Generative Information Hiding of Iris Feature Data Based on Gaussian Fuzzy Algorithm

Zhou ShuChen (✉ 20101192@huanghuai.edu.cn)

Huanghuai University <https://orcid.org/0000-0001-7483-1067>

Waqas Jadoon

COMSATS Institute of Information Technology - Abbottabad Campus

Faisal Rehman

COMSATS Institute of Information Technology - Abbottabad Campus

Iftikhar Ahmed Khan

COMSATS Institute of Information Technology - Abbottabad Campus

Yang Tianming

Huanghuai University

Research

Keywords: Gaussian fuzzy algorithm, Iris feature data, Feature extraction, Information hiding

Posted Date: July 23rd, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-666943/v1>

License: This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Generative Information Hiding of Iris Feature Data Based on Gaussian Fuzzy Algorithm

Shuchen Zhou^{1,2} (20101192@huanghuai.edu.cn), Waqas Jadoon² (Waqas_jadoon@cuiatd.edu.pk), Faisal Rehman² (frehman@cuiatd.edu.pk), Iftikhar Ahmed Khan² (iftikharahmed@cuiatd.edu.pk), Tianming Yang¹ (ytm@huanghuai.edu.cn)

¹ Institute of International Education, Huanghuai University, Zhumadian, 463000, P.R. China

² Department of Computer Science, COMSATS University Islamabad, Abbottabad Campus 22060, Islamabad, Pakistan email:20101192@huanghuai.edu.cn

Abstract: The existing methods used for hiding the iris feature data were time-consuming for iris feature extraction. Meanwhile, the information security after hiding was also low, leading to low efficiency and security of information hiding. Therefore, a method of hiding iris features data generative information based on a Gaussian fuzzy algorithm was proposed. In the preprocessing stage of the image, the weighted average method was adopted for the gray-level transformation of the iris image, and the Gaussian fuzzy algorithm was used to smooth the image. In addition, the Laplacian convolution kernel was used to sharpen the image. The iris regions were normalized. The iris feature data was extracted by employing 2D Gabor wavelet. Moreover, the iris feature data was encrypted and decrypted using the AES algorithm, and hence, effectively enhancing the security of the generative information of iris feature data. Experimental results show that the proposed method can extract iris feature information within ten seconds, and the data security coefficient is high thus the proposed method efficiently realizes the information hiding.

Keywords: Gaussian fuzzy algorithm; Iris feature data; Feature extraction; Information hiding;

1 Introduction

In many biometrics identification methods, the iris recognition has attracted more and more attention due to its unique advantages ^[1]. Some researches The literature review has shown that the error rate of iris recognition system is the lowest among all the biometrics identification methods ^[2]. Generally, the iris acquisition is simple, and its security is higher than other technologies. In field of military and enterprise, there have been some mature iris recognition systems. In India, the iris recognition has been used to build an iris identity database nationwide. In civil fields, the access control and attendance system based on iris recognition technology have been applied preliminary ^[3-4]. In information society, the importance of information security is self-evident ^[5]. Therefore, more and more people have paid attention to the iris feature data generative information hiding techniques, which have become the key research field among scientific community.

Liu Mingming ^[6] proposed an information hiding method based on the generative countermeasure network. This method replaces the category label with the secret information as the driver, and directly generates the stego-image for transmission, and then extracts the secret information through the discriminator, and thus to realize the carrier-free information hiding with the help of generative countermeasures network. This method is time consuming, and the efficiency of information hiding is low. Zeng nehong ^[7] proposed an information hiding method based on TIN iterative encryption filtering algorithm. This method constructs the initial grid to

select seed points. In terms of selection, the neighborhood convolution was used to judge seed point and construct virtual seed point. Then, TIN iterative encryption filtering was carried out. Finally, the grid size was changed according to the filtering time, so that information hiding was achieved. The security coefficient of this method was low, and the effectiveness was poor. Wang Zhao ^[8] proposed a method of information hiding based on fault-tolerant learning on ring and GSW. This method constructed a public key encryption scheme based on the problem of fault-tolerant learning difficulties on ring, provided it with additive and multiplicative homomorphism by approximating the eigenvectors. Meanwhile, this method reduced the computational complexity of polynomial multiplication by fast Fourier transform. Finally, a hierarchical homomorphism encryption scheme was constructed to realize the information hiding, but this method can't effectively achieve information hiding, resulting in low effectiveness. Jiang Yi et al ^[9] proposed an information hiding method based on chaotic Z-mapping. This method encrypted the feature data information by key and thus to realize the information hiding, but it was time consuming to encrypt the feature data, resulting in low efficiency.

In order to address the above-mentioned issues in existing techniques, a method of hiding generative information of iris feature data that is based on Gaussian fuzzy algorithm was proposed. For preprocessing of iris images, the weighted average algorithm is applied to gray levels, then images are smooth using a Gaussian fuzzy algorithm to reduce the effect of noise for feature extraction process. Laplacian operator is used to sharpen the image and pave the way for feature extraction of iris image. Before feature extraction, the iris regions were normalized, and information is encrypted by Advanced Encryption Standard (AES). Compared with the existing methods, the performance of the proposed method is verified with respect to iris feature extraction time and information hiding security.

2. Methodology

2.1 Iris Image Preprocessing Based on Gaussian Fuzzy Algorithm

2.1.1 Image Gray Level Processing

The method of hiding generative information of iris feature data based on Gaussian fuzzy algorithm uses the weighted average method to process the gray level of image. The weighted average method is an empirical method for gray level transformation of images. This method is based on the fact that the color discrimination cells of human eye are most sensitive to green, but slightly insensitive to blue. Based on this feature, three weights with different coefficients can be applied on image pixels to obtain a gray level image. Because the human eye is most sensitive to green, the weight of the green coefficient is set as the maximum, and the next is red, and blue is the last ^[10]. The weighting formula is:

$$Gray(i, j) = 0.299 * R(i, j) + 0.578 * G(i, j) + 0.114 * B(i, j) \quad (1)$$

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

2.1.2 Image Smoothing

The 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 Gaussian fuzzy algorithm smooths the image by Gaussian fuzzy algorithm. According to the two-dimensional Gauss function, the weight of each position in the convolution template can be obtained as,

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

In Formula (2), x and y represent the distance from the neighborhood pixel to the center pixel. The parameter σ represents the standard deviation of 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 which results in reduce noise reduction effect^[12] and less blurred image. $G(x, y)$ denotes the weight of each point.

In the formula above, Gaussian filtering is related to the distance with center pixel. The closer the distance is, the greater the weight. We can select neighborhood pixels with a distance of less than one for calculation. At this time, we can calculate the pixels in the top, bottom, left and right neighborhood of the center pixel, or select the neighborhood pixels with a distance of less than two for calculation. They correspond to 8-neighborhood pixels. The larger the distance is, the more computation it will take for smoothing process, and the processing efficiency will be decreased. Generally, the 8-neighborhood pixels are enough. These neighborhoods are called convolution templates or convolution kernels^[13]. The 8-neighborhood Gauss convolution template is like a 3*3 matrix, and the method of generating template is shown as follows:

(1) Set the center point of the template as the origin point and get the coordinate value of each position in 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 template. The parameter value of σ is generally 0.8.

$$\nabla^2 f = \frac{\partial^2 f}{\partial^2 x^2} + \frac{\partial^2 f}{\partial^2 y^2} \quad (3)$$

(3) The results calculated by Gaussian function are all decimal, which is not convenient for 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 upper left corner is selected as the benchmark in the proposed method.

The calculation steps of normalization are shown as follows: take the reciprocal of the coefficient in upper left corner as the normalization coefficient, multiply each result in template by this value, and then round numbers, then get a 3 * 3 Gaussian convolution template:

$$\frac{1}{16} \begin{bmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 1 \end{bmatrix} \quad (4)$$

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 neighborhood ^[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 source image, and then the corresponding pixels are multiplied. After that, all the results in convolution kernel are added, and then we can get some pixel values, which can replace the pixel values of 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:

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

The convolution operation is shown in Figure 2:

Figure 2. Convolution operation

2.1.3 Image Sharpening

In the proposed method, Laplacian convolution kernel was used to sharpen the image ^[17]. Laplacian operator is a two-dimensional isotropic measure of the second-order spatial derivative of image. Laplacian operator can highlight the region where the intensity changes rapidly, so it is often applied in edge detection task. Laplace operator belongs to isotropic differential operator. 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:

$$\nabla^2 f = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} \quad (6)$$

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

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

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

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

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

$$\nabla^2 f(x, y) = f(x+1, y) + f(x-1, y) + f(x, y+1) + f(x, y-1) - 4f(x, y) \quad (9)$$

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

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

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.

the sharpened convolution kernel is shown in Figure 3:

0	1	0
1	-4	1
0	1	0

Figure 3. Sharpened convolution kernel

2.2 Proposed Methodology for Generative Information Hiding Method for IRIS Features

2.2.1 Iris Feature Data Extraction

1) Normalization of iris region

$I(x, y)$ represents the original iris image before normalization. $I(r, \theta)$ represents the iris rectangular image converted by normalization. (x, y) represents the coordinate value of the pixels on iris image in rectangular coordinate system before normalization. (r, θ) represents the polar coordinate value of the pixels taking the pupil circle center as the reference point. The iris boundary circle center is not coincided 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 as following.

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

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

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

$$I[x(\rho, \theta), y(\rho, \theta)] \rightarrow I(r, \theta) \quad (13)$$

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 actual iris image. After weighting, the points with same weight in iris region are mapped to the same circumference in rectangular coordinate, so that the points on the whole iris can be mapped to a rectangle with the same size and specification 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.

Figure 4. Normalized Geometric Model of Iris

In Figure 4, I is the center of outer boundary of iris. P is the reference point of 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 iris can be obtained. Thus, the points on 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 iris and the reference point of pupil. PB is the pupil radius r_p . PA is the radius R_l of outer boundary, and they are known. PIC and AIC are right triangle. Let ϕ be the angle $\angle IPC$ 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 iris region can be calculated by the elastic model. According to the geometric relationship, we can see that:

$$\phi = \arctan\left(\frac{PQ}{IO}\right) \quad (14)$$

$$\Delta r = \sqrt{PQ^2 + IQ^2} \quad (15)$$

$$\angle IPC = \pi - \theta + \phi \quad (16)$$

For right triangle IPC :

$$PC = \Delta r \cos(\pi - \theta + \phi) \quad (17)$$

For right triangle IAC :

$$AC = \sqrt{IA^2 - IC^2} = \sqrt{R_I^2 - (\Delta r^2 - (\Delta r \cos(\pi - \theta + \phi))^2)} \quad (18)$$

Based on above formulas, PA is:

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

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 $R(\theta)$. 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 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 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 iris region to $M \times N$ rectangle region is shown as follows:

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

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

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 iris inner boundary are located on the circumference with same radius which takes the reference point as the center. In other words, all points on inner boundary have the same radius to expand. However, the center of iris outer boundary is not coincided with the reference point, and there is a position deviation. When angles are different, different points on iris outer boundary have different radii during coordinate conversion, so the outer boundary of each point in iris region is shown as follows:

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

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

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

In Formula (22), $i=1,2,\dots,M$; $j=1,2,\dots,N$; $\theta = j \times \pi / 180$. After the normalization, any point on the iris region can be regarded as a linear combination of internal and external boundary radii:

$$R_p = (\theta, \rho) = (1 - \rho)r(\theta) + \rho R(\theta) \quad (23)$$

In Formula (23), $r(\theta)$ denotes the inner boundary radius of iris. $R(\theta)$ denotes the outer boundary radius of iris. ρ is the normalized weighting coefficient. When $\rho=0$, this point is the point of the inner boundary of iris. When $\rho=1$, it means that it is exactly the point of the outer boundary of iris. ρ changes in intervals $[0,1]$, the iris region can be normalized to the weight of inner and outer boundary. 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 Gaussian fuzzy algorithm uses 2D Gabor wavelet to extract the iris feature. The filtering result is complex number, so that the real part and the virtual part can be coded by phases and the binary feature code of iris can be obtained^[20]. The formula of calculating Gabor filter is:

$$h_{\{R_e, I_m\}} = \text{sgn}_{\{R_e, I_m\}} \iint_{\rho\phi} I(\rho, \theta) e^{-i\omega(\theta_0 - \theta)} e^{-(\eta_0 - \rho)^2 \frac{2}{\sigma^2}} \rho d\rho d\theta \quad (24)$$

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

$$\text{Code} = (B_1, B_2, B_3, \dots, B_j, \dots, B_k) \quad (25)$$

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 corresponding iris feature code b_j is:

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

2.2.2 Information Hiding

The method of hiding generative information of iris feature data based on Gauss 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 feature vector is generated by Reed-Solomon algorithm^[21]. Then, Hash technology is used to hash the feature vector into 128-bit binary string as encryption key. Finally, Advanced Encryption Standard (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 decryption iris, and then error correction coding (ECC) is used to correct these features. Finally, Hash technology is used to convert them into 128-bit decryption key for decryption.

Hash converts the input of any length into output of fixed length through hash algorithm. Its mathematical expression is:

$$h = H(M) \quad (27)$$

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 $[0, 15]$ integer interval.

(2) Reed-Solomon code (N, K) of feature vector is calculated. Generally, RS code includes

two parts: source words and check words. Only the check word is reserved, which is called ECC, and its length is $2T = N - K$.

(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 $4 \times 256 = 1024$ -bits. Next, MDS algorithm is used to hash 1024-bit binary string into 128-bit binary encryption key^[22].

(4) AES is used to encrypt the plaintext.

The flow of AES encryption algorithm is shown in Figure 7:

Figure 7. Flow of AES Encryption Algorithm

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 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 Hash algorithm (MD5) which is the same as the encryption process.

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

Figure 8. Decryption Flow

3 Experimental Results and Discussion

In order to verify the overall effectiveness of the proposed method, it is necessary to test this method. In the experimental setting, thirteen groups of pictures provided by thirteen volunteers were selected from 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 used in experimentation was Simulink. The proposed generative information hiding method of iris feature data based on Gaussian fuzzy algorithm (Method 1), the information hiding method based on generative antagonism network (Method 2)^[26], the information hiding method based on TIN iterative encryption filter algorithm (Method 3)^[27] and the method based on the fault-tolerant learning on ring and the GSW (Method 4)^[8] were adopted for the test , 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 Gauss fuzzy algorithm (proposed method) is lower than that of the method based on generative countermeasure network, the method based on TIN iterative encryption filtering algorithm and the method based on fault tolerance learning on ring and GSW. Because the Method 1, the proposed technique of hiding generative information of iris feature data based on Gaussian fuzzy algorithm uses Gaussian fuzzy algorithm to smooth the image before extracting the iris feature. This method removes the noise in 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 interval $[0, 10]$. The higher the security coefficient, the higher the security of information, the better the effectiveness of the method. The generative information hiding method of iris feature data based on Gaussian fuzzy algorithm (Method 1), the information hiding method based on generative antagonism network (Method 2), the information

hiding method based on TIN iterative encryption filter algorithm (Method 3) and the method based on the fault-tolerant learning on ring and the GSW (Method 4) are adopted for test, 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 generative countermeasure network, the method based on TIN iterative encryption filtering algorithm, the method based on the fault-tolerant learning on ring and the GSW. Because the proposed method 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.

4 CONCLUSIONS

As a new type of identity authentication, biometric authentication has been developed rapidly

in recent years. Biometrics refers to some features determined by birth, and it can be maintained stability in a long period, such as face, fingerprint, palmprint and iris. Biometric technology is to use these features as human identity credentials for identification and authentication, and the iris recognition technology has become a hot research topic. At present, the iris feature data generative information hiding method has the problems of low information hiding efficiency and low information security. Therefore, a new method based on Gauss fuzzy algorithm is proposed. Experimental results show that the proposed method can extract the iris feature data within ten seconds, and the data security coefficient is higher than traditional methods. This method can effectively realize information hiding and solve the shortcomings in the existing techniques, which lays a foundation for the development of iris recognition technology in the field of information security.

References

- [1] Li S, Chen X, Wang Z, et al. (2018). Data Hiding in Iris Image for Privacy Protection. *IETE Technical Review*, 35(sup1): 34-41.
- [2] Wang Y L, Ma J, Li H Q, et al. (2019). Race classification based on deep features and Fisher vectors of iris texture. *Journal of Image and Graphics* 23(1):28-38.
- [3] Winston J J, Hemanth D J. (2019). A comprehensive review on iris image-based biometric system. *Soft Computing*, 23(19): 9361-9384.
- [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.
- [5] Li X, Jiang Y, Chen M, et al. (2018). Research on iris image encryption based on deep learning. *EURASIP Journal on Image and Video Processing*, 18(1): 1-10.
- [6] Liu M M, Zhang M Q, Liu J, et al. (2018). Coverless Information Hiding Based on Generative Adversarial Networks. *Journal of Applied Sciences* 36:371-382.
- [7] Zeng N H, Yue Y C, Wei Z Y, et al. (2016). An improved irregular triangular network encryption method of vehicle-borne LiDAR point clouds[J]. *Science of Surveying and Mapping* 041:136-139,46.
- [8] Wang Z, Ding Y & Wang H Y. (2016). Leveled fully homomorphic encryption scheme based on Ring-LWE-GSW. *Journal of Computer Applications* 36:962-965.
- [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, et al. (2018). Developing Iris Recognition System for Smartphone Security. *Multimedia Tools and Applications*, 77(12): 14579-14603.
- [11] Xiang S J & Luo X R. (2016). Reversible Data Hiding in Encrypted Image Based on Homomorphic Public Key Cryptosystem. *Journal of Software* 27:1592-1601.
- [12] Wei S Q, Yang W, Shen Y, et al. (2016). A Covert Communication Method Based on Reliable Packet Ordering. *Journal of Chinese Computer Systems* 37:124-128.
- [13] Rong X & Zhao Y. (2017). Trustworthiness attestation scheme for virtual machine based on certificateless ring signature. *Journal of Computer Applications* 37:378-382.
- [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. (2019). Adaptive reversible image data hiding using pixel permutation. *Journal of Image and Graphics* 23:1-8.
- [16] Fang T H, Lei L H, Zhang S, et al. (2016). Adaptive Model of Information Hiding for the

- Same Type. Journal of Beijing University of Posts and Telecommunications 39:35-39.
- [17] Zhang W J, Wu S, Yu M S, et al. (2016). Data encryption algorithm of cloud-assisted WBAN using multi-valued and ambiguous attribute. Application Research of Computers 33:1537-1541.
- [18] Shi B, Wang Y P & Li T H. (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 43:651-657.
- [19] Shao B Y, Liu X Y, Shen C D, et al. (2016). Research and Application on Data Decryption of BITLOCKER Driver Encryption. Computer Science 43:198-201.
- [20] Yu R, Huang J & He C M. (2016). Smart grid monitoring and secure transmission system based on SM4 parallel encryption. Application of Electronic Technique 42:66-69.
- [21] Wu D N & Wang X M. (2016). Multi-user Fuzzy Retrieval Encryption Scheme Under Cloud Environment. Computer Engineering 42:18-22.
- [22] Zhou S L, Chen G X, Wu L F, et al. (2016). Anonymity Technology of User Network Behavior Based on Trusted Neighbors Selecting for Big Data Privacy Protection. Computer Science 43:136-139.
- [23] Tao L B, Shen J J, Xue M, et al. (2016). Privacy Protection from Implicit Attacks in Cloud Computing Environment. Computer Science 43:184-187.
- [24] Zhang Q. (2019). Harmonic data storage safety control method of distribution network based on blind number BM model. Power System and Clean Energy 35:43-48.
- [25] Fu A M, Song J Y, Su M, et al. (2017). A Security Client-side Deduplication with Encrypted Data in Cloud Storage. Acta Electronica Sinica 45:2863-2872.
- [26] Yang, Z., et al.(2020), GAN-TStega: Text Steganography Based on Generative Adversarial Networks, in Digital Forensics and Watermarking. 18-31.
- [27] Zhao, X., et al.(2016), Improved progressive TIN densification filtering algorithm for airborne LiDAR data in forested areas. ISPRS Journal of Photogrammetry and Remote Sensing. 117: 79-91.

Declarations

- **Availability of data and materials:** Data and materials sharing are not applicable to this article as no datasets were generated. The dataset used in experimentation is publicly available and properly cited in the manuscript.
- **Competing interests:** The authors declare no conflict of interest.
- **Funding:** This work was supported in part by the research grants provided by Huanghuai University, Zhumadian, 463000, P.R. China.
- **Author Contributions:** Conceptualization, Shuchen Zhou, Waqas Jadoon and Faisal Rehman; writing—original draft preparation, Shuchen Zhou and Tianming Yang ; validation, Waqas Jadoon, Faisal Rehman and Iftikhar Ahmed Khan; writing—review and editing, Shuchen Zhou, Waqas Jadoon and Iftikhar Ahmed Khan; supervision, Waqas Jadoon; funding acquisition, Tianming Yang.

- **Acknowledgments:** The authors would like to thank the anonymous referees for their valuable comments and suggestions.
- **Authors' information:**

Shuchen Zhou received his bachelor's degree in computer science and technology and master's degree in computer application technology from Henan University, China in 2007 and 2010 respectively. He is currently a PhD student at COMSATS University Islamabad Pakistan. He is also a lecturer in the school of international education of Huanghuai University, China. His current research interests include edge computing, information hiding and digital watermarking, etc. He has published more than 10 papers.

Waqas Jadoon received the Ph.D. degree in Computer Science from Sichuan University China in 2014. Currently, he is an Assistant Professor at COMSATS University Islamabad, Abbottabad, Pakistan and is an approved Ph.D Supervisor from Higher Education Commission (HEC) Pakistan. His research interests focus on Pattern Recognition, Image Processing, theory and applications of Machine Learning.

Faisal Rehman is a Ph.D in computer science and is working as Assistant Professor at COMSATS University Islamabad, Pakistan.

Iftikhar Ahmed Khan is a Ph.D in computer science and is working as Assistant Professor at COMSATS University Islamabad, Pakistan.

Tianming Yang is a Ph.D in computer science and is working as Professor at Huanghuai University, China.