataset. A performance comparison between the proposed one and other models on CASIA-Iris-Syn is shown in Table 5. Among all the models compared, the proposed method has the highest accuracy (.9998), exceeding [37] (.9569). This shows that samples were correctly classified with impressive precision. Its score of .99880 put it far ahead of the ViT-based models [38] (.9424) and [37] ViT-L16: .9608, ViT-L32: .9465]. With an F-score of .99870, the proposed approach exceeds ViT-L16 (.9403) and ViT-L32 (.9388), having the optimum balance between Precision and Recall. The suggested method's .99850 recall indicates remarkable true positive detection, exceeding other models such as ViT-L16 (.9569) and [38] (.9407). In terms of accuracy, precision, F-score, and recall, the proposed method performs better than any other model.

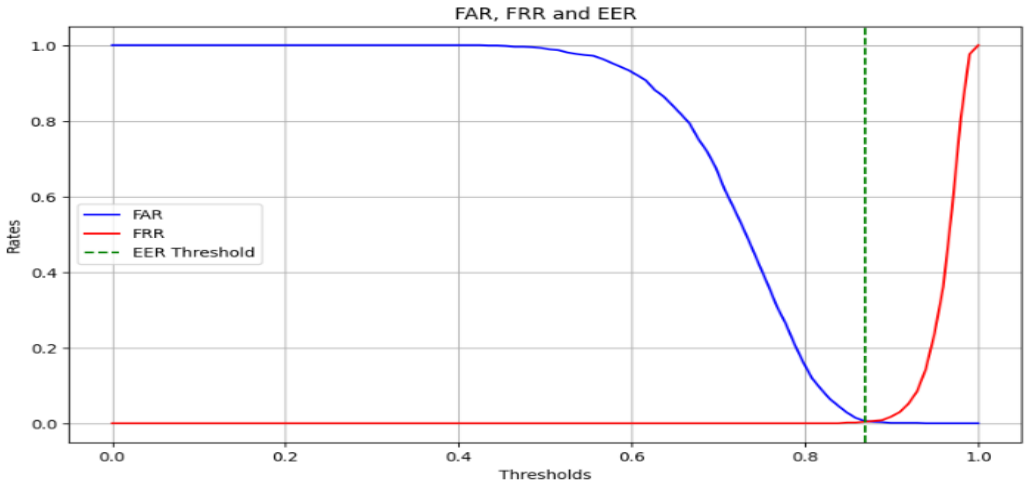

Fig. 6 Performance analysis of the proposed system on CASIA-Iris-Syn

Table 5. Performance comparison of the proposed model and other models on CASIA-Iris-Syn

Ref. No.		Accuracy	Precision	F1-score	Recall
[37]	ViT-L16	.9569	.9608	.9403	.9569
	ViT-L32	.9403	.9465	.9388	.9564
[38]		.9703	.9424	-	.9407
Proposed Method		**.99980**	**.9988**	**.9987**	**.9985**

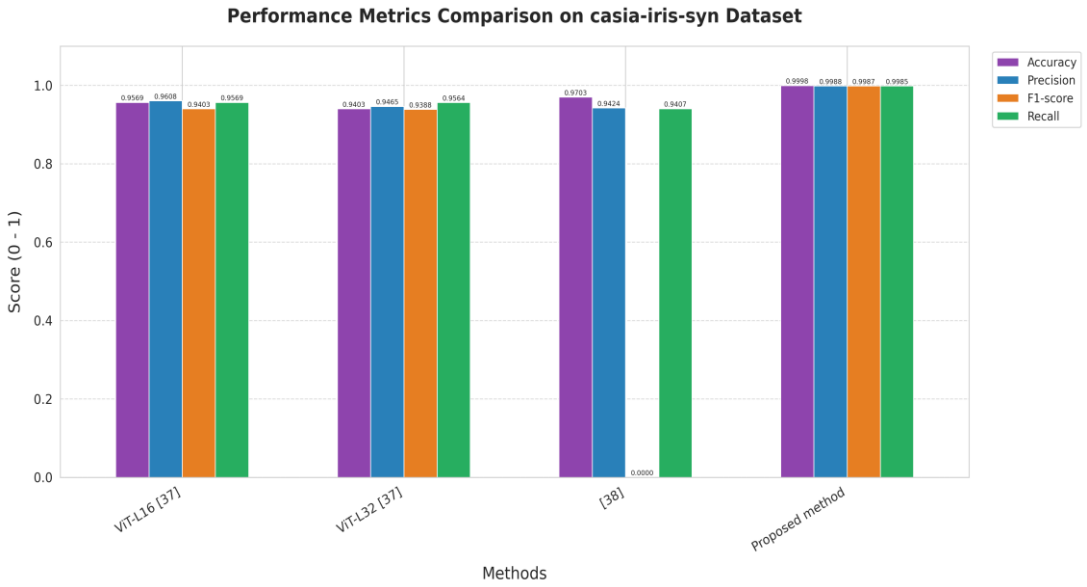

Fig. 7 Performance Metrics Comparison on CASIA-Iris-Syn Dataset

4.7 Evaluation of the proposed system's performance on IITD-Iris-V1

The proposed method also outperformed the comparable methods in [39], [40], and [41], achieving high accuracy (0.9898) and the highest specificity (0.9911), which indicates excellent performance in identifying negative cases and reducing false positives. It also achieved the highest precision (0.99035), surpassing [39] (0.9703) and significantly outperforming [40], where precision values were very low (0.1333 and 0.1111). The F-score of the proposed method (0.9716) reflects a strong balance between precision and recall, close to the best value in [39] (0.9805), and much higher than the weak F-scores in [40]. Although modified SOM 1 and 2 in [41] showed good accuracy (0.980 and 0.984), the lack of precision and F-score data limits their evaluation Fig. 8, 9 display the performance analysis of the suggested model on IITD-Iris-V1 dataset. A performance comparison between the proposed one and other models on IITD-Iris-V1 is shown in Table 6. Overall, the proposed method demonstrates the most balanced and reliable performance, making it the most suitable for sensitive applications like medical diagnostics.

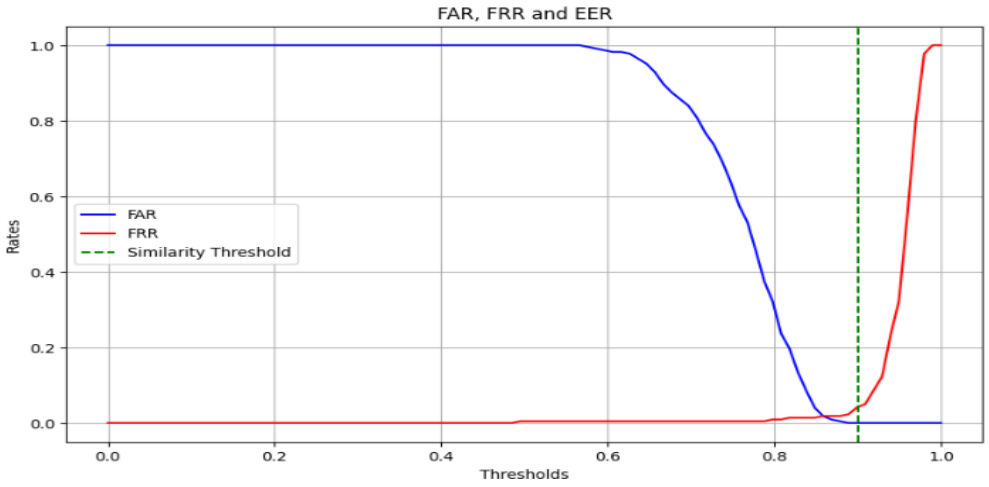

Fig. 8 Performance analysis of the proposed system on IITD-Iris-V1

Table 6. Performance comparison of the proposed model and other models on IITD-Iris-V1

Ref.No		Accuracy	Specificity	Precision	F-score
[39]	RISNet without segmentation	0.9942	0.9804	0.9703	0.9805
[40]	IRISNet with normalized	0.9732	0.9709	0.1333	0.2353
[41]	modified SOM 1	.98	0.95	-	
[41]	modified SOM 2	.984	0.95	-	
Proposed Method		**.9898**	**.9911**	**0.99035**	**0.9716**

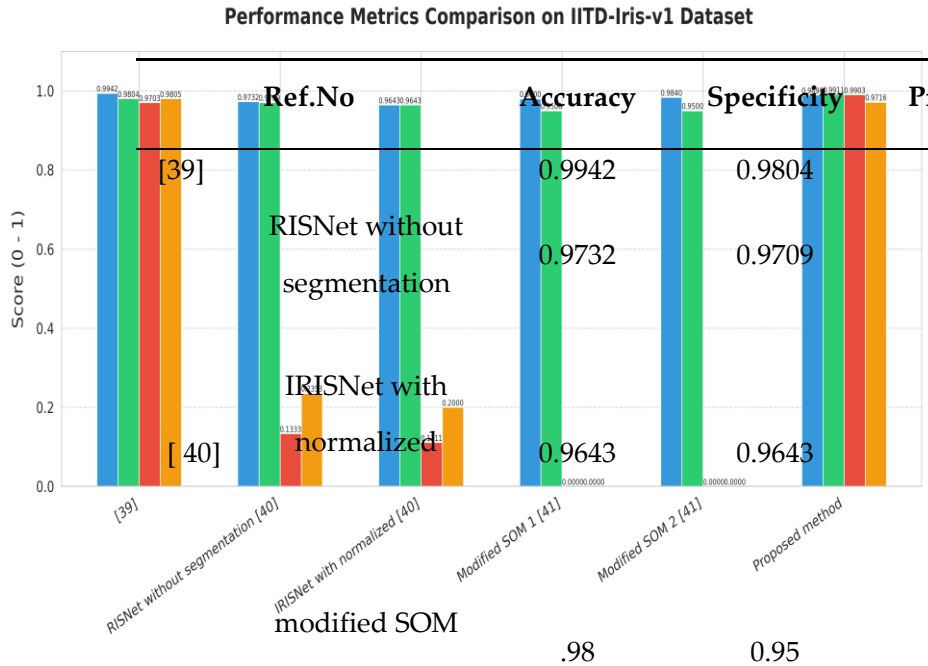

Fig .9 Performance Metrics Comparison on IITD-Iris-V1 Dataset

4.3 Security Analysis

This section evaluates the proposed approach against critical security properties such as **Unlinkability, Renewability, irreversibility, brute force resistance, key guessing resistance, quantum resistance, and confidentiality** based on (FHE) and (BF). The implementation uses cryptographic and dynamic data processing techniques to ensure strong protection against various security threats [42]. Table 7 shows the overall security properties of the proposed system through multidimensional analysis:

Table 7. shows the analysis of the Security Phase for each security property.

Security Property	Techniques Used	Protection Level	Potential Attacks	Defense Mechanism Analysis
Unlinkability	Dynamic keys, Secure Bloom Filter (SBF)	High	Correlation attacks	Encrypted data cannot be linked across sessions or entities due to key rotation and hashing [43]
Renewability	Dynamic key management	High	Compromised key reuse	Automatic key rotation (weekly) with secure re-encryption cancelable templates [44]
Irreversibility	CKKS	High	Template reconstruction	Fully homomorphic operations prevent decryption of raw biometric features [42]
Brute-force Resistance	256-bit cryptographic keys	High	Exhaustive key search	Computational infeasibility (2^{256} combinations) with PBKDF2 key derivation [45]
Key Guessing	CKKS with PBKDF2/Argon2	High	Dictionary attacks	Multi-factor key derivation with salt and iterations [28]
Quantum Resistance	CKKS (Lattice-based)	Medium	Shor's algorithm	Currently quantum-susceptible; future upgrade to NIST-approved PQC required [46]
Confidentiality	CKKS encrypted operations	High	Eavesdropping, MITM	End-to-end encryption with no plaintext exposure during processing [47]

Unlinkability, Renewability, and Irreversibility represent fundamental requirements when handling confidential data such as biometric identifiers, since continuous feature updates prevent cross-referencing and correlation between different instances [42]. Quantum Resistance has emerged as a critical necessity given the

rapid advancement in quantum computing technologies, which pose significant threats to existing cryptographic frameworks and could compromise current encryption methodologies [46].

5. Conclusions

This research paper aims to develop an improved biometric iris recognition system that combines high accuracy with advanced security. The proposed framework addresses the security vulnerability of traditional biometric systems by incorporating advanced techniques, including: improving input image quality, extracting biometric features using deep neural networks, securing these features with fully homomorphic encryption, and storing them in a scalable Bloom data structure. Results demonstrate that the system outperforms previous systems in accuracy rates, while meeting international security requirements. The framework provides strong resistance to various types of security threats, including data protection during processing, storage, and transmission. Despite the achievements, the system faces challenges related to high computational complexity, large memory requirements, and scalability challenges with increasing user numbers. Therefore, future studies focus on expanding the system to include additional and multiple biometric features, reducing the size of encrypted data, improving system performance to reduce response time by 30%, and developing intelligent encrypted data management mechanisms that support up to 100,000 users while maintaining recognition accuracy above 99%.This research represents an important contribution to the development of secure and scalable biometric authentication systems, opening new horizons for its applications in sensitive sectors that require the highest levels of security and privacy.

6. References

[1] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Syst. Appl.*, vol. 143, p. 113114, Apr. 2020

[2] J. Taylor, "Major breach found in biometrics system used by banks, UK police and defence firms," *The Guardian*, 2019. [Online]. Available: https://www.theguardian.com

[3] Y. Yin, S. H. He, and R. Z. Zhang, "Deep Learning for Iris Recognition: A Review," in Deep Learning for Biometric Recognition, Springer, pp. xx–yy, Mar. 2023.

[4] Anonymous, "Privacy-preserving data aggregation in smart metering systems," *Smarter Energy: From Smart Metering to the Smart Grid*, pp. 29–57, Oct. 2016.

[5] M. Tan and Q. Le, "EfficientNet: Rethinking model scaling for convolutional neural networks," *arXiv preprint arXiv:1905.11946*, 2019.

[6] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "Fully homomorphic encryption without bootstrapping," *ACM Trans. Comput. Theory*, vol. 6, no. 3, pp. 1–36, 2014.

[7] S. Geravand and M. Ahmadi, "Bloom filter applications in network security: A state-of-the-art survey," *Comput. Netw.*, vol. 57, no. 18, pp. 4047-4064, 2013.

[8] R. F. Soliman et al., "Efficient cancelable iris recognition scheme based on modified logistic map," *Proc. Nat. Acad. Sci. India Sect. A*, vol. 90, no. 1, pp. 101–107, Sep. 2018.

[9] Y. Chen, Y. Wo, R. Xie, C. Wu, and G. Han, "Deep secure quantization: On secure biometric hashing against similarity-based attacks," *Signal Process.*, vol. 154, pp. 314–323, Jan. 2019.

[10] W. U. Wickramaarachchi, D. Zhao, J. Zhou, and J. Xiang, "An effective Iris biometric privacy protection scheme with renewability," *J. Inf. Secur. Appl.*, vol. 80, p. 103684, Feb. 2024.

[11] T. Sudhakar and M. Gavrilova, "Cancelable biometrics using deep learning as a cloud service," *IEEE Access*, vol. 8, pp. 112932–112943, 2020

[12] M. Sandhya, D. K. Vallabhadas, and S. Rathod, "Revocable iris templates using partial sort and randomised look-up table mapping," *Int. J. Biom.*, vol. 15, no. 1, p. 21, 2023.

[13] P. Punithavathi and S. Geetha, "Random permutation-based linear discriminant analysis for cancelable biometric recognition," *Lect. Notes Electr. Eng.*, pp. 593–603, 2021.

[14] G. M. Salama et al., "Cancelable biometric system for IOT applications based on optical double random phase encoding," *Opt. Express*, vol. 30, no. 21, p. 37816, Sep. 2022.

[15] R. H. Farouk, H. Mohsen, and Y. M. El-Latif, "A proposed biometric technique for improving iris recognition," *Int. J. Comput. Intell. Syst.*, vol. 15, no. 1, Sep. 2022.

[16] E. Abdellatef et al., "Cancelable face and Iris recognition system based on Deep Learning," *Opt. Quantum Electron.*, vol. 54, no. 11, Sep. 2022.

[17] J. A. Singh, C. Vashist, P. Gaurav, and A. Nigam, "A generic framework for deep incremental cancelable template generation," *Neurocomputing*, vol. 467, pp. 83–98, Jan. 2022.

[18] Y. Wu and X. Zhang, "A three-party iris recognition model based on homomorphic encryption and CS-LBP feature extraction algorithm," *Proc. Int. Conf. Pattern Recognit. Image Anal. (PRIA)*, p. 51, May 2023.

[19] K. Zuiderveld, "Contrast Limited Adaptive Histogram Equalization," *Graphics Gems*, pp. 474–485, 1994.

[20] C. Tomasi and R. Manduchi, "Bilateral filtering for gray and color images," *Proc. Sixth Int. Conf. Comput. Vis. (ICCV)*, pp. 839–846, 1998.

[21] M. O. Al-Hatmi and J. H. Yousif, "A review of Image Enhancement Systems and a case study of Salt & Pepper noise removing," *Int. J. Comput. Appl. Sci. (IJOCAAS)*, vol. 2, no. 3, pp. 171–176, 2017.

[22] R. Hummel, "Image enhancement by histogram transformation," *Comput. Graph. Image Process.*, vol. 6, no. 2, pp. 184–195, 1977.

[23] C. Palm and T. M. Lehmann, "Classification of color textures by Gabor filtering," *Mach. Graph. Vis.*, vol. 11, no. 2/3, pp. 195-220, 2002.

[24] H. Ibrahim and N. S. P. Kong, "Brightness preserving dynamic histogram equalization for image contrast enhancement," *IEEE Trans. Consum. Electron.*, vol. 53, no. 4, pp. 1752-1758, 2007.

[25] S. Ruder, "An overview of multi-task learning in deep neural networks," *arXiv preprint arXiv:1706.05098*, 2017.

[26] *M. A. M. Joy et al., "Automated parkinson's disease detection from brain mri images using deep convolutional neural network," in 2023 26th International Conference on Computer and Information Technology (ICCIT), Dec. 2023, pp. 1–6.*

[27] A. Benaissa, et al., "Tenseal: A library for encrypted tensor operations using homomorphic encryption," *arXiv preprint arXiv:2104.03152*, 2021.

[28] P. Sathishkumar, K. Pugalarasan, C. Ponnparamaguru, and M. Vasanthkumar, "Improving healthcare data security using Cheon-Kim-Kim-Song (CKKS) homomorphic encryption," *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*, pp. 1–6, Apr. 2024. doi:10.1109/ickecs61492.2024.10616691.

[29] E. Lee, et al., "Optimization of homomorphic comparison algorithm on RNS-CKKS scheme," *IEEE Access*, vol. 10, pp. 26163-26176, 2022.

[30] S. Nayak, R. Patgiri, and A. Borah, "A survey on the roles of Bloom filter in implementation of the named data networking," *Comput. Netw.*, vol. 196, p. 108232, 2021.

[31] Lewi, K., et al., "Securing update propagation with homomorphic hashing," *Cryptology ePrint Arch.*, 2019.

[32] W. Lu, A. L. Varna, and M. Wu, "Confidentiality-preserving image search: A comparative study between homomorphic encryption and distance-preserving randomization," *IEEE Access*, vol. 2, pp. 125-141, 2014.

[33] H. V. Nguyen and L. Bai, "Cosine similarity metric learning for face verification," *Proc. Asian Conf. Comput. Vis.*, pp. 1752-1758, 2010.

[34] Institute of Automation, Chinese Academy of Sciences, "CASIA Iris Image Database (Version Syn)," [Online]. Available: http://biometrics.idealtest.org/downloadDB.do?id=4 [Accessed: Jul. 25, 2025].

[35] IIT Delhi Database. [Online]. Available: http://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm

[36] Kaggle, "Kaggle Platform for Data Science and Machine Learning," [Online]. Available: https://www.kaggle.com/

[37] S. Ennajar and W. Bouarifi, "Monitoring Student Attendance Through Vision Transformer-based Iris Recognition," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 2, 2024.

[38] B. Hassan et al., "Sip-segnet: A deep convolutional encoder-decoder network for joint semantic segmentation and extraction of sclera, iris and pupil based on periocular region suppression," *arXiv preprint arXiv:2003.00825*, 2020

[39] K. S. Balasubramanian, V. Jeganathan, and T. Subramani, "Deep Learning-Based Iris Segmentation Algorithm for Effective Iris Recognition System," *Proc. Eng. Technol. Innov.*, vol. 23, 2023.

[40] M. Omran and E. N. AlShemmary, "An iris recognition system using deep convolutional neural network," *J. Phys. Conf. Ser.*, vol. 1530, no. 1, 2020

[41] M. A. Pathak and B. Raj, "Privacy-preserving speaker verification using password-like matching," *Proc. 2012 IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, pp. 1849–1852, 2012.

[42] S.-C. Wu, P.-L. Hung, and A. L. Swindlehurst, "ECG biometric recognition: unlinkability, irreversibility, and security," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 487-500, Jan. 2022.

[43] A. Abdennebi and K. Kaya, "A bloom filter survey: Variants for different domain applications," *arXiv preprint arXiv:2106.12189*, 2021.

[44] E. Affum, et al., "Lattice Puncturable Attribute Based Proxy Re-encryption Scheme and Its Application in Information Centric Network," in *Future of Information and Communication Conference*, Cham: Springer International Publishing, 2022.

[45] A. Aloufi, et al., "Computing blindfolded on data homomorphically encrypted under multiple keys: An extended survey," *arXiv preprint arXiv:2007.09270*, 2020

[46] R. Agrawal, "Hardware accelerators for post-quantum cryptography and fully homomorphic encryption," Ph.D. dissertation, Boston University, 2023.

[47J. Choi, J. Choi, Y. Lee, and J. S. Hong, "Privacy-Preserving Rule Induction Using CKKS," *IEEE Access*, vol. 12, pp. 171540–171558, 2024, doi: 10.1109/ACCESS.2024.3498040