Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8841021, 15 pages
https://doi.org/10.1155/2020/8841021

Research Article

Enhanced Biometric Recognition for Secure Authentication Using Iris Preprocessing and Hyperelliptic Curve Cryptography

Vani Rajasekar,[1] **J. Premalatha**,[2] **and K. Sathya**[3]

[1]Dept of CSE, Kongu Engineering College, Perundurai, Erode, India
[2]Dept of IT, Kongu Engineering College, Perundurai, Erode, India
[3]Dept of CT/UG, Kongu Engineering College, Perundurai, Erode, India

Correspondence should be addressed to Vani Rajasekar; vanikecit@gmail.com

Received 22 March 2020; Revised 5 July 2020; Accepted 21 August 2020; Published 17 September 2020

Academic Editor: Daniel G. Reina

Biometrics combined with cryptography can be employed to solve the conceptual and factual identity frauds in digital authentication. Biometric traits are proven to provide enhanced security for detecting crimes because of its interesting features such as accuracy, stability, and uniqueness. Although diverse techniques have been raised to address this objective, limitations such as higher computational time, minimal accuracy, and maximum recognition time remain. To overcome these challenges, an enhanced iris recognition approach has been proposed based on hyperelliptic curve cryptography (HECC). The proposed study uses the 2D Gabor filter approach for perfect feature extraction in iris preprocessing. A lightweight cryptographic scheme called HECC was employed to encrypt the iris template to avoid intentional attack by the intruders. The benchmark CASIA Iris V-4 and IITD iris datasets were used in the proposed approach for experimental analysis. The result analysis witnessed that the prime objective of the research such as lesser false acceptance rate, lesser false rejection rate, maximum accuracy of 99.74%, maximum true acceptance rate of 100%, and minimal recognition time of 3 seconds has been achieved. Also, it has been identified that the proposed study outperforms other existing well-known techniques.

1. Introduction

With the advancement of information technology, there is a gradual increase in crime and identity fraud. To address the issues related to identity fraud, heightened security mechanism is needed. Biometric recognition is the most eminent technology for person authentication in identification systems. Biometric traits accurately determine the identity of a person either by means of their physiological characteristics (finger, iris, hand, face) and behavioral characteristics (gait, signature, voice). The most reliable and leading biometric technology is the iris recognition system. The iris authentication is the most accurate and domain-bounded recognition approach which uses distinctive patterns of the human iris. The unique nature of the iris is set between the cornea and the region of the pupil in the eye. The iris diameter is 12 mm, and the size of the pupil varies from 10% to 80%. The texture details of the iris such as furrows, cornea, filaments, flecks, and arching ligaments make the iris unique. The unique feature of the iris is extracted after proper preprocessing techniques such as localization, normalization, and segmentation. A 2D Gabor filter is used in the proposed for accurate feature extraction from the iris.

In addition to the feature extraction of the iris, a proper encryption is also a major demand. The need for encryption in the iris recognition is when original template is stored in database; the intruder may compromise and give access to sensitive data of a user. To overcome these challenges, HECC is proposed for encrypting the iris template. HECC is a lightweight cryptographic approach [1] that uses very less key size of 80 bits. HECC provides higher security with lower computational time; hence, it is the most applicable for real time

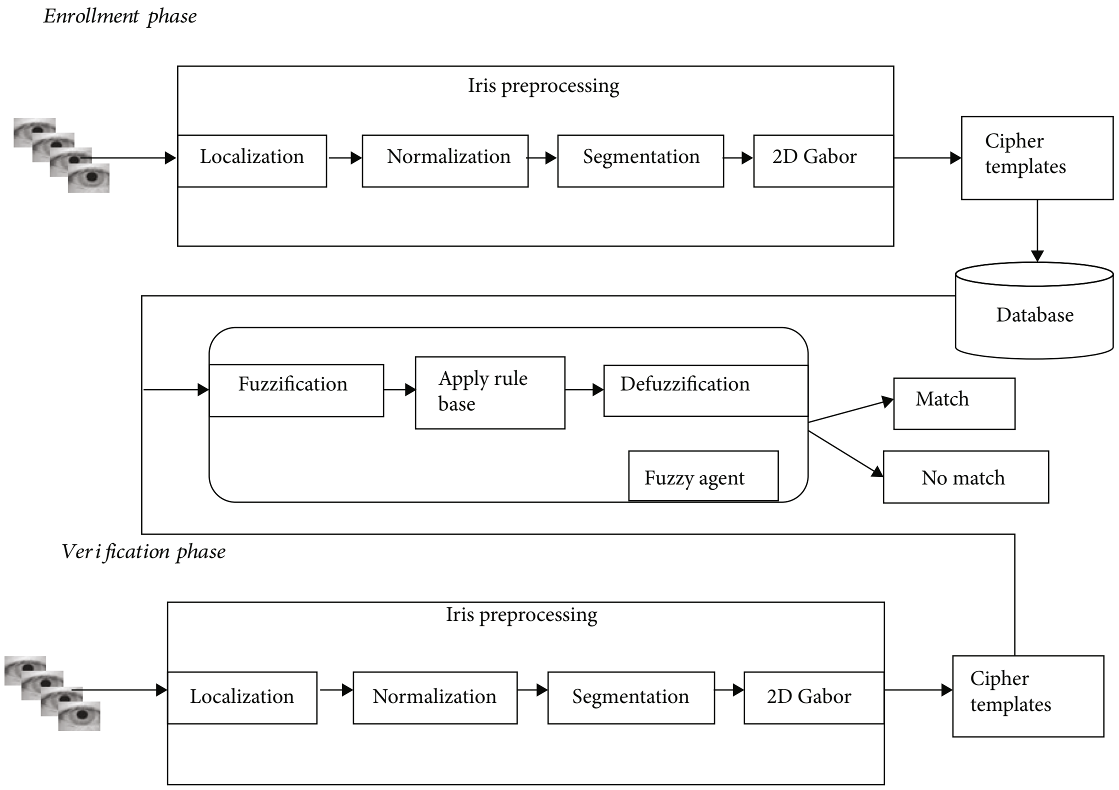

Figure 1: A flow diagram of proposed methodology.

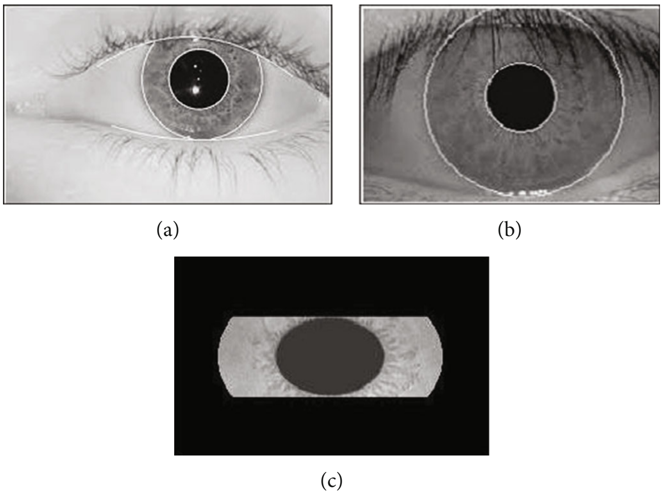

Figure 2: Iris preprocessing: (a) original iris; (b) iris localization; (c) iris segmentation.

applications such as military, E-passport, credit card services, and banking applications. The inclusion of AI technique and fuzzy logic in this research will increase and refine the knowledge stored in the system; thereby, it lowers the recognition error and enhances the accuracy of proposed system.

The major contribution of the paper is to address all the security-related issues. Enhanced iris recognition with HECC encryption [2] and fuzzy logic for feature matching has been developed and tested, and result shows that it provides very

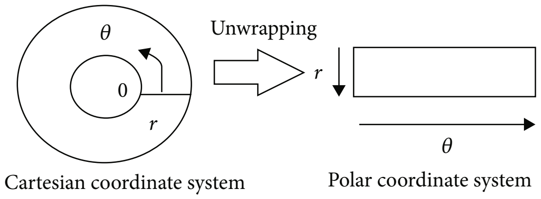

Figure 3: Daugman’s rubber sheet model.

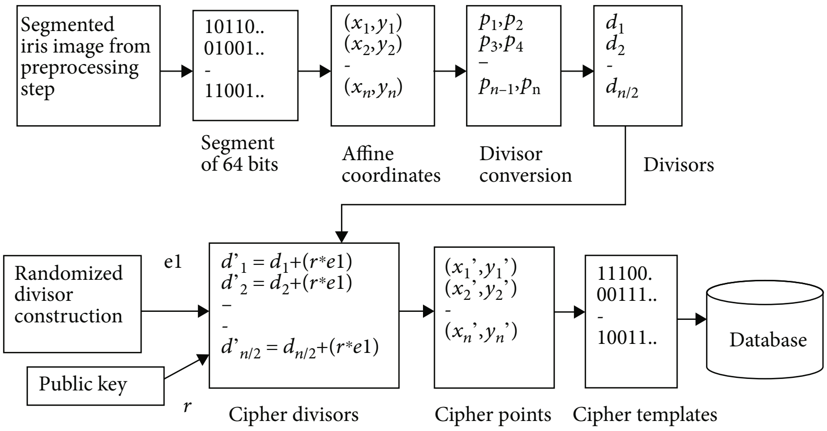

FIGURE 4: Hyperelliptic curve cryptographic approach.

```
Input: 64 bit large prime number
Output: HEC of Genus-2 with larger cardinality N
Process:
While true
Do Repeat
Repeat choosing p=64 bits
Until factoring of $p = \varpi * \omega$ as prime ideals
Compute all the expected cardinality N
Until at least one of them desires cardinality N
For s=1,2,3 then p=4s+3 where $s \in N$
Compute roots as $J_s = \{J_s^{(i)}\}$
Where $(j_1, j_2, j_3) \in (J_1, J_2, J_3)$
Calculate conic $\theta_{j_1,j_2,j_3}(x_1, x_2, x_3)$
If a point $(A_1, A_2, A_3)$lies with $\theta_{j_1,j_2,j_3}(x_1, x_2, x_3)$=0 then
Calculate $h_{j_1,j_2,j_3}$ and intersecting polynomial
If intersecting polynomial contain a root in $F_p$ then
Locate Genus-2 HEC
Identify the random divisor
Compute N and If N is seems to be favor
Stop and return Curve C and cardinality N
```

ALGORITHM 1: Extended Complex Multiplication (ECM).

```
Input: 64 bit Iris template
Output: Iris template within 64 bits
Process:
For each sample, $T_i$ do
$T'_i = (T_i \times (2^{-1}) \bmod p) \bmod p$
```

ALGORITHM 2: Restricted Iris Template (RIT).

```
Input: p1(a1,b1), p2(a2,b2)
Output: $d = (X^2 + A * X + B, C * X + D) \bmod p$
Process:
Compute the below equations
1. $A = (-a1 - a2) \bmod p$
2. $B = (a1 * a2) \bmod p$
Solve C and D as follows
1. $C * a1 + D = b1$
2. $C * a2 + D = b2$
Return divisor as $d = (X^2 + A * X + B, C * X + D) \bmod p$
```

ALGORITHM 3: Point to Divisor Conversion (PDC).

less recognition time, higher accuracy, lower false rejection rate, and false acceptance rate. The remainder of the paper is organized in following ways. Section 2 describes the related work carried out in the field of iris recognition, fuzzy logic in biometric, and hyperelliptic curve cryptography. Section 3 provides brief note on hyperelliptic curve selection, fuzzy logic introduction, and dataset used in proposed methodology. Section 4 explains about the proposed technology with four steps of iris preprocessing, HECC encryption, fuzzy logic matching, and decision. Section 5 is mainly devoted for result comparison and discussion based on two datasets, CASIA iris and IITD dataset. General conclusion about proposed technique and future scope is explained in Section 6. Till now, no applications have been proposed in combination with iris recognition with HECC encryption and fuzzy logic.

2. Related Works

This section provides the brief overview of various iris recognition and encryption techniques. Aparna et al. [3] discussed stable biometric characteristics to recognize a person. Result analysis shows that their scheme shows good performance on CASIA database. Kalka et al. [4] used various metrics for iris recognition. Their scheme was based on occlusion, gaze deviation, and light reflection based on ICE database. Sun et al. [5] specify iris recognition based on three approaches, i.e., coarse iris classification, iris aliveness detection, and coarse iris classification. Yongqiang et al. [6] proposed an iris recognition model based on global and local iris features. Their scheme uses privacy projection algorithm which converts high dimensionality data into lower

```
*Input:* p prime number and HEC curve C
*Output:* Randomized divisor e1
*Process:*
While true
Let a1, a2 be the two numbers such that $a1, a2 \in \{1, 2, 3, ..p - 1\}$
Calculate $S1 = \sqrt{f(a1) \bmod p}$
Calculate $S2 = \sqrt{f(a2) \bmod p}$
Where f(a1) and f(a2) are curve functions
If $(S1^2 \bmod p == f(a1) \bmod p)\&\&(S2^2 \bmod p == f(a2) \bmod p)$
p1= (a1,S1) and p2= (a2,S2) are valid points
Form divisor e1 using algorithm PDC with points p1 and p2, break
Return randomized divisor e1.
```

Algorithm 4: Randomized Construction of Divisors (RCD).

```
*Input:* Divisors d1=[a1,b1], d2=[a2,b2]
*Output:* d=d1+d2
*Process:*
Calculate
    S1=gcd(a1,a2)
    S1=e1a1+e2a2
Compute.
    D=gcd(S1,b1+b2+h)
    D=C1S1+C2(b1+b2+h)
Calculate t1=C1e1, t2=C1e2, t3=C2
Compute $u = a1a2/D^2$
Compute $v = (t1a1b2 + t2a2b1 + t3(b1b2 + f)/D) \bmod u$
Repeat
Calculate$t' = f - hv - v^2/u$, $k' = (-v - h) \bmod t'$
$u = t'$, $v = k'$
Until deg(u)<=g
Form u as a monic
Return cipher divisor as d'[u,v]
```

Algorithm 5: Divisor Addition based on Cantor Algorithm (DACA).

```
*Input:* $d = (X^2 + A * X + B, C * X + D) \bmod p$
*Output:* p1(a1,b1), p2(a2,b2)
*Process:*
Calculate
$X^2 + A * X = -b \bmod p$
$(X + A * (2^{-1} \bmod p))^2 \bmod p = -b - A * (2^{-1} \bmod p) \bmod p$
$(X + A * (2^{-1} \bmod p)) \bmod p = sqrt \bmod p(-b - A * (2^{-1} \bmod p) \bmod p)$
Compute
$X1 = (sqrtm(-b * (2^{-1} \bmod p)) - A * (2^{-1} \bmod p)) \bmod p$
$X2 = (-sqrtm(-b * (2^{-1} \bmod p)) - A * (2^{-1} \bmod p)) \bmod p$
Calculate
$Y1 = v(X1)$
$Y2 = v(X2)$
Return $(X1, Y1)$and$(X2, Y2)$
```

Algorithm 6: Divisor to Point Conversion (DPC).

dimensionality data. Vani Rajasekar et al. [7] have proposed an authentication scheme based on signcryption with HECC. It is shown in their work that HECC provides much higher security than other cryptographic algorithms. Zhou et al. [8] developed an enhanced iris recognition model that outperforms the Daugman's model [9]. Their scheme uses snake

```
Input: Original iris template I
Output: Encrypted iris template I'
Process:
Choose genus 2 HEC using ECM
Convert original iris template to points in HEC
Convert all the points of HEC to divisors using PDC
Select random divisor e11 based on algorithm RCD
Select public key $r \in \{2, 3, 4..p-1\}$
For each 4 consecutive samples (I1, I2, I3, I4) do
Form randomized divisor e1 using algorithm RCD
Calculate $d'_i = d + (r * e1)$using DACA
Return all computed cipher divisors$d'_i$.
Convert cipher divisors to cipher points using DPC
Convert cipher points to cipher template
Store cipher template in database
```

Algorithm 7: Proposed Iris Template Encryption (ITE).

model and vector field convolution technique to accurately determine the inner edge of the iris. Poursaberi et al.'s [10] iris recognition approach is based on hamming and harmonic mean distance. The dataset used in their method in CASIA V1 and feature extraction method used were wavelet daubechies2. Their observation includes, rather than smaller part of the iris, more reliable part produces more accuracy.

Galbally et al. [11] developed a mechanism that not only for iris authentication but also used for immediate liveliness detection of the iris. Burak et al. [12] identified a biometric recognition approach in which the performance greatly depends on coding bits and noise level. Daugman et al. [13] used the Gaussian filter for segmentation of an iris image. Their performance greatly varies due to light illumination and reflections. Neda et al. [14] developed a hybrid robust iris recognition approach that uses 2D Gabor filter for feature extraction and neural network; PSO algorithm was employed to improve the generalization performance. Kalka et al. uses different metrics for iris recognition such as iris occlusion, amount of reflection, and gaze deviation. Their estimation was mainly on the bottom portion of iris, and datasets used were ICE, CASIA, and WVU. Ch SA et al. [2] developed a signcryption scheme based on HECC. Their analysis shows that encryption using HECC provides much higher security compared to other cryptographic algorithms. Reyes et al. [15] focused mainly on the iris texture and variability. Their scheme uses pseudo polar arrangement for matching and biomechanical model to enhance the recognition rate and accuracy.

Aditya Dixit et al. [16] developed iris recognition approach based on fuzzy logic-based edge detection in the iris. A distinct approach is specified for iris localization and edge detection. Result analysis shows that efficient edge detection has performed in their scheme. Malarvizhi et al. [17] presented a multibiometric recognition approach using soft computing approach combines with fuzzy. They used fuzzy logic to obtain a good fusion score on multibiometric (finger print and iris). The algorithm used in their scheme is Adaptive Fuzzy Genetic Algorithm (AFGA) which can be used for both unimodal and multimodal biometric schemes. Their result showed that their scheme outperforms other multimodal biometric verification and authentication strategies as it includes fuzzy logic fusion strategies. Saracevic et al. [18, 19] proposed a novel iris recognition approach based on stylometric features. Their approach uses machine learning techniques which improves the performance of iris recognition compared to other state of art approaches.

From the observations of above literatures, it has been studied that optimal iris recognition approach can be designed using iris localization, segmentation, and normalization. The 2D Gabor kernel filter acts as a perfect feature extraction mechanism in the iris. There is a need for encryption of original iris template before stored in the database because there is a possibility for an intruder to compromise the template database. The problem identified and literature survey has motivated the research in following ways.

(i) Iris preprocessing with the 2D Gabor filter can be used on normalized iris image for enhanced feature extraction

(ii) A novel approach called HECC can be used for encryption of original iris template as this is a lightweight cryptographic mechanism which provides much higher security in less computational time

(iii) Fuzzy logic can be included in verification phase to increase the accuracy and recognition rate

3. Preliminaries

3.1. HEC and Selection of Genus 2 Curve. For efficient communication to be established among mobile devices, the major requirement is higher security and less power constraints. The existing cryptographic algorithms such as RSA, AES, DES, and elliptic curve cryptography have not satisfied such requirements because of its larger key size and complex mathematical calculations involved in encryption and decryption process. HECC is a lightweight cryptographic scheme that has lesser key size and provides higher security than the existing schemes. The most attractive feature of HEC is that Genus 2 of HEC is mainly bounded on finite fields and algebraic geometry. Let S be a finite field and $\bar{S}$ be algebraic closure of S. The HEC with genus 2 over S is given by

$$\text{Curve}, C : f(x) = y^2 + h(x)y \,\text{in}\, S[x, y]. \tag{1}$$

In equation (1), $h(x)$ ε $S(x)$ is defined as polynomial with degree g whereas $f(x)$ denotes a monic polynomial with degree $2g+1$. The most important point in HEC is choosing of appropriate curve for application. The proposed research work uses a method called Extended Complex Multiplication (ECM) over P (prime field), and length of p is 64 bits. Hence, the time taken for executing brute force attack by the attacker in the proposed system will be much higher than the time taken for cryptanalysis.

3.2. Selection of Genus 2 Group Elements and Group Operations. The group elements of HEC are not a rational

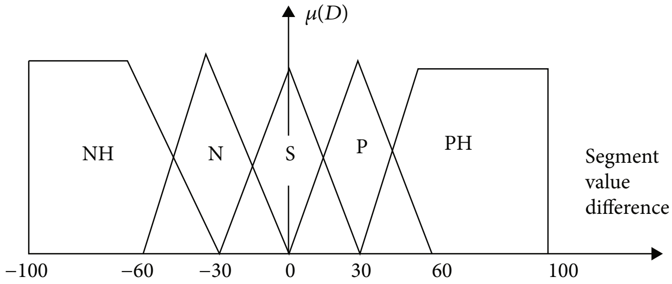

Figure 5: Fuzzy input.

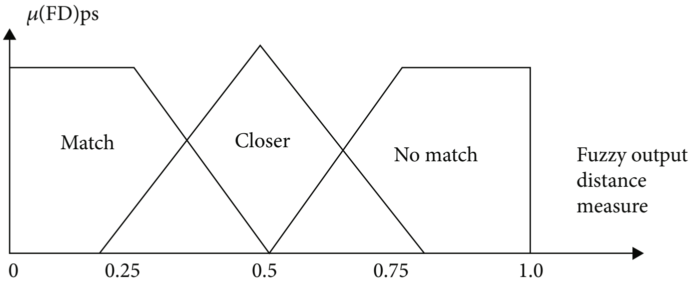

Figure 6: Fuzzy output.

Table 1: Performance evaluation with varying thresholds on CASIA dataset.

Threshold	50 iris samples			100 iris samples		
	FAR	FRR	TAR	FAR	FRR	TAR
0.45	0	50	0	0	100	0
0.50	0	47	6	0	97	3
0.55	0	41	19	0	87	13
0.60	0	35	30	0	54	46
0.65	1	22	56	0	37	63
0.70	5	5	90	15	15	85
0.75	19	3	94	53	9	91
0.80	41	1	98	89	4	96
0.85	50	0	100	97	0	100

point as in case of elliptic curve instead a divisor. In proposed research work, a divisor of HEC is identified by combining certain number of points using a technique called the Mumford representation. Generally, HECC allows addictive group which involves divisor addition, divisor doubling, and divisor inversion. The proposed research uses a technique called the Cantor algorithm for divisor addition and divisor inversion.

3.3. Fuzzy Logic. Fuzzy logic provides valuable flexibility in case of imprecision and uncertainty. Generally, fuzzy contains some tolerance towards imprecision of data. The architecture of fuzzy logic has four major parts.

(i) Rule base: rule base defines a set of rules. The decision-making system uses IF-THEN conditions. These conditions are mainly a form of linguistic information

(ii) Fuzzification: it is a process where crisp number or direct inputs from processors; sensors are converted in to fuzzy sets. The fuzzy sets are then given as input to application systems

(iii) Inference engine: inference engine matches the fuzzy input with the rule base. Based on the matching degree, it determines the next control actions to be processed

(iv) Defuzzification: it is a process where fuzzy set given by inference engine is converted into the crisp value output. These outputs are used in many expert systems for reducing the error

3.4. Dataset Used. There are two datasets used in the proposed research work. One of which is the Chinese Academy of Science and Institute of Automation (CASIA) Iris Image Database Version 4.0 [20]. This dataset is an extension of CASIA Iris Image Database Version 3.0. The dataset contains 54,600 iris images captured from 2,800 distinct subjects. All images are jpeg files of 8 bit gray scale. One of the subset of CASIA V4 is Iris Thousand image dataset; it has 20,000 high quality iris images. Another dataset used in this research is the Indian Institute of Technology Delhi (IITD) iris image dataset [21]. This contains about 2240 iris image acquired from 224 different users. The age group of those users is about 14-55 years made up of 176 males and 48 females. Each image in the dataset contains higher resolution of about 320×240 pixels. Because of this high resolution, both the datasets are well suited for analysis of real time biometric authentication models.

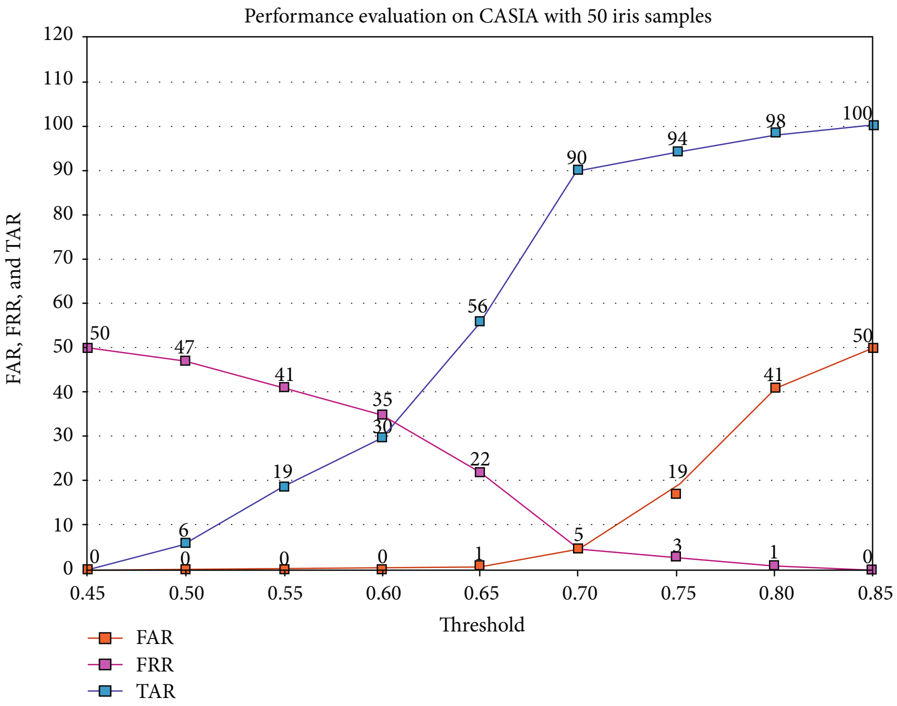

Figure 7: Plot of FAR, FRR, and TAR with varying threshold on CASIA dataset with 50 iris images.

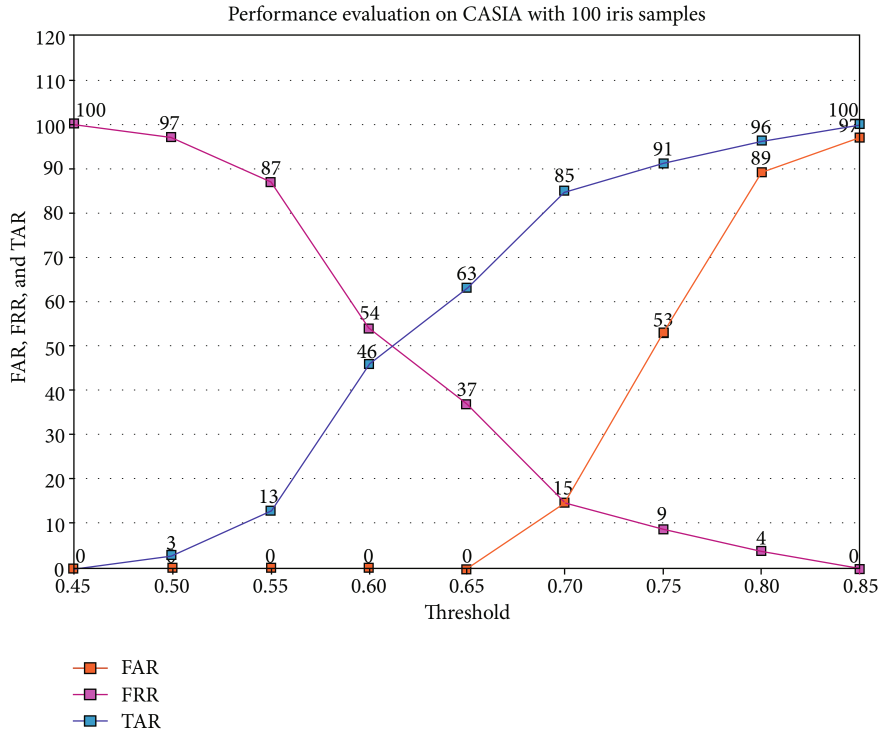

Figure 8: Plot of FAR, FRR, and TAR with varying threshold on CASIA dataset with 100 iris images.

4. Proposed Methodology

The iris is a unique physiological biometric trait of a person that can be used for authentication in many applications. The proposed study employs in two major modes of operation: (a) enrollment phase and (b) verification phase. The enrollment phase consists of iris preprocessing, creation of cipher templates, and storing of cipher templates to database. After preprocessing, 64 bit original noise removed templates are converted to cipher templates using encryption in HECC

Table 2: Performance evaluation with varying thresholds on IITD iris dataset.

Threshold	50 iris samples			100 iris samples		
	FAR	FRR	TAR	FAR	FRR	TAR
0.45	0	50	0	0	100	0
0.50	0	45	10	0	95	5
0.55	0	37	26	0	79	21
0.60	0	25	50	0	58	42
0.65	2	20	60	7	40	60
0.70	6	6	88	15	15	85
0.75	20	3	94	39	8	92
0.80	38	1	98	67	2	98
0.85	50	0	100	99	0	100

approach, and all obtained cipher templates are stored in the application database. The verification steps consist of acquire of iris image, iris preprocessing, and creation of cipher template using HECC. The resultant cipher template is to be compared with the enrolled template stored in database. The comparison and decision-making process are based on the fuzzy logic. The overview of proposed methodology is given in Figure 1.

4.1. Iris Preprocessing. High quality of iris image acquisition generally results in higher accuracy for any authentication procedure. The iris image preprocessing consists of two phases: (1) iris localization and (2) iris normalization. These were performed to identify the ROI (region of interest) of the iris and also to minimize the unwanted noise present in iris image.

4.1.1. Iris Localization. This procedure detects the border internally and externally without error that separates the sclera and pupil part of the iris. The proposed work uses Circular Hough Transform Algorithm (CHTA) for localization. The gray scale format can be applied to the captured image. In the iris, the regions where dim pixels surrounded by light pixels are known as holes. A Canny Edge Detection algorithm is used to locate the edge map on gray image. The CHTA is applied on the specific areas to perfectly identify the inner and outer circle iris parameters given in Figure 2(b).

4.1.2. Iris Normalization. Conversion of iris image in Cartesian products to polar coordinates is called normalization. The proposed work used Daugman's rubber sheet model for normalization shown in Figure 3. Here, the ring of iris image is transformed to rectangular projection of size (64×512). The images of iris area are $I(X,Y)$, Cartesian coordinates are (X,Y), polar coordinates are specified as (r,θ), $(X1,Y1)$, and $(X2,Y2)$ represents the iris and pupil boundaries in θ direction.

$$\begin{aligned} &I(X(r,\theta), Y(r,\theta)) \rightarrow I(r,\theta). \\ &X(r,\theta) = (1-r)X2(\theta) + rX1(\theta). \\ &Y(r,\theta) = (1-r)Y2(\theta) + rY1(\theta). \end{aligned} \tag{2}$$

4.1.3. Iris Segmentation. Segmentation is examined to be the major important step in iris preprocessing given in Figure 2(c). The proposed work uses centroid and bounding box method to identify the center and radius of the located pupil. To fix the lower and upper column in both horizontal and vertical direction, the center coordinate value of the pupil is added to and subtracted from radius, respectively. The iris part is segmented to 50 pixels from either side of pupil boundary to generate iris template based on CASIA Iris dataset [22].

4.1.4. 2D Gabor Kernel Filter. The 2D Gabor kernel filter is the excellent feature extraction mechanism of the iris. The more prominent features of this filter are the decomposition of input image into various images based on their textural information. A Gabor filter bank was employed to explain the channels present in frequency domain and spatial domain simultaneously. The filter parameters are precisely chosen for the determination of human visualization. The superfluous nature of the Gabor filter reduces the feature dimension. The Gabor kernel approach was chosen in which each trained samples are twisted with the other Gabor channels. The distance between and within the Gabor channels is calculated. The 2D Gabor filter representation in spatial domain is given as

$$G\lambda\psi\theta\Omega\gamma(X, Y) = \exp\left(-\frac{X'^2 + \gamma^2 Y'^2}{2\Omega^2}\right)\cos\left(2\Pi\frac{X'}{\lambda} + \psi\right), \tag{3}$$

where

$$\begin{aligned} X' &= X\cos(\theta) + Y\sin(\theta), \\ Y' &= Y\cos(\theta) - X\sin(\theta). \end{aligned} \tag{4}$$

In equation (3), λ is the sinusoidal function wavelength, θ is the Gabor filter orientation, ψ is the offset of Gabor filter, Ω represents the bandwidth, and γ represents the aspect ratio.

4.2. Hyperelliptic Curve Cryptographic Approach. The steps involved in HECC approach are (a) Extended Complex Multiplication (ECM) to select the proper genus 2 HEC with cardinality N, (b) Restricted Iris Template (RIT) to reduce the template size within 64 bits, and (c) Point to Divisor Conversion (PDC) algorithm to convert HEC points to divisors which is based on the Mumford representation. Once the divisors are generated, the next step is (d) Randomized Construction of Divisors (RCD) to generate random divisor which then combines with sequence of divisors from step (c) forms the cipher divisors by the procedure Divisor Addition based on Cantor Algorithm (DACA). (e) Cipher divisors are converted to cipher points using the algorithm Divisor to Point Conversion (DPC). The cipher templates are retrieved from cipher points as this is the final step in HECC approach. The cipher templates are stored in database. The flow diagram of HECC approach is depicted in Figure 4, and the

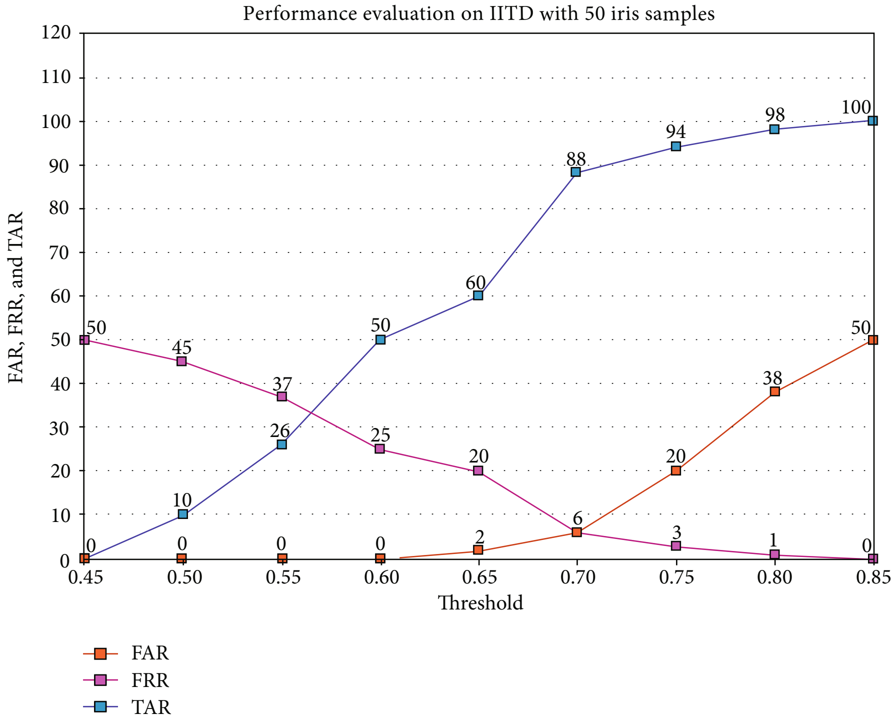

Figure 9: Plot of FAR, FRR, and TAR with varying threshold on IITD dataset with 50 iris images.

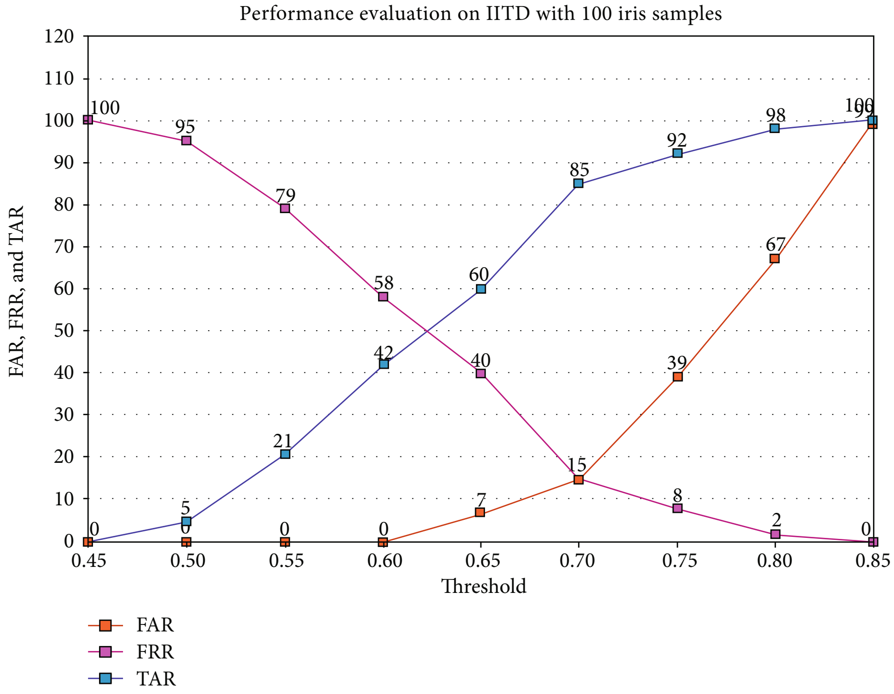

Figure 10: Plot of FAR, FRR, and TAR with varying threshold on IITD dataset with 100 iris images.

entire step involved in encryption is specified in algorithm 7 (Iris Template Encryption) ITE.

4.2.1. Designing of HEC Using ECM. The security of the proposed system can be enhanced by concept of Discrete Logarithmic Problem (DLP) of HEC. This denotes the selection of suitable prime number of size 64 bits, and a group order is always the multiplication of 64 bit prime number. The curve selection of HEC based on ECM is given in algorithm 1. The proposed system is designed to have iris image of size

64 bits. The genus 2 curve must generate to encompass all 64 bit binary sequences. As HEC is a form of genus 2 above GF (P), it will not be possible to generate included 64 bit sequences. Hence, iris segmented image after the 2D Gabor filter applied is restricted to generate the points which lies in the prime field which is depicted in algorithm 2.

4.2.2. HEC Points and HEC Divisors. HEC with genus 2 over 2g+1 is given in equation (1), and all nontrivial elements in HEC are specified as divisors. The divisors are symbolized with the monic polynomials $u(x)$ and $v(x)$. It depends mainly on three rules: (a) u should be monic, (b) degree calculated for v should always be lower than degree calculated for u, and (c) degree of u and $v <$ genus 2. The group operation of HEC is constructed on divisors, so it is needed to convert curve points to divisors and divisors to curve points. And because of group property HECC, it is faster than elliptic curve cryptography (ECC). Hence, HECC is well suited for lightweight cryptographic applications. Algorithm 3 represents the conversion of HEC points to divisors. The divisor of HEC is based on the Mumford representation with two pair of polynomials u and v.

$$\begin{aligned} u(X) &= X^2 + A * X + B. \\ v(X) &= C * X + D. \end{aligned} \tag{5}$$

4.2.3. Randomized Divisor Construction. The proposed biometric cryptosystem is a nondeterministic one in which for identical iris and key values it produces varied cipher template all the time. It is the worthwhile property of the proposed approach as it removes the known cipher text attack. Therefore, randomized divisor construction is in need all the time. The steps involved are specified in algorithm 4.

4.2.4. Divisor Grouping. The divisor grouping in HEC is based on the Cantor algorithm. This algorithm takes two randomized divisor as input and generate unique divisor as output. As hyperelliptic operation is generally formed on additive group, the required method for proposed cryptosystem is divisor addition in template encryption. Algorithm 5 depicts the steps involved in divisor addition.

4.2.5. Iris Template Encryption. The main question of template encryption in the proposed scheme is to avoid the eavesdropping of sensitive data by the attacker or sometimes the compromising of original template database by the attacker. One possible solution for this challenge is to ensure the privacy preserving of biometric template by means of cryptographic primitives. The direct employment of such cryptographic primitive is encryption of biometric template using HECC. The cipher divisors are converted to cipher points using the algorithm 6 DPC. The proposed encryption method converts the original iris template into cipher iris template. The processes of proposed encryption are depicted in algorithm 7.

4.3. Fuzzy Logic in Verification Phase. The cipher templates are stored in database during the enrollment phase. On verification of individuals, iris image is acquired, and it undergoes preprocessing; cipher templates are created by encryption using HECC. Fuzzy logic is used for identification of individuals. The process involved in fuzzy logic is defined as follows.

Table 3: Performance evaluation with varying thresholds on CASIA dataset.

Threshold	50 iris samples			100 iris samples		
	FAR	FRR	TAR	FAR	FRR	TAR
0.45	0	50	0	0	100	0
0.50	0	47	6	0	97	3
0.55	0	40	20	0	89	11
0.60	0	32	36	0	52	48
0.65	0	25	50	0	30	70
0.70	4	4	92	12	12	89
0.75	17	3	94	50	7	93
0.80	39	1	98	84	2	99
0.85	50	0	100	92	0	100

4.3.1. Agents Involved. The proposed approach contains a fuzzy input and output, a rule base.

4.3.2. Fuzzy Input. The fuzzy input denotes the magnitude of differences occurs between encrypted iris code in verification and encrypted iris code stored in database. Suppose, if the matching cipher iris code is 0.50 and iris code value in the database is 0.30, then fuzzy system's crisp input will be 0.50-0.30 = 0.2. The input is amplified by 100 which results in the input range -100 to 100. The fuzzy input is specified in Figure 5, where NH is negative high, PH is positive high, N is negative, P positive, and S is small.

4.3.3. Fuzzy Output. The output of proposed fuzzy approach is denoted as Fuzzy Output Distance (FOD) per segment of iris. The FOD denotes how closer the two segments of iris are. If the matching rate is high, then the score moves towards zero. If the matching rate is less, then the score moves towards 1. The fuzzy output is specified in Figure 6.

4.3.4. Rule Base. Rule base is considered to be knowledge inference in the system. The rule base of the proposed approach is given below.

```
IF segment value difference is 'Negative High'
    THEN FOD measure is 'No Match'
IF segment value difference is 'Negative'
    THEN FOD measure is 'Closer'
IF segment value difference is 'Small'
    THEN FOD measure is 'Match'
IF segment value difference is 'Positive'
    THEN FOD measure is 'Closer'
IF segment value difference is 'Positive High'
    THEN FOD measure is 'No Match'
```

5. Results and Discussion

The proposed method is implemented in Anaconda 3 (Spyder) using Python programming language with the

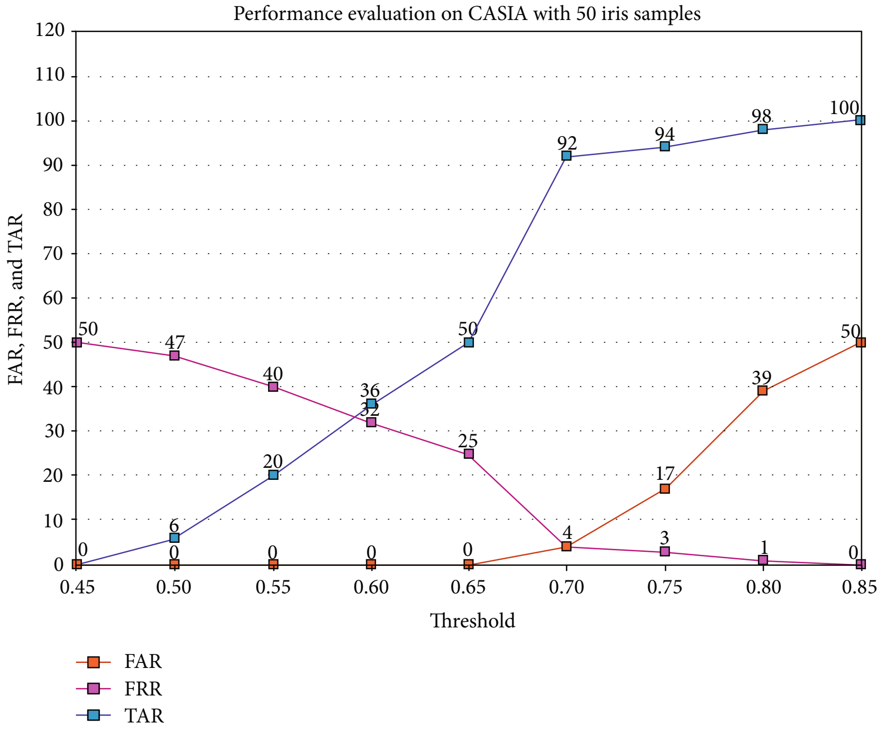

FIGURE 11: Plot of FAR, FRR, and TAR with varying threshold on CASIA dataset with 50 iris images.

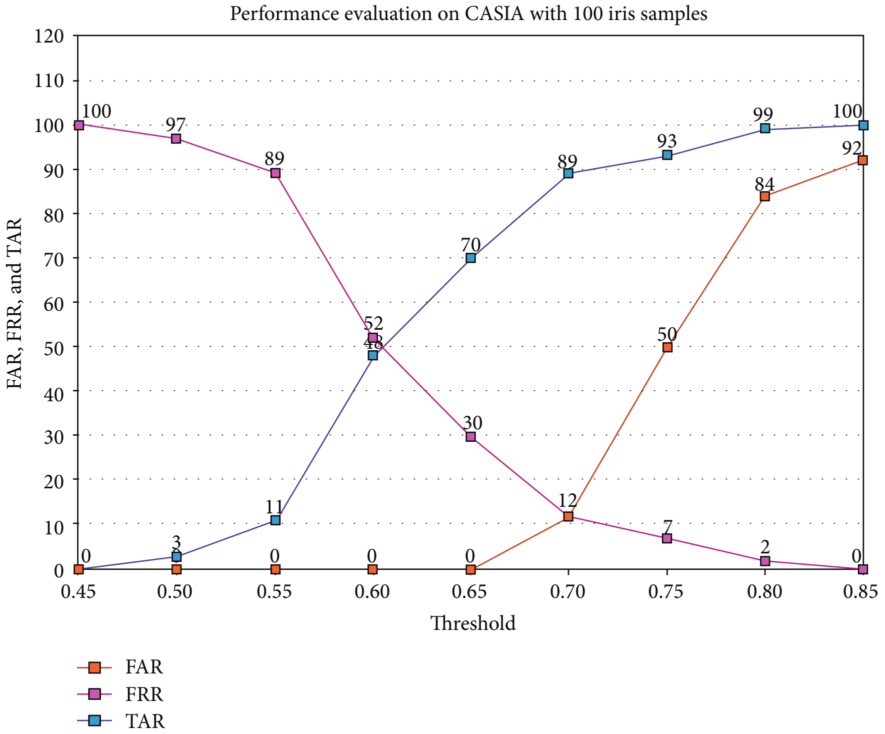

FIGURE 12: Plot of FAR, FRR, and TAR with varying threshold on CASIA dataset with 100 iris images.

system having i5 processor and 8 GB RAM. The experimental set up of proposed method is divided into training set and test set. From the two datasets, CASIA and IITD iris, 9 images were taken for training, and one image is used for testing. The following five metrics are considered for determining the effectiveness of the proposed research. They are false acceptance rate (FAR), false rejection rate (FRR), true acceptance rate (TAR), equal error rate (EER), and accuracy.

(i) False acceptance rate (FAR): it is the probability where the biometric system fallaciously accepts the unauthorized user. It happens when biometric system inaccurately matches the cipher template of user with the stored cipher template in database.

(ii) False rejection rate (FRR): it is the probability where the biometric system refuses access to the authorized user. It happens when biometric system fails to match the cipher template of user with the stored cipher template in database.

(iii) True acceptance rate (TAR): it is the probability in where the biometric system correctly recognize the authorized user.

(iv) Equal error rate (EER): the rate in which FAR meets FRR is known as ERR.

(v) Accuracy: refers to number of legitimate users granted access to the number of attempts for authentication.

5.1. Performance Evaluation of Proposed Methodology without Fuzzy Logic. The performance measure of proposed system without fuzzy logic is evaluated. In this case, instead of fuzzy logic, general hamming distance calculation is used to compare the encrypted iris on verification phase. The equation of hamming distance is given as

$$D(s, t) = \sqrt{\sum_{i=1}^{n} (s_i - t_i)^2}, \tag{6}$$

where s_i is the cipher template stored in database and t_i is the cipher template of test iris image.

5.1.1. Performance Evaluation on CASIA Iris Thousand Dataset. To understand the feasibility of proposed method, 50 persons' iris samples from CASIA Iris Thousand dataset are taken, and parameters such as FAR, FRR, ERR, TAR, and accuracy are computed for variation of threshold values as shown in Table 1. From the analysis, it is witnessed that the proposed method has maximum TAR of 100% and optimum TAR of 87%. The average EER in the proposed method on CASIA dataset is 4% at threshold 0.70. The graphical representation of performance metrics is specified in Figures 7 and 8.

5.1.2. Performance Evaluation of Proposed Method on IITD Iris Dataset. To understand the feasibility of proposed method, 50 persons' iris samples from IITD iris dataset are taken, and parameters such as FAR, FRR, ERR, TAR, and accuracy are computed for variation of threshold values as shown in Table 2. From the analysis on IITD iris data, it is inferred that the proposed methods have maximum TAR of 100%. The EER of 4% is identified at the threshold 0.70 with optimum TAR of 88%. The graphical representation of performance metrics is specified in Figures 9 and 10.

Table 4: Performance evaluation with varying thresholds on IITD iris dataset.

Threshold	50 iris samples			100 iris samples		
	FAR	FRR	TAR	FAR	FRR	TAR
0.45	0	50	0	0	100	0
0.50	0	44	12	0	93	7
0.55	0	36	28	0	79	21
0.60	0	22	56	0	52	48
0.65	0	19	62	0	38	62
0.70	5	5	90	13	13	87
0.75	19	1	98	37	7	93
0.80	36	0	99	63	0	99
0.85	50	0	100	97	0	100

5.2. Performance Evaluation of Proposed Methodology Using Fuzzy Logic. The proposed technique with fuzzy logic is analyzed on both CASIA Iris and IITD dataset. From the analysis, it is proved that fuzzy logic provides enhanced accuracy and less ERR.

5.2.1. Performance Evaluation of Proposed Method on CASIA Iris Thousand Dataset. To understand the feasibility of proposed method, 50 persons' iris samples from CASIA Iris Thousand dataset are taken, and parameters such as FAR, FRR, ERR, TAR, and accuracy are computed for variation of threshold values as shown in Table 3. From the analysis, it is witnessed that the proposed method has maximum TAR of 100% and optimum TAR of 91%. The average EER in the proposed method on CASIA dataset is 2.5% at threshold 0.70. The graphical representation of performance metrics is specified in Figures 11 and 12.

5.2.2. Performance Evaluation of Proposed Method on IITD Iris Dataset. To understand the feasibility of proposed method, 50 persons' iris samples from IITD iris dataset are taken, and parameters such as FAR, FRR, ERR, TAR, and accuracy are computed for variation of threshold values as shown in Table 4. From the analysis on IITD iris data, it is inferred that the proposed methods have maximum TAR of 100%. The EER of 2.5% is identified at the threshold 0.70 with optimum TAR of 90%. The graphical representation of performance metrics is specified in Figures 13 and 14.

5.3. Comparison of Accuracy and Maximum TAR of Proposed Method with Existing Methods. Table 5 shows the EER, maximum TAR, optimum TAR, and accuracy of proposed method on both CASIA Iris and IITD iris datasets. The recognition time of proposed method is specified in seconds. The comparison denotes that methodology with fuzzy logic has less error rate and more optimal. The performance metric of the proposed scheme is compared with the state-of-art existing scheme in view of accuracy and maximum TAR as shown in Table 6.

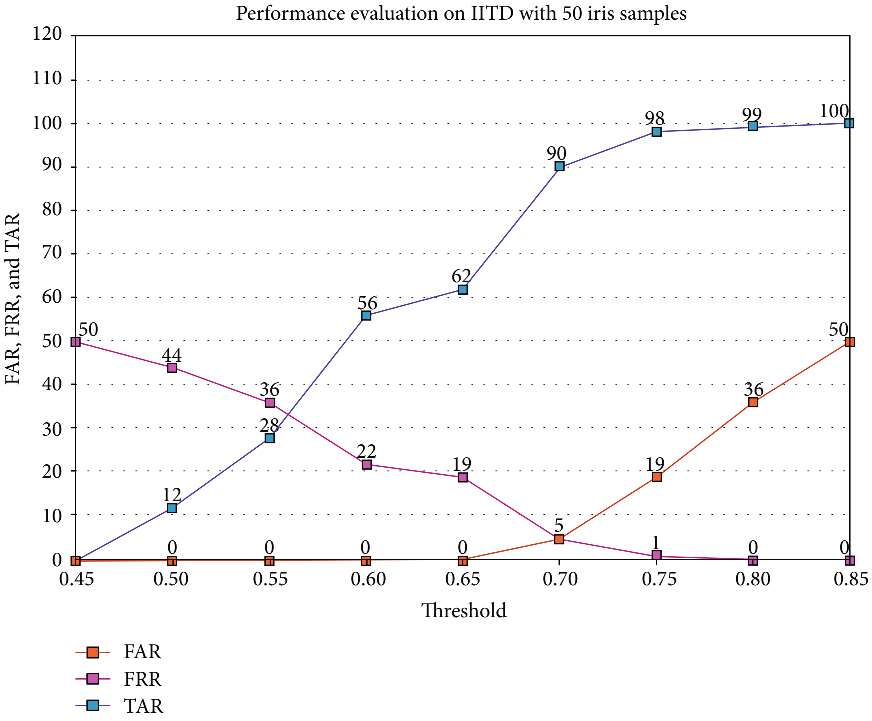

Figure 13: Plot of FAR, FRR, and TAR with varying threshold on IITD dataset with 50 iris images.

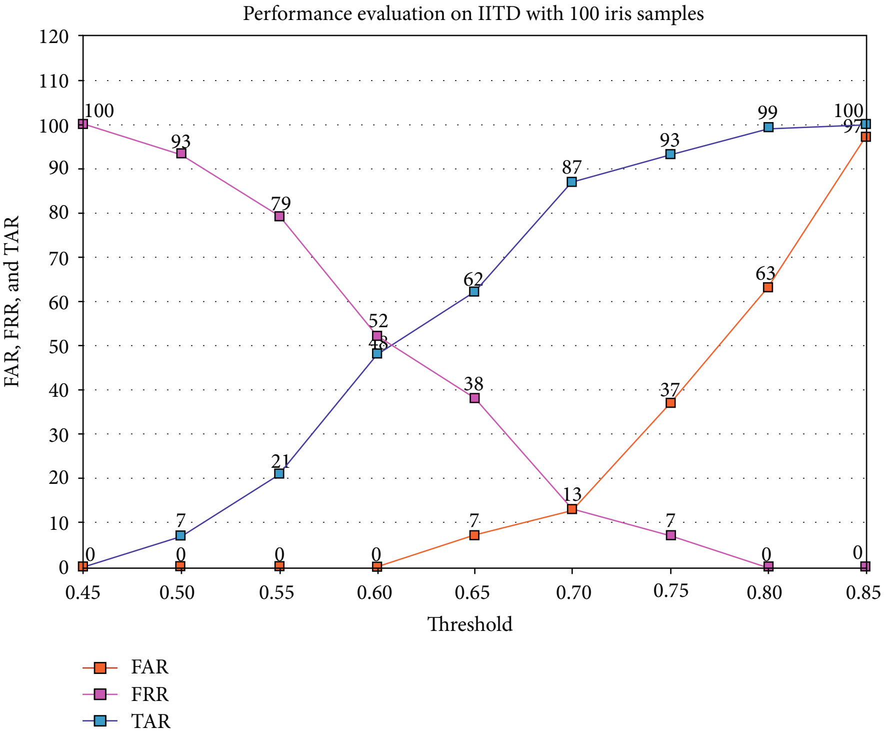

Figure 14: Plot of FAR, FRR, and TAR with varying threshold on IITD dataset with 100 iris images.

6. Conclusion and Future Work

The proposed study presented a two novel approach such as 2D Gabor kernel for feature extraction and HECC approach for encrypting original iris template to cipher templates. The major need of encrypting the iris template is to avoid the compromising of template database by the attacker. The research has been implemented on CASIA Iris V4 and IITD

Table 5: Performance parameters of proposed method on both iris dataset.

Methodology	Dataset used	EER	Maximum TAR	Optimum TAR	Accuracy	Recognition time (sec)
Proposed technique without fuzzy logic	CASIA Iris Thousand	4%	100%	87%	99.68%	3.4 s
	IITD iris	4%	100%	88%	99.70%	3.2 s
Proposed technique using fuzzy logic	CASIA Iris Thousand	2.5%	100%	91%	99.78%	3 s
	IITD iris	2.5%	100%	90%	99.7%	3 s

Table 6: Accuracy and maximum TAR of proposed and existing authentication schemes.

Methods	Dataset used	Algorithm used	Maximum TAR	Accuracy
Deepanshu kumar et al. [23]	MMU	DWT+DCT	75.59%	80%
N.L. Manasa et al.	CASIA	LBP score level fusion	97%	98.2%
Mohamed Abdolahi et al. [24]	CASIA	Fuzzy logic	93%	97.5%
Gayathri et al. [25]	IITK iris	Fusion technique	87%	99.2%
Velmurugan et al. [26]	CASIA and IITD iris	DCT wavelet technique	91%	99.4%
Fernando et al. [27]	CASIA internal v-3	2D Gabor	99.8%	99%
Mohamed Hamaz Abed [28]	CHUK iris	DWT and cosine	99.25%	98%
Serestina et al. [29]	CASIA and UBIRIS	Vote-based strategies	96%	99.6%
Proposed iris recognition without fuzzy logic	CASIA and IITD iris	2D Gabor + HECC	100%	99.69%
Proposed iris recognition using fuzzy logic	CASIA and IITD iris	2D Gabor + HECC+ fuzzy logic	100%	99.74%

iris dataset. More attention has been given on evaluating the efficiency of the proposed algorithm. The result analysis witnessed that the proposed research has maximum TAR of 100%, less ERR of 2.5%, and enhanced accuracy of 99.74% with very less recognition time of 3 seconds. The method also outperforms the existing iris authentication techniques by means of accuracy and maximum TAR. Because of such higher accuracy and security, the proposed study will find its applications in military applications, border control applications, banking, Aadhar, etc. Future work will investigate on implementing soft computing approaches along with fuzzy in biometric recognition.

Data Availability

The dataset used for experimental analysis are CASIA Iris V-4 and IITD Dataset which is publically available.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. A. Ch, N. uddin, M. Sher, A. Ghani, H. Naqvi, and A. Irshad, "An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography," *Multimedia Tools and Applications*, vol. 74, no. 5, pp. 1711–1723, 2015.

[2] S. A. Ch, N. Nizamuddin, and M. Sher, "Public verifiable signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem," in *Information Systems, Technology and Management. ICISTM 2012*, S. Dua, A. Gangopadhyay, P. Thulasiraman, U. Straccia, M. Shepherd, and B. Stein, Eds., vol. 285 of Communications in Computer and Information Science, Springer, Berlin, Heidelberg, 2012.

[3] G. Aparna Gale and S. S. Salankar, "Evolution of performance analysis of iris recognition system by using hybrid methods of feature extraction and matching by hybrid classifier for iris recognition system," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, India, 2016.

[4] N. D. Kalka, Jinyu Zuo, N. A. Schmid, and B. Cukic, "Estimating and fusing quality factors for iris biometric images," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 40, no. 3, pp. 509–524, 2010.

[5] Z. Sun, H. Zhang, T. Tan, and J. Wang, "Iris image classification based on hierarchical visual codebook," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 36, no. 6, pp. 1120–1133, 2014.

[6] Y. Li, "Iris recognition algorithm based on MMC-SPP," *International Journal of signa processing, image processing and pattern recognition*, vol. 8, no. 2, 2015.

[7] V. Rajasekar, J. Premalatha, and K. Sathya, "An efficient signcryption scheme for secure authentication using hyper elliptic curve cryptography and Keccak hashing," *International Journal of Recent Technology and Engineering*, vol. 8, no. 3, pp. 1593–1598, 2019.

[8] S. Zhou and J. Sun, "A novel approach for code match in iris recognition," in *2013 IEEE/ACIS 12th International Conference on Computer and Information Science (ICIS)*, pp. 123–128, Niigata, Japan, 2013.

[9] J. Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, 2004.

[10] A. Poursaberi and B. N. Araabi, "Iris recognition for partially occluded images: methodology and sensitivity analysis,"

Eurasip Journal on Advances in Signal Processing, vol. 2007, Article ID 036751, 2006.

[11] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveliness detection based on quality related features," in *IEEE Biometrics Compendium, IEEE RFIC Virtual Journal, IEEE RFID Virtual Journal*, pp. 271–276, New Delhi, India, 2012.

[12] B. K. Gul and Ç. Kurnaz, "The impact of coding and noise on iris recognition system performance," in *2016 24th Signal Processing and Communication Application Conference (SIU)*, Zonguldak, Turkey, 2016.

[13] J. Daugman, "Iris recognition at airports and border crossings," *Encyclopedia of Biometrics*, pp. 819–825, 2009.

[14] N. Ahmadi and G. Akbarizadeh, "Hybrid robust iris recognition approach using iris image pre-processing, two-dimensional gabor features and multi-layer perceptron neural network/PSO," *IET Biometrics*, vol. 7, no. 2, pp. 153–162, 2017.

[15] I. Tomeo-Reyes, A. Ross, D. Antwan Clark, and V. Chandran, "A biomedical approach to iris normalization," in *International Conference on Biometrics*, pp. 9–16, Thailand, 2015.

[16] A. Dixit, S. Pathak, and R. Raj, "An efficient fuzzy based edge estimation for iris localization and pupil detection in human eye for automated cataract detection system," in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Bangalore, India, 2018.

[17] N. Malarvizhi, P. Selavarani, and P. Raj, "Adaptive fuzzy genetic algorithm for multi biometric authentication," *Multimedia Tools and Applications*, vol. 79, no. 13-14, pp. 9131–9144, 2020.

[18] S. Adamović, V. Miškovic, N. Maček et al., "An efficient novel approach for iris recognition based on stylometric features and machine learning techniques," *Future Generation Computer Systems*, vol. 107, pp. 144–157, 2020.

[19] M. Saracevic, S. Adamovic, and E. Bisevac, "Applications of Catalan numbers and lattice path combinatorial problem in cryptography," *Acta Polytechnica Hungarica*, vol. 15, no. 7, pp. 91–110, 2018.

[20] "CASIA V.4 iris image database version three," http://www.cbsr.ia.ac.cn.

[21] A. Kumar and A. Passi, "Comparison and combination of iris matchers for reliable personal identification," in *2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pp. 21–27, Anchorage, AK, USA, 2008.

[22] "CASIA," http://biometrics.idealtest.org.

[23] D. Kumar, M. Sastry, and K. Manikantan, "Iris recognition using contrast enhancement and spectrum-based feature extraction," in *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, pp. 1–7, Pudukkottai, India, 2016.

[24] A. Mohamed, M. Majid, and J. Mehdi, "Multimodal biometric system fusion using fingerprint, iris with fuzzy logic," *International Journal of Soft Computing and Engineering*, vol. 2, no. 6, 2013.

[25] R. Gayathri and P. Ramamoorthy, "Feature level fusion of palm print and iris," *International Journal of Computer Science Issues*, vol. 9, no. 4, p. 1, 2012.

[26] S. Velmurugan and S. Selvarajan, "A multimodal authentication for biometric recognition system using hybrid fusion techniques," *Cluster Computing*, vol. 22, no. S6, pp. 13429–13436, 2019.

[27] B. Fernando, M. Glasston, L. Eduardo, H. C. Paulo, and A. Gaurda, "Exploring the scalability of multiple signatures in iris recognition using GA on the acceptance of frontier search," in *2017 IEEE Congress on Evolutionary Computation (CEC)*, pp. 1843–1847, San Sebastian, Spain, 2017.

[28] M. H. Abed, "Iris recognition model based on principal component analysis and two levels Haar wavelet transform," *Case study CUHK and UTIRIS databases*, pp. 485–500, Journal of college of education, 2017.

[29] S. Viriri and J. Tapamo, "Iris pattern recognition based on cumulative sums and majority vote methods," *International journal of Advanced Robotics Systems*, vol. 14, no. 3, p. 172988141770393, 2017.