IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 42, No. 4, August, 2025, pp. 2097-2105
Journal homepage: http://iieta.org/journals/ts

Generative Information Hiding of Iris Feature Data via Gaussian Fuzzy Processing and Advanced Encryption Standard-Based Encryption

Shuchen Zhou[1*], Dingyi Liu[2]

[1] Institute of International Education, Huanghuai University, Zhumadian 463000, China
[2] Department of Cybersecurity, Henan Police College, Zhengzhou 450046, China

Corresponding Author Email: 20101192@huanghuai.edu.cn

https://doi.org/10.18280/ts.420422

Received: 25 December 2024
Revised: 19 June 2025
Accepted: 28 June 2025
Available online: 14 August 2025

Keywords:
gaussian fuzzy algorithm, iris biometric features, Gabor wavelet, Advanced Encryption Standard (AES) encryption, information hiding, feature extraction, image preprocessing

ABSTRACT

Conventional methods for hiding iris feature data have been hindered by inefficient feature extraction processes and inadequate post-hiding information security, thereby limiting both performance and applicability. To address these challenges, a generative information hiding approach for iris feature data has been developed, based on a Gaussian fuzzy algorithm and Advanced Encryption Standard (AES) encryption. In the preprocessing phase, a weighted averaging technique was employed for greyscale conversion, followed by Gaussian fuzzy smoothing to reduce noise while preserving structural integrity. Subsequent image sharpening was conducted using a Laplacian convolution kernel to enhance edge definition. The iris region was then localized and normalized to a fixed size, ensuring geometric invariance during feature extraction. Two-dimensional Gabor wavelets were utilized for the extraction of robust and discriminative iris features, given their proven effectiveness in capturing both spatial frequency and orientation information. To ensure data confidentiality, the extracted iris features were encrypted using the AES, with a corresponding decryption process integrated within the generative information hiding framework. This dual-layer strategy ensured that both the biometric feature data and the hidden information remained secure against unauthorized access or reconstruction. Experimental validation demonstrated that the proposed method enabled iris feature extraction within ten seconds on standard computing hardware, with a significantly improved data security coefficient compared to conventional techniques. Furthermore, the proposed methodology achieved a high level of imperceptibility and robustness, supporting its application in biometric security systems and privacy-preserving identity verification. These findings suggest that the integration of Gaussian fuzzy processing with secure encryption offers an effective pathway for reliable and efficient iris feature data concealment.

1. INTRODUCTION

Among various biometric identification technologies, iris recognition has garnered increasing attention due to its superior accuracy, high security, and inherent resistance to forgery and ageing effects [1]. Studies have demonstrated that iris recognition systems exhibit the lowest error rates among all biometric modalities [2]. Furthermore, iris acquisition procedures are generally non-invasive and straightforward, rendering the technology suitable for both high-security and large-scale applications. Mature iris recognition systems have already been deployed in military and enterprise domains, while large-scale national implementations, such as India's nationwide iris identity database, have further underscored the practicality of this approach in real-world scenarios. In civil applications, iris-based access control and attendance management systems have been preliminarily adopted, highlighting the expanding utility of this modality [3, 4]. In parallel with the growth of biometric technologies, the importance of information security has become increasingly evident in the digital era [5]. As a result, the secure concealment and transmission of sensitive biometric feature data—particularly iris features—has emerged as a focal point within the domain of information hiding. The technique known as generative information hiding, which integrates feature extraction and encryption within a single unified framework, is receiving significant research interest.

Several methodologies have been introduced to advance the field of information hiding. Liu et al. [6] proposed a generative adversarial network (GAN)-based approach, in which secret information is used to replace class labels as a generator input, enabling the synthesis of stego-images for covert transmission. The embedded information is subsequently recovered through a discriminator. Although this method eliminates the need for an explicit carrier, it suffers from high computational complexity and low hiding efficiency. Zheng et al. [7] proposes an improved TIN iterative encryption filtering algorithm (AGPTD) based on adaptive mesh, which dynamically selects optimal initial seed points through adaptive mesh partitioning and iteratively refines the TIN model through progressive encryption. While demonstrating strong adaptability in complex terrains, the algorithm shows reduced modeling accuracy in scenarios with insufficient feature points (low vegetation areas) and elevation abruptions (steep slopes), requiring further optimization through multi-source data fusion. Kaur et al. [8] introduced the CMNT scheme, while the CNT cryptographic primitives were specifically developed for Fully Homomorphic Encryption (FHE) over integers. These schemes have shown remarkable strengths in the realm of integer-based FHE, especially in reducing public key size and enhancing computational efficiency. Nevertheless, they still encounter several challenges, including significant computational overhead, intricate noise management, and considerable implementation complexity. Despite these obstacles, ongoing advancements in cryptographic research and continuous optimization of techniques are expected to broaden their applications in the future. They hold great promise in providing robust support for secure data processing in complex environments, such as cloud computing. Jiang et al. [9] explored a chaotic Z-mapping-based approach, encrypting feature data through key-based transformations. However, its encryption process is time-consuming, thereby diminishing the overall efficiency of information hiding.

To overcome the limitations associated with the aforementioned methods—namely high computational cost, inadequate security, and poor feature extraction efficiency—a generative information hiding method for iris feature data based on a Gaussian fuzzy algorithm is proposed. In the preprocessing phase, a weighted average greyscale conversion is employed, followed by Gaussian fuzzy smoothing to suppress noise and enhance feature consistency. The Laplacian operator is then applied to sharpen image edges, thereby facilitating more precise iris region localization. Subsequent normalization of the iris region ensures spatial invariance, enabling robust feature extraction using two-dimensional Gabor wavelets. The extracted iris feature data is securely encrypted and decrypted using the AES, thereby achieving both concealment and protection of sensitive biometric information. Experimental evaluations have demonstrated that the proposed approach significantly reduces feature extraction time while improving the security coefficient, thereby offering a viable solution for efficient and secure biometric data hiding.

2. IRIS IMAGE PREPROCESSING BASED ON GAUSSIAN FUZZY ALGORITHM

2.1 Image gray processing

The method of hiding generative information of iris feature data based on the Gaussian fuzzy algorithm employs the weighted average technique to convert the image to grayscale. The weighted average is an empirical greyscale conversion method grounded in the principle that the human eye's colour-sensitive cells are most responsive to green and less sensitive to blue. Based on this characteristic, different weights are assigned to the red, green, and blue components when converting the image to grayscale. As the human eye is most sensitive to green, the highest weight is allocated to the green channel, followed by red, and finally blue [10]. The weighting formula is:

$$\begin{aligned} Gray(i,j) = 0.299 * R(i,j) + 0.578 \\ * G(i,j) + 0.114 * B(i,j) \end{aligned} \tag{1}$$

All the coefficients in Formula (1) are empirical coefficients.

2.2 Image smoothing

Image smoothing is a process of averaging the neighborhoods of image pixels, which has the effect of blurring pixels, so it is also called image blurring or image filtering [11]. The method of hiding generative information of iris feature data based on the Gaussian fuzzy algorithm smooths the image by the Gaussian fuzzy algorithm. According to the two-dimensional Gaussian function, the weight of each position in the convolution template can be obtained.

$$G(x,y) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2} \tag{2}$$

In Formula (2), x and y represent the distance from the neighborhood pixel to the center pixel. Parameter σ represents the standard deviation of the pixel, which defines the dispersion degree of pixel distribution. The larger the value of σ, the more dispersive the data, the better the smoothness of the image, but the smoothed image is more blurred. The smaller the value of σ, the more centralized the data distribution, the worse the noise reduction effect [12], the clearer the smoothed image. $G(x,y)$ denotes the weight of each point.

In the Gaussian filtering process, the assigned weight is inversely related to the distance from the central pixel—pixels closer to the center are given higher weights. For computational purposes, neighborhood pixels within a distance of less than one unit may be selected, which typically includes the pixels directly above, below, to the left, and to the right of the central pixel. Alternatively, neighborhood pixels within a distance of less than two units can be used, encompassing all eight surrounding pixels, commonly referred to as the 8-neighbourhood. While increasing the neighborhood size can improve smoothing performance, it also significantly increases computational complexity and reduces processing efficiency. In practice, the 8-neighbourhood is generally sufficient for effective filtering. These neighborhood regions are represented using convolution templates, also known as convolution kernels [13]. The 8-neighbourhood Gaussian convolution template takes the form of a 3×3 matrix, and the method for generating this template is described as follows:

(1) Set the center point of the template as the origin point and get the coordinate value of each position in the template (see Figure 1).

（-1,1）	（0,1）	（1,1）
（-1,0）	（0,0）	（1,0）
（-1,-1）	（0,-1）	（1,-1）

Figure 1. Gaussian convolution kernel

(2) The coordinate values are substituted into Formula (3) to calculate the values of coefficients in the template. The parameter value of σ is generally 0.8.

$$\nabla^2 f = \frac{\partial^2 f}{\partial^2 x^2} + \frac{\partial^2 f}{\partial y^2} \tag{3}$$

(3) The results calculated by the Gaussian function are all decimal, which is not convenient for the following calculation, so it is necessary to normalize the results. For normalization, a basic parameter needs to be selected at first. There is no special requirement for the position of this parameter. The result of any neighborhood can be selected as the normalization reference parameter [14]. The result of the upper left corner is selected as the benchmark in the proposed method.

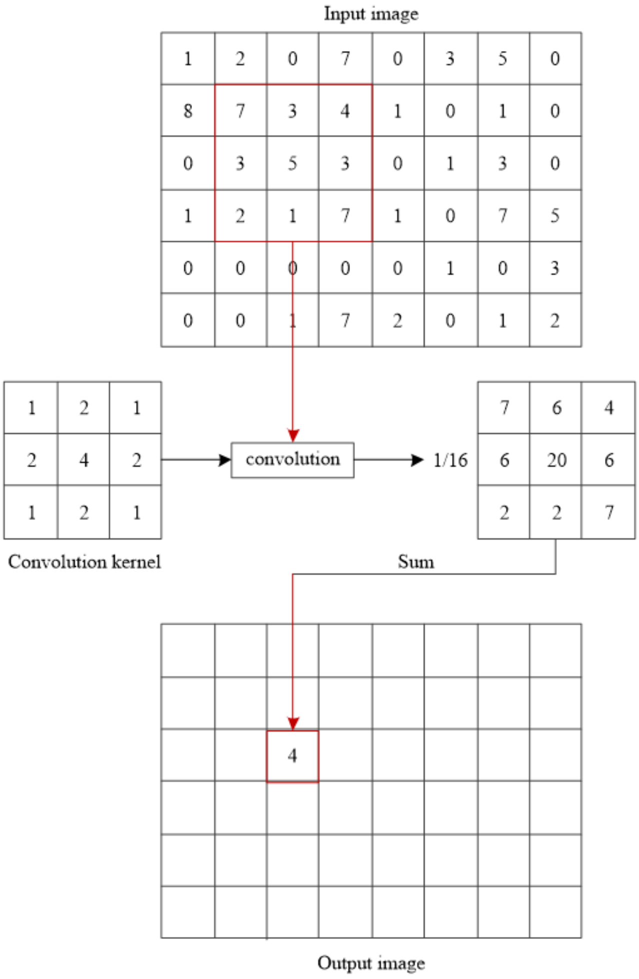


Figure 2. Convolution operation

The steps for normalization are as follows: the reciprocal of the coefficient in the upper-left corner of the template is first taken as the normalization coefficient. Each value in the template is then multiplied by this coefficient, followed by rounding to the nearest integer. This process yields a 3×3 Gaussian convolution template:

$$\frac{1}{16}\begin{bmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 1 \end{bmatrix} \tag{4}$$

After getting the Gaussian convolution template, it is necessary to use the template to smooth the image. The method of smoothing operation is to use the image to convolve with the template. The concept of convolution originates from signal processing, which can combine two signals to produce a third signal. The convolution is often used to calculate signal attenuation in engineering neighborhoods [15]. In addition, the image can be regarded as a two-dimensional function and a discrete signal, so the convolution can also be adopted for image processing. The operation of image convolution is not complicated. Firstly, a convolution kernel (Gaussian template) is used to overlap the convolution template and the source image from the upper left corner of the source image, and then the corresponding pixels are multiplied. After that, all the results in the convolution kernel are added, and then we can get some pixel values, which can replace the pixel values of the original center point. Overall, it is a process of convolution kernel accumulation, replacement and translation on image [16]. Thus, the image convolution is defined as follows:

$$H(x,y) = \sum_{i=0}^{M_i-1}\sum_{j=0}^{M_{j-1}} I(x+i-a_i, y+j-a_j)G(i,j) \tag{5}$$

The convolution operation is shown in Figure 2.

2.3 Image sharpening

In the proposed method, a Laplacian convolution kernel was used to sharpen the image [17]. The Laplacian operator is a two-dimensional isotropic measure of the second-order spatial derivative of an image. The Laplacian operator can highlight the region where the intensity changes rapidly, so it is often applied in edge detection tasks. The Laplace operator belongs to isotropic differential operators. It is very simple, but it has the feature of rotation invariance. Assuming that the image is a two-dimensional function *f*(*x*,*y*), the Laplacian operator is defined as:

$$\nabla^2 f = \frac{\partial^2 f}{\partial^2 x^2} + \frac{\partial^2 f}{\partial y^2} \tag{6}$$

In the direction *x*, the second-order differential operation is defined as:

$$\frac{\partial^2 f}{\partial x^2} = f(x+1,y) + f(x-1,y) - 2f(x,y) \tag{7}$$

In the direction *y*, the second-order differential operation is defined as:

$$\frac{\partial^2 f}{\partial^2 y^2} = f(x,y+1) + f(x,y-1) - 2f(x,y) \tag{8}$$

Combined with the above formula, the second-order Laplacian operator of two-dimensional image is obtained.

$$\begin{aligned}\nabla^2 f(x,y) &= f(x+1,y) + f(x-1,y) \\ &+ f(x,y+1) + f(x,y-1) - 4f(x,y)\end{aligned} \tag{9}$$

Finally, the mathematical formula of an image sharpened by the Laplacian operator can be obtained:

$$g(x,y) = f(x,y) + c[\nabla^2 f(x,y)] \tag{10}$$

In Formula (10), *f*(*x*,*y*) represents the input image, and *g*(*x*,*y*) denotes the sharpened image. *c* is a constant coefficient, and it is generally one.

According to the second-order Laplacian operator, the sharpened convolution kernel can be obtained (Figure 3).

0	1	0
1	-4	1
0	1	0

Figure 3. Sharpened convolution kernel

3. GENERATIVE INFORMATION HIDING METHOD OF IRIS FEATURE DATA

3.1 Iris feature data extraction

(1) Normalization of iris region

I(*x*,*y*) represents the original iris image before normalization. *I*(*r*,*θ*) represents the iris rectangular image converted by normalization. (*x*,*y*) represents the coordinate value of the point on the iris image in the rectangular coordinate system before normalization. (*r*,*θ*) represents the polar coordinate value of the point, taking the pupil circle center as the reference point. The iris boundary circle center does not coincide with the pupil, so the value of (*r*,*θ*) is calculated by the pupil center and the boundary circle center. $[x_p(\theta), y_p(\theta)]$ and $[x_i(\theta), y_i(\theta)]$ denote the corresponding points with the pupil as the reference point on the inner and outer boundaries of the iris, when the angle is *θ*, and then the coordinates are normalized:

$$x(\rho,\theta) = (1-\rho) * x_\rho(\theta) + \rho * x_i(\theta) \tag{11}$$

$$y(\rho,\theta) = (1-\rho) * y_\rho(\theta) + \rho * y_i(\theta) \tag{12}$$

Thus, the iris is regarded as an elastic region, and then the points in the iris region can be denoted by the weighted coordinates of the inner and outer boundaries of the iris.

$$I[x(\rho,\theta), y(\rho,\theta)] \rightarrow I(r,\theta) \tag{13}$$

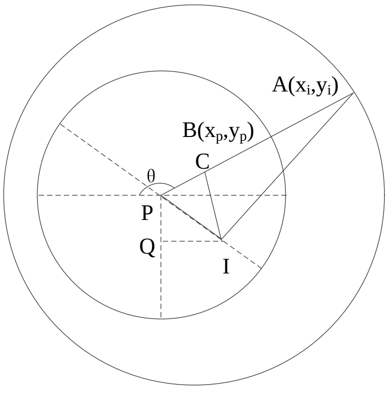


Figure 4. Normalized geometric model of iris

In this way, the points with the same weight can be located on the same circumference, even if these points are not on the same circle in the actual iris image. After weighting, the points with the same weight in the iris region are mapped to the same circumference in rectangular coordinates, so that the points on the whole iris can be mapped to a rectangle with the same size and specifications one by one [18].

The geometric relationship among the inner boundary point, outer boundary point, pupil reference point and outer boundary circle center is shown in Figure 4.

In Figure 4, *I* is the center of the outer boundary of the iris. *P* is the reference point of the pupil. *P* is the starting point, and it rotates θ°anticlockwise relative to the horizontal direction, and then the intersection points (*A* and *B*) with the inner and outer boundaries of the iris can be obtained. Thus, the points on the line segment *AB* can be represented by the weight of *A* and *B*. The *PA* vertical line is drawn through *I*. Respectively, *IQ* and *PQ* represent the horizontal distance and vertical distance between the outer boundary point of the iris and the reference point of the pupil. *PB* is the pupil radius r_p. *PA* is the radius R_I of the outer boundary, and they are known. *PIC* and *AIC* are the right triangle. Let *ϕ* be the angle *∠IPC* between the line between pupil center and outer boundary center and the horizontal direction. *Δr* is the distance between the two lines. As long as the length of *PA* is calculated, the normalization parameters corresponding to the pixels in the iris region can be calculated by the elastic model. According to the geometric relationship, we can see that:

$$\phi = \arctan\left(\frac{PQ}{IQ}\right) \tag{14}$$

$$\Delta r = \sqrt{PQ^2 + IQ^2} \tag{15}$$

$$\angle IPC = \pi - \theta + \phi \tag{16}$$

For right triangle *IPC*:

$$PC = \Delta r \cos(\pi - \theta + \phi) \tag{17}$$

For right triangle *IAC*:

$$\begin{aligned} AC &= \sqrt{IA^2 - IC^2} \\ &= \sqrt{R_I^2 - (\Delta r^2 - (\Delta r \cos(\pi - \theta + \phi))^2)} \end{aligned} \tag{18}$$

Based on above formulas, *PA* is:

$$\begin{aligned} PA = PC + AC = \Delta r \cos(\pi - \theta + \phi) \\ + \sqrt{R_I^2 - (\Delta r^2 - (\Delta r \cos(\pi - \theta + \phi))^2)} \end{aligned} \tag{19}$$

In Formula (19), *PA* takes the pupil center as the reference point. When the angle on iris region is *θ*, the corresponding normalized outer boundary is *R*(*θ*). Let *N* represent the number of angle samples when expanding, and *M* is the number of radius samples. The specific value depends on the size of the picture and the required recognition accuracy. The larger the collected image is, the larger the value of *N* and *M*, so that the detail texture of the iris can be fully expanded. Meanwhile, it is necessary to increase the value of these two values during the high-precision recognition. Otherwise, some texture information will be normalized to a point, leading to iris information loss. The process of normalizing the iris region to an *M*×*N* rectangle region is shown as follows:

Step 1: the parameter equation $(x_p, y_p, r_p), (x_o, y_o, R_I)$ of the inner and outer boundary of the iris image *I*(*x*,*y*) is established through the positioning algorithm. Respectively, r_p and R_I represent the radiuses of the inner and outer boundaries of the iris.

Step 2: calculate the angle ϕ between the line between pupil center and boundary center and the horizontal direction, as well as the distance Δr between the iris boundary center and the pupil center:

$$\begin{cases} \phi = \arctan \dfrac{y_p - y_o}{x_p - x_o} \\ \Delta r = \sqrt{(x_p - x_o)^2 + (y_p - y_o)^2} \end{cases} \tag{20}$$

Step 3: the iris is elastic. When the pupil is opening and closing, the change of each point is linear [19]. When the pupil center is taken as the reference point to expand, all points on the iris inner boundary are located on the circumference with the same radius, which takes the reference point as the center. In other words, all points on the inner boundary have the same radius to expand. However, the center of the iris outer boundary does not coincide with the reference point, and there is a position deviation. When angles are different, different points on the iris outer boundary have different radii during coordinate conversion, so the outer boundary of each point in the iris region is shown as follows:

$$\begin{cases} \theta = j \times \dfrac{\pi}{180} \\ R(\theta) = \Delta r \cos(\pi - \theta + \phi) \\ + \sqrt{R_I^2 - \Delta r^2 + (\Delta r \cos(\pi - \theta + \phi)^2)} \end{cases} \tag{21}$$

Step 4: the final iris region can be normalized as follows:

$$\begin{cases} R_p = \left(1 - \dfrac{i}{M+1}\right) \times r(\theta) + \dfrac{i}{M+1} \times R(\theta) \\ x = X_p + R_p \cos(\theta) \\ y = Y_p + R_p \sin(\theta) \end{cases} \tag{22}$$

In Formula (22), i=1,2,⋯,M; j=1,2,⋯,N; θ=j×π/180. After the normalization, any point on the iris region can be regarded as a linear combination of internal and external boundary radii:

$$R_P = (\theta, \rho) = (1 - \rho) r(\theta) + \rho R(\theta) \tag{23}$$

In Formula (23), $r(\theta)$ denotes the inner boundary radius of the iris. $R(\theta)$ denotes the outer boundary radius of the iris. ρ is the normalized weighting coefficient. When ρ=0, this point is the point of the outer boundary of the iris. When ρ=1, it means that it is exactly the point of the outer boundary of the iris. ρ changes in intervals [0,1], the iris region can be normalized to the weight of the inner and outer boundaries. ρ determines the width of the normalized rectangle and θ determines the length of the normalized rectangle.

(2) Iris feature extraction

The method of hiding generative information of iris feature data based on the Gaussian fuzzy algorithm uses 2D Gabor wavelets to extract the iris feature. The filtering result is a complex number, so that the real part and the virtual part can be coded by phases, and the binary feature code of the iris can be obtained [20]. The formula for calculating a Gabor filter is:

$$h_{\{R_e, I_m\}} = \mathrm{sgn}_{\{R_e, I_m\}} \iint_{\rho\phi} I(\rho, \theta) e^{-i\omega(\theta_0 - \theta)} e^{-(r_0 - \rho)^{\frac{2}{\alpha^2}}} \rho d\rho d\theta \tag{24}$$

In Formula (24), $I(\rho,\theta)$ denotes the iris image. Let *Code* represent the final iris code, then:

$$Code = (B_1, B_2, B_3, \mathrm{K}, B_j, \mathrm{K}, B_k) \tag{25}$$

In Formula (25), B_j represents the phase code generated by Gabor filtering for each pixel. It is also a 2-bit encoding of four combinations of 0 and 1. The real part and virtual part of $h_{\{R_e,I_m\}}$ are represented by h_r and h_i respectively, and the value of the corresponding iris feature code b_j is:

$$\begin{cases} h_r > 0, h_i > 0 \\ h_r > 0, h_i < 0 \\ h_r < 0, h_i > 0 \\ h_r < 0, h_i < 0 \end{cases} \Rightarrow \begin{cases} b_j = 11 \\ b_j = 10 \\ b_j = 01 \\ b_j = 00 \end{cases} \tag{26}$$

3.2 Information hiding

The method of hiding generative information of iris feature data based on the Gaussian fuzzy algorithm realizes the information hiding by encrypting iris feature data. The process of information encryption and decryption is shown in Figure 5 and Figure 6.

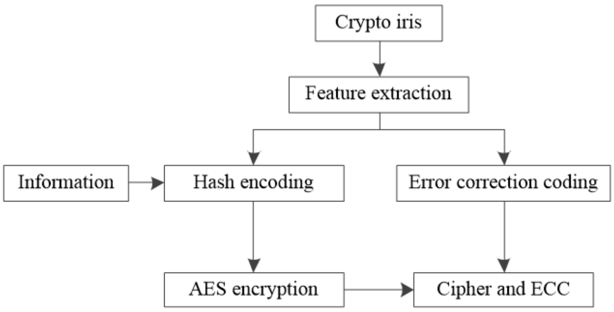


Figure 5. Encryption framework

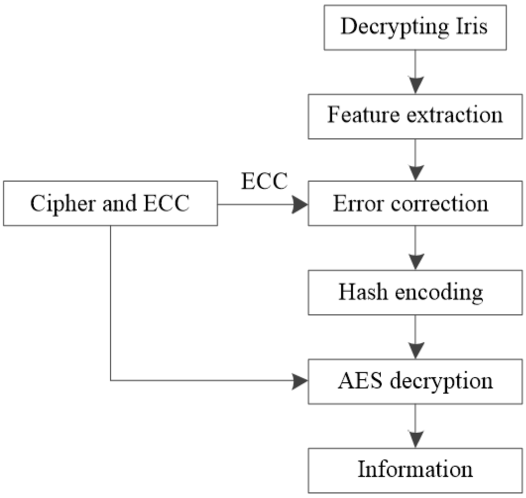


Figure 6. Decryption framework

In the encryption stage, the feature vector is extracted from the iris image at first, and then the error correction coding (ECC) of the feature vector is generated by the Reed-Solomon algorithm [21]. Then, hash technology is used to hash the feature vector into a 128-bit binary string as an encryption key. Finally, AES is used to encrypt the information. After encryption, only ciphertext and error correction code are reserved, and other parts are deleted.

In the decryption stage, the features are extracted from the decrypted iris, and then ECC is used to correct these features. Finally, hash technology is used to convert them into a 128-bit decryption key for decryption.

Hash is generally translated as “sanlie” or “haxi” in Chinese. It hashes the input of any length into output of fixed length through the hash algorithm. Its mathematical expression is:

$$h = H(M) \tag{27}$$

In Formula (27), *H*() is a one-way hash function. *M* is the pre-mapping. *h* is the hash value.

The encryption mainly includes four steps:

(1) Firstly, the dimension is extracted from the encrypted iris, *N*=256. The feature vector of each dimension is in the [0,15] integer interval.

(2) Reed-Solomon code (*N*,*K*) of the feature vector is calculated. Generally, the *RS* code includes two parts: source words and check words. Only the check word is reserved, which is called ECC, and its length is 2*T*=*N*-*K*.

(3) Each dimension of a vector has been quantized to an integer interval [0,15], so each dimension can be converted into a 4-bit binary number. Thus, a 256-dimensional feature vector will be converted into a binary string with 4×256=1024 bits. Next, the MDS algorithm is used to hash a 1024-bit binary string into a 128-bit binary encryption key [22].

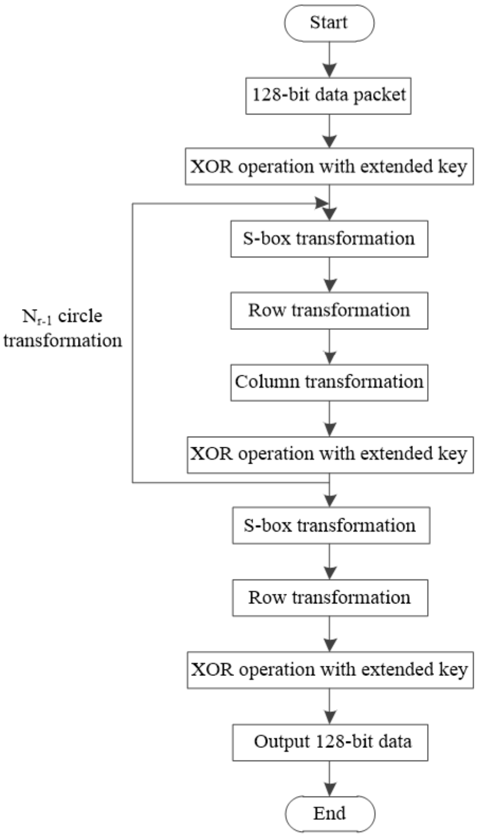


Figure 7. Flow of AES encryption algorithm

(4) AES is used to encrypt the plaintext.

The flow of the AES encryption algorithm is shown in Figure 7.

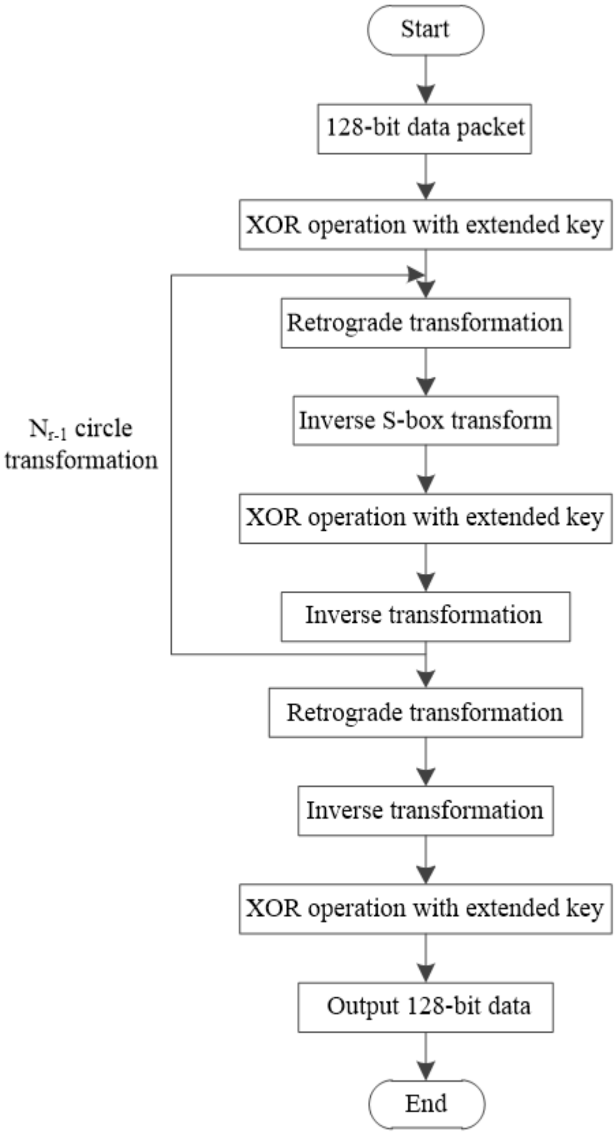
The decryption process is shown in Figure 8. The decryption process can be described as:

(1) The quantized feature vector is extracted from the decrypted iris.

(2) ECC preserved in the encryption process is used to correct the decrypted iris feature vector through the standard Reed-Solomon decoding algorithm, and thus to eliminate the fuzzification between the decrypted iris eigenvector and the encrypted vector [23].

(3) Then, the corrected vector is transformed into a 1024-bit binary string, and the string is hashed into a 128-bit decryption key by the hash algorithm (MD5), which is the same as the encryption process.

(4) Finally, the AES decryption algorithm is used to convert ciphertext into plaintext. If the difference between the decryption vector and the encryption vector is less than the threshold value *T*, then the Reed-Solomon error correction algorithm can convert the decryption vector into the vector that is exactly the same as the encryption vector, and thus generate the decryption key, which is exactly the same as the encryption key. Finally, the plaintext can be obtained [24, 25].

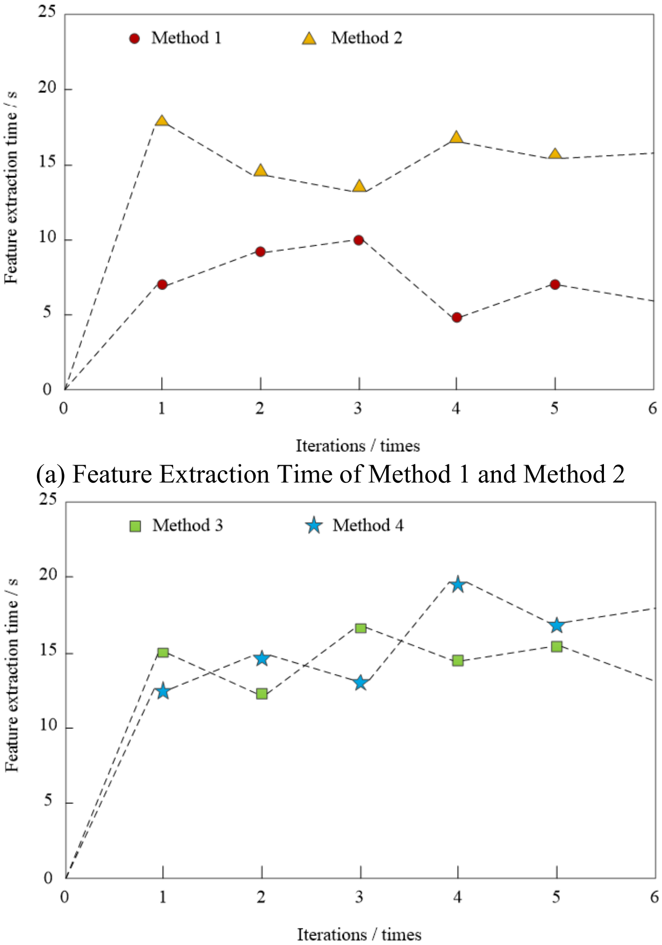


Start
128-bit data packet
XOR operation with extended key
Retrograde transformation
Inverse S-box transform
XOR operation with extended key
Inverse transformation
N_{r-1} circle transformation
Retrograde transformation
Inverse transformation
XOR operation with extended key
Output 128-bit data
End

Figure 8. Decryption flow

4. EXPERIMENT AND DISCUSSION

In order to verify the overall effectiveness of the method of hiding generative information of iris feature data based on the Gaussian fuzzy algorithm, it is necessary to test this method. In the test, thirteen groups of pictures provided by thirteen volunteers were selected from the CASIA-Iris V3 Interval database. Each group of pictures included 8-10 iris pictures. All of them were collected from the same side of the eye. The test platform was Simulink. The generative information hiding method of iris feature data based on the Gaussian fuzzy algorithm (Method 1), the information hiding method based on the generative antagonism network (Method 2), the information hiding method based on the TIN iterative encryption filter algorithm (Method 3), and the method based on fault-tolerant learning on a ring and the GSW (Method 4) were adopted for testing, respectively. The time of extracting iris feature data by different methods was compared. The test results are shown in Figure 9.



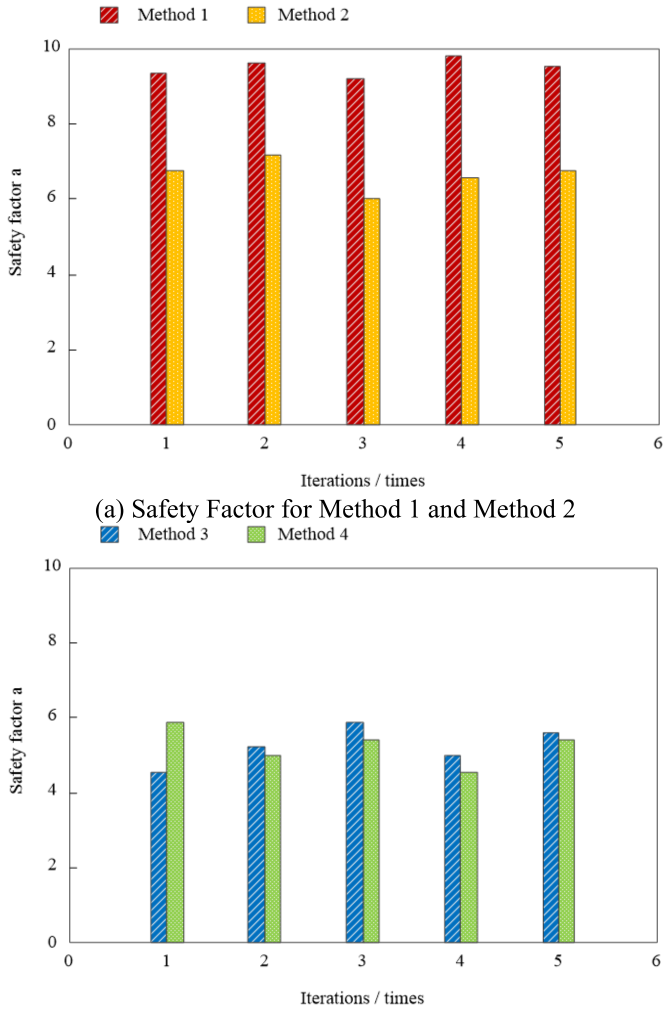
(a) Feature Extraction Time of Method 1 and Method 2

(b) Feature Extraction Time of Method 3 and Method 4

Figure 9. Feature extraction time of different methods

After analyzing the data in Figure 9, we can see that the time of extracting iris features in multiple iterations by the method based on the Gaussian fuzzy algorithm is lower than that of the method based on the generative countermeasure network, the method based on the TIN iterative encryption filtering algorithm and the method based on fault tolerance learning on a ring and GSW. Because the method of hiding generative information of iris feature data based on the Gaussian fuzzy algorithm uses the Gaussian fuzzy algorithm to smooth the image before extracting the iris feature. This method removes the noise in the image, eliminates the interference of noise on the iris feature extraction, shortens the feature extraction time, and improves the efficiency of information hiding.

The value of safety factor *a* is in the interval [0, 10]. The higher the security coefficient, the higher the security of information, and the better the effectiveness of the method. The generative information hiding method of iris feature data based on the Gaussian fuzzy algorithm (Method 1), the information hiding method based on the generative antagonism network (Method 2), the information hiding method based on the TIN iterative encryption filter algorithm (Method 3) and the method based on fault-tolerant learning on a ring and the GSW (Method 4) are adopted for testing, and the safety factor *a* in different methods is compared. The results are shown in Figure 10.



(a) Safety Factor for Method 1 and Method 2

(b) Safety Factor for Method 3 and Method 4

Figure 10. Safety factors of different methods

Figure 10 shows that the security coefficients of the proposed method in multiple iterations are higher than those of the method based on the generative countermeasure network, the method based on the TIN iterative encryption filtering algorithm, the method based on fault-tolerant learning on a ring and the GSW. Because the iris feature data-generated information-hiding method based on the Gaussian fuzzy algorithm uses the AES algorithm to encrypt the iris feature data, and thus to improve the security of information. Finally, the effectiveness of the proposed method was proved.

5. CONCLUSIONS

Biometric authentication, as an emerging form of identity verification, has witnessed rapid development in recent years. Biometrics refers to physiological characteristics determined at birth, which exhibit long-term stability and uniqueness—such as facial features, fingerprints, palmprints, and irises. Biometric technologies utilize these inherent traits as identity credentials for personal identification and verification. Among them, iris recognition has garnered significant research interest due to its high reliability and precision. However, existing generative information hiding methods for iris feature data are often limited by low efficiency and insufficient security. To address these limitations, a novel approach based on the Gaussian fuzzy algorithm has been proposed. Experimental results have demonstrated that iris feature data can be extracted within ten seconds using the proposed method, with a data security coefficient markedly higher than that of conventional techniques. This method not only enhances the effectiveness of information hiding but also addresses the shortcomings of current approaches, thereby laying a robust foundation for advancing iris recognition technology in the field of information security.

ACKNOWLEDGEMENTS

This paper was supported by the 2023 Henan Provincial Demonstration Course for Research-Oriented Teaching: Database Principles and Applications (Gaojiao [2023] No. 36); 2024 Huanghuai University Special Project for Higher Education Teaching Reform Research: AI-Empowered Innovation and Practice of Research-Oriented Teaching Model-Taking "Database" as an Example (Grant No.: 2024XJCZLX31); Higher Education Research Project (Grant No.: 2025SXHLX258); Huanghuai University Young Key Teachers Support Program; Research Merit-based Funding Program for Overseas Educated Personnel in Henan Province (Letter of Henan Human Resources and Social Security Office [2026] No. 51).

REFERENCES

[1] Sawhney, R., Sharma, S., Narayan, V., Srivastava, S., Awasthi, S., Kumar, N. (2024). A scientific programming based effective and precise iris acknowledgement algorithm. Traitement du Signal, 41(6): 2947-2960. https://doi.org/10.18280/ts.410614

[2] Farouk, R.H., Mohsen, H., Abd El-Latif, Y.M. (2022). Iris recognition system techniques: A literature survey and comparative study. In 2022 5th International Conference on Computing and Informatics (ICCI), New Cairo, Cairo, Egypt, pp. 194-199. https://doi.org/10.1109/ICCI54321.2022.9756079

[3] Winston, J.J., Hemanth, D.J. (2019). A comprehensive review on iris image-based biometric system. Soft Computing, 23(19): 9361-9384. https://doi.org/10.1007/s00500-018-3497-y

[4] Subban, R., Susitha, N., Mankame, D.P. (2018). Efficient iris recognition using Haralick features based extraction and fuzzy particle swarm optimization. Cluster Computing, 21(1): 79-90. https://doi.org/10.1007/s10586-017-0934-0

[5] Li, X., Jiang, Y., Chen, M., Li, F. (2018). Research on iris image encryption based on deep learning. EURASIP Journal on Image and Video Processing, 2018(1): 126. https://doi.org/10.1186/s13640-018-0358-7

[6] Liu, M.M., Zhang, M.Q., Liu, J., Zhang, Y.N., Ke, Y. (2018). Coverless information hiding based on generative adversarial networks. Journal of Applied Sciences, 36: 371-382.

[7] Zheng, J., Xiang, M., Zhang, T., Zhou, J. (2024). An improved adaptive grid-based progressive triangulated irregular network densification algorithm for filtering airborne LiDAR data. Remote Sensing, 16(20): 3846. https://doi.org/10.3390/rs16203846

[8] Kaur, A., Gajjar, N., Savani, V. (2024). Fully homomorphic encryption for embedded systems: IP core design and implementation. In World Conference on Artificial Intelligence: Advances and Applications, Singapore: Springer Nature Singapore, pp. 79-91. https://doi.org/10.1007/978-981-97-4496-1_6

[9] Jiang, Y., Liu, Y.L., Luo, Y.H. (2016). QR code encryption mechanism based on chaotic Z-Mapping algorithm. Computer Engineering and Design, 37: 2361-2365.

[10] Elrefaei, L.A., Hamid, D.H., Bayazed, A.A., Bushnak, S.S., Maasher, S.Y. (2018). Developing iris recognition system for smartphone security. Multimedia Tools and Applications, 77(12): 14579-14603. https://doi.org/10.1007/s11042-017-5049-3

[11] Li, S., Liu, Y., Zeng, J., Liu, Y., Li, Y., Xie, Q. (2024). Image smoothing method based on global gradient sparsity and local relative gradient constraint optimization. Scientific Reports, 14(1): 15152. https://doi.org/10.1038/s41598-024-65886-5

[12] Wei, S.Q., Yang, W., Shen, Y. (2016). A covert communication method based on reliable packet ordering. Journal of Chinese Computer Systems, 37(1): 124-128.

[13] Rong, X., Zhao, Y. (2017). Trustworthiness attestation scheme for virtual machine based on certificateless ring signature. Journal of Computer Applications, 37(2): 378-382.

[14] Ke, Y., Zhang, M.Q., Liu, J. (2016). Separable reversible Hexadecimal data hiding in encrypted domain. Journal of Computer Applications, 36: 3082-3087.

[15] Wang, J.L., Sun, X., Feng, X.Q. (2018). Adaptive reversible image data hiding using pixel permutation. Journal of Image and Graphics, 23(1): 1-8.

[16] Zhang, S., Wang, P., Sun, Y. (2016). Adaptive model of information hiding for the same type. Journal of Beijing University of Posts and Telecommunications, 39(4): 35. https://doi.org/10.13190/j.jbupt.2016.04.007

[17] Zhang, W.J., Wu, C., Yu, M.S. (2016). Data encryption algorithm of cloud-assisted WBAN using multi-valued and ambiguous attribute. Application Research of Computers, 33(5): 1537-1541.

[18] Shi, B., Wang, Y., Li, T. (2018). A densification method for base station observation data and its application to post processing of differential GNSS. Geomatics and Information Science of Wuhan University, 43(5): 651-657. https://doi.org/10.13203/j.whugis20160339

[19] Strauch, C., Naber, M. (2022). Irissometry: Effects of pupil size on iris elasticity measured with video-based feature tracking. Investigative Ophthalmology & Visual Science, 63(2): 20-20. https://doi.org/10.1167/iovs.63.2.20

[20] Lv, L., Yuan, Q., Li, Z. (2019). An algorithm of Iris feature-extracting based on 2D Log-Gabor. Multimedia Tools and Applications, 78(16): 22643-22666. https://doi.org/10.1007/s11042-019-7551-2

[21] Wu, D.N., Wang, X.M. (2016). Multi-user fuzzy retrieval encryption scheme under cloud environment. Computer Engineering, 42: 18-22.

[22] Petterson, H.N., Rehnholm, J., Vikström, S., Åslund, M., Åstrand, E., Tomasic, I. (2020). Iris identification using wavelet decomposition and Gabor filter. In 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, pp. 265-270. https://doi.org/10.23919/MIPRO48935.2020.9245439

[23] Tao, L.B., Shen, J.J., Xue, M., Cai, L.G. (2016). Privacy protection from implicit attacks in cloud computing environment. Computer Science, 43(51): 184-187.

[24] Tang, N., Chen, C., Han, Y.S. (2024). Fast error and erasure decoding algorithm for reed-Solomon codes. IEEE Communications Letters, 28(4): 759-762.

[25] Fu, A.M., Song, J.Y., Su, M., Li, S. (2017). A security client-side deduplication with encrypted data in cloud storage. Acta Electronica Sinica, 45(12): 2863-2872.