Received: 23 March 2019 | Revised: 8 July 2019 | Accepted: 28 August 2019

DOI: 10.4218/etrij.2019-0145

SPECIAL ISSUE

ETRI Journal WILEY

Concealment of iris features based on artificial noises

Wenming Jiao[1,2] | **Heng Zhang**[1] | **Qiyan Zang**[1] | **Weiwei Xu**[1,2] | **Shuaiwei Zhang**[1] | **Jian Zhang**[1] | **Hongran Li**[1]

[1]Jiangsu Ocean University, Lianyungang Jiangsu, China

[2]China University of Mining and Technology, Xuzhou Jiangsu, China

Correspondence
Heng Zhang, Jiangsu Ocean University, Lianyungang Jiangsu, China.
Email: ezhangheng@gmail.com

Funding information
This research was supported by the The National Natural Science Foundation of China under Grant 61873106, National Nature Science Foundation of Jiangsu Province under Grant BK20171264, Jiangsu Qing Lan Project to Cultivate Middle-aged and Young Science Leaders, Jiangsu Six Talent Peak Project under Grants XYDXX-047, XYDXX-140, University Science Research General Research General Project of Jiangsu Province under Grant 18KJB520005, Lianyungang Hai Yan Plan under Grants 2018-ZD-003, 2018-QD-001, 2018-QD-012, and Natural Science Foundation Project of Huaihai Institute of Technology under Grant Z2017005.

Although iris recognition verification is considered to be the safest method of biometric verification, studies have shown that iris features may be illegally used. To protect iris features and further improve the security of iris recognition and verification, this study applies the Gaussian and Laplacian mechanisms and to hide iris features by differentiating privacy. The efficiency of the algorithm and evaluation of the image quality by the image hashing algorithm are selected as indicators to evaluate these mechanisms. The experimental results indicate that the security of an iris image can be significantly improved using differential privacy protection.

KEYWORDS
differential privacy, hash algorithm, iris features, noise mechanism, similarity comparison

1 | INTRODUCTION

With the increasing prominence of the Internet plus concepts in recent years, the security of personal information is becoming increasingly important. Biometrics technology is an important method of protecting personal information by analyzing the inherent physiological or behavioral characteristics of human beings. The biological characteristics of a human body mainly include fingerprints, face, irises, voice, gait, signature, and so on, and iris features are considered to be the most secure biometric authentication technology at present [1–3]. Academic and business circles are paying increasing attention to identity a recognition technology based on iris feature extraction. Lasker et al [4] proposed a new approach to recognize an iris from distantly acquired facial images by utilizing multiple feature descriptors and classifiers. Wang et al [5] investigated cross-spectral iris recognition using a series of deep learning architectures. Iris recognition has been employed in some departments that require a high security performance, such as banking systems and security agencies, and some environments with high requirements for identity verification.

However, owing to the insecure nature of iris image information in the process of network transmission, a

malicious attacker has an opportunity to leak or destroy the original image information by an attack [6]. Because of the uniqueness and immutability of an iris image, once it is leaked, our privacy information may at the risk of long-term disclosure. In view of the malicious destruction of the iris image information and undesired spreading of the private information of a victim, a method of improving iris image security remains an imminent problem that requires a solution.

Therefore, numerous recent works have focused on designing biometric encryption algorithms. Fridrich et al [7,8] developed a block cipher based on a two-dimensional chaotic cryptosystem, which used a two-dimensional chaotic system, such as Baker mapping and standard mapping, to achieve effective encryption of the image data. Simoens et al [9] proposed a framework for the template security and privacy protection protocols in biometric authentication systems based on a cryptographic template. Torres et al [10] used homomorphic encryption for secure iris recognition. However, the recognition of the iris was mainly based on the Hamming distance for the similarity measurement, and the time complexity of the program was high. Bringer et al [11] used a chaotic circuit to complete the calculation and matching of all iris distances.

Although the above encryption methods are limited to iris privacy protection on a semi-honest model, malicious attackers may steal information from a server or tamper with it. Therefore, in the current well-known concept of clouds, if a cloud is used to store the user iris information, then it may be compromised [12,13].

Differential privacy can effectively solve the above problems. It has become the mainstream privacy protection method owing to its reliable mathematical foundation. It achieves the effect of privacy protection by adding a random noise to the original data, and the added noise is strictly indistinguishable. Therefore, an attacker cannot accurately know the amount of noise added. Even if an attacker has a certain background knowledge, it is difficult to effectively attack the data. Differential privacy not only reduces the risk of privacy leakage but also guarantees the availability of data to a certain extent. It is a rigorous anti-attack mode with strong privacy protection [14].

Another problem is how to evaluate the privacy protection performance of iris images. An image hashing algorithm is often used for image similarity comparison. It maps an image into a fixed-length digital sequence by a hash function, and uses a visual information feature to construct the hash value. Constructing an image hashing algorithm usually requires attention to robustness and uniqueness. In this study, an iris image is protected by differential privacy, and the original image and differential privacy image are similarly detected by the image hashing algorithm.

The contributions of this paper are given below.

1. We provide two differential privacy protection methods to protect iris image privacy that is improve the security of an iris image and avoid the risk of privacy leakage.
2. We present a hash algorithm to compare the differential privacy protection performance after the differential privacy protection of iris images using a Laplacian noise and Gaussian noise.

2 | RELATED WORK

Various works have investigated how to use or design improved differential privacy algorithms to meet privacy requirements. Zhang et al [15] adopted a face image publishing method based on the Fourier transform and differential privacy technology. The Laplace noise mechanism was used to add noise to the selected coefficients so that the whole process satisfied ε-differential privacy. Benjamin et al [16] achieved low bounds on the differential privacy enforced by algorithms. They systematically searched for large privacy violations, with which they could compute the low bounds of the differential privacy from multiple random algorithms. To ensure that a training model contains numerous representative datasets without exposing private information, Martin et al [17] trained deep neural networks to learn and fine-tune the privacy costs within the differential privacy framework. Thee et al [18] used the matrix-variate Gaussian mechanism to solve the problem of traditional mechanisms failing to take advantage of the matrix structure features after adding an independent and identically distributed noise. Abhishek et al [19] designed new optimal locally differentially private mechanisms for statistical learning problems for all privacy levels, and presented practicable approaches for large-scale locally private model training that were previously impossible. All these works supposed that differential privacy plays a significant role in the field of privacy protection.

Another research topic that is related to this study is the design of a similarity effect evaluation method for iris images. Venkatesan et al [20] first proposed the concept of "image hashing." The algorithm used a random signal processing strategy to irreversibly compress an image into a random binary string and exhibited robustness to the image changes due to compression, geometric distortion, and other attacks. Kalker et al [21] introduced perceptual hashing into the research field of hash algorithms. Fridrich et al [22] proposed an image hashing algorithm based on the DCT coefficients and compressed sensing. Lu et al [23] constructed an image hashing extraction method suitable for image copy detection by extracting robust Harris corners and normalized triangle meshes. Kozat et al [24] jointly proposed the use of matrix invariance to construct

image hashing. The image was regarded as a numerical matrix, and the features of the secondary image were extracted by an singular value decomposition (SVD) transform to form an image hashing value. This method guarantees the robustness of image hashing by the invariance of SVD and achieves a good ability to resist the normal operation of images. Tang et al [25] proposed a novel image segmentation algorithm that still showed a strong robustness after an image was attacked by a rotational transformation. Hao et al [26] studied string similarity search for both short and long strings, and proposed two new hash-based labeling techniques. Zhen et al [27] proposed a texture feature to extract image hashing values. This method effectively improved the uniqueness and perceptual robustness of the hash values, but the amount of computational data was large. However, it is worth mentioning that all these works were done from the perspective of the image pixel matrix.

3 | PROBLEM FORMULATION

In this section, we describe the iris features, introduce differential privacy, and then state the main problem that we are interested in.

3.1 | Iris feature description

Iris feature extraction is an important step in iris recognition. Feature extraction encodes the obtained image texture information and forms a code corresponding to the texture information [28]. Good features should meet the characteristics of high resolution and low dimensions.

Wavelet transform zero-crossing can represent the mutation information of a signal. Mutation information reflects the important features in an iris texture. Boles [29] proposed a zero-crossing detection and encoding method based on wavelet transform, which used the wavelet transform zero-crossing information of iris digital images as the iris features. In this method, before encoding the iris texture images, an iris digital image is sampled by the concentric circle centered on the center of the iris, and the two-dimensional iris digital image is converted into a one-dimensional signal. Finally, it is transformed by a specific wavelet function. The specific wavelet function is defined as the second derivative of a smoothing function. The definition of the mother wavelet function is

$$\psi(x)=\frac{d^2\theta(x)}{dx^2}. \tag{1}$$

In the formula, $\theta(x)$ is a smooth function. According to the definition of the dyadic wavelet transform,

$$W_{2^j}f(x)=2^{2j}\frac{d^2}{dx^2}\left(f\times\theta_{2^j}\right)(x). \tag{2}$$

The dyadic wavelet transform, $W_{2^j}f(x)$, of $f(x)$ is proportional to the second derivative of $f(x)$ smoothed by $\theta_{2^j}(x)=\left(1/2^j\right)\theta\left(x/2^j\right)$. The zero-crossings of the transform correspond to the inflection points of $f(x)\times\theta_{2^j}(x)$, which is the part of the function curve that changes drastically.

3.2 | Differential privacy

Differential privacy is not required to guarantee the integrity of a dataset but to protect the privacy of each individual in the dataset. Its concept is that each single element has a limited impact on the output in the dataset. Therefore, an attacker after observing the query result cannot infer which individual in the dataset is affected. Specifically, an attacker cannot know whether an individual exists in such a dataset.

Definition 1 Differential privacy [30]: For a random algorithm, M, P_m is a set of all the values that algorithm M can output. If for any pair of adjacent datasets D and D', any subset S_m of P_m, the algorithm, M, satisfies

$$\Pr[M(D)\in S_m]\le e^{\varepsilon}\Pr[M(D')\in S_m]. \tag{3}$$

Then the algorithm, M, satisfies ε-differential privacy, where the parameter, ε, is a privacy protection budget. From the above equation, the smaller the parameter, ε, the more similar is the probability distribution of the query results returned by the differential privacy algorithm acting on a pair of adjacent datasets. The more difficult it is for an attacker to distinguish this pair of adjacent datasets, the higher is the degree of protection. In extreme cases, when $\varepsilon = 0$, an attacker cannot distinguish between a pair of adjacent datasets, and the degree of protection is the highest. Conversely, the larger the parameter, ε, the lower the degree of protection.

The differential privacy mechanism maps the query result of a normal query function, $f(\cdot)$, to a randomized value range, and returns a query result to the user with a certain probability distribution. The parameter, ε, is used to control the proximity of the probability distribution on a pair of adjacent datasets so that the output results are almost identical on a pair of adjacent datasets. Therefore, an attacker cannot distinguish this pair, and the purpose of protecting the individual private information in a dataset is realized.

Differential privacy can protect user privacy information by adding noise to the query results, and the amount of the noise is a key amount. To ensure both, the added noise protects the user privacy and the data are not available due to excessive noise. Function sensitivity is an important parameter for controlling noise. By controlling the generated noise size by the global sensitivity, a privacy protection mechanism that satisfies the differential privacy requirement can be realized.

Definition 2 Global sensitivity [31]: For a query function, f, its form is f: $D \rightarrow R$, where D is a dataset and R is the result of the query function. For a pair of arbitrary adjacent datasets, D and D', their global sensitivity is defined as follows:

$$S(f) = \max_{D,D'} ||f(D) - f(D')||_1, \quad (4)$$

where $||f(D) - f(D')||_1$ is the Manhattan distance between $f(D)$ and $f(D')$.

Global sensitivity reflects the maximum range of the changes that a query function can make when querying a pair of adjacent datasets. It is independent of the dataset and only determined by the query function itself.

3.3 | Problem of interest

In this study, a differential privacy-preserving algorithm for iris images is investigated, and two common mechanisms of differential privacy protection algorithm are used to protect iris privacy. The following issues will be addressed in this paper:

1. How to adopt the differential privacy of two noise mechanisms to protect the privacy of iris images?
2. What type of noise mechanism can achieve the optimal performance when the privacy protection parameters are consistent?

4 | IRIS FEATURES HIDDEN APPROACH

We have introduced iris features and the differential privacy method. The next step is to define the iris privacy-preserving approach and provide an algorithm to verify iris image similarity. As shown in Figure 1, after the iris features are extracted from an iris image, they are differentially protected. Image similarity verification is performed on the processed and original iris images using an image hashing algorithm. Then the privacy protection effects of the differential privacy based on the different noise mechanisms on the iris images are compared.

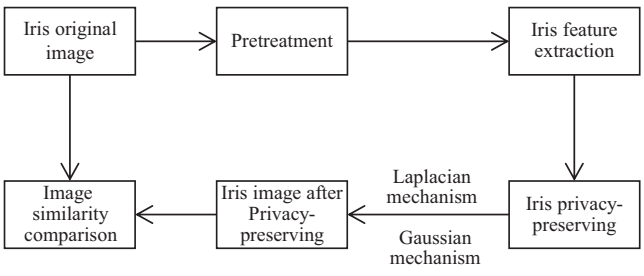


FIGURE 1 Iris privacy protection system flow chart

4.1 | Iris privacy-preserving approach

The main technology to achieve differential privacy is the noise mechanism, which mainly uses a noise to disturb the output, thus achieving differential privacy protection. Because a noise mechanism is subject to the global sensitivity and privacy budget, this paper focuses on the Laplacian mechanism and Gaussian mechanism.

Definition 3 Laplacian mechanism [32]: Given a private dataset, μ, the random algorithm expressed in Equation 5 satisfies (ε, 0)-differential privacy.

$$M_L(\mu) = \mu + V, \quad (5)$$

where V represents the noise following the Laplacian distribution, and its probability density function is

$$F(x) = \frac{1}{2b} e^{-\frac{|x|}{b}}. \quad (6)$$

The scale parameter is $b = S_f/\varepsilon$. In the process of data release, the Laplace mechanism can be used to add the noise of the original query result to the Laplacian distribution so that it can realize (ε, 0)-differential privacy protection.

Definition 4 Gaussian mechanism [33]: Given a private dataset, μ, the random algorithm expressed in (6) satisfies (ε, δ)-differential privacy.

$$M_G(\mu) = \mu + W, \quad (7)$$

where $W \sim N(0, \sigma^2)$ represents the noise with the Gaussian distribution,

$$\sigma \geq \frac{cS_f}{\varepsilon}, \quad c^2 > 2\ln\frac{1.25}{\delta}. \quad (8)$$

In the data release process, the Gaussian mechanism can be used to add a noise following the Gaussian distribution to the original data of the query so that it can realize (ε, δ)-differential privacy protection.

The Laplacian mechanism and Gaussian mechanism implement differential privacy protection by adding a noise to the original data. The noise level is related to the sensitivity, Δd, and privacy protection budget, ε. When ε is constant, the smaller the Δd is, the lesser the added noise is. When Δd is constant, the smaller the ε, the more noise is added.

The Laplacian mechanism satisfies (ε, 0)-differential privacy, and the output on each pair of adjacent datasets is approximately the same. For the Laplacian mechanism that has been practiced, the Gaussian mechanism is used for (ε, δ)-differential privacy to add a noise following the Gaussian distribution during the data release process. Gaussian noise and Laplacian noise distribution images have similar wave

trajectories, ensuring that the overall statistical output of the original data is unchanged after adding the noise.

In this paper, there are two types of differential privacy based on the distinctive noise mechanisms being added to protect the iris image information. The corresponding algorithms are provided in Algorithms 1 and 2.

In these algorithms, we need to set some initial values. The iris image matrix is denoted by I. S_f is the sensitivity index, and ε is the noise parameter. ψ is a random variable matrix following a uniform distribution in the range, (−0.5, 0.5), namely, $\psi \sim$ Uni(−0.5, 0.5). ζ and ξ are random variable matrices following a uniform distribution in the range, (0, 1), namely, $\zeta \sim$ Uni(0, 1), $\xi \sim$ Uni(0, 1). Their dimensions are the same as those of matrix I. We traverse all the image pixel values in the iris image matrix, I, and add a noise that meets the privacy requirements. Then a new matrix of pixel values is obtained. If the image pixel value in the generated matrix exceeds 255, then the image pixel value is assigned 255. According to the above steps, we obtain the iris image matrix after differential privacy.

Algorithm 1 Iris de-identification based on the Laplacian mechanism

Process begins;
Input: ε; S_f; iris image matrix I; image pixel value $I_{s,t}$, where the row is s and the column is t, $s = 1, 2, 3, \cdots, k$, and $t = 1, 2, 3, \cdots, l$;
$b = S_f/\varepsilon$;
Generate the matrix, ψ, consisting of random numbers following a uniform distribution Uni$(-0.5, 0.5)$; its dimension is the same as that of matrix I.
for s := 1 to k do
  for t := 1 to l do
    $Q_{s,t} = -b \times sign(\psi_{s,t}) \times \ln(1 - 2abs(\psi_{s,t}))$;
    $R_{s,t} = 255 * (I_{s,t}/255 + Q_{s,t})$;
    if $R_{x,y} > 255$ then
      $R_{x,y}$=255;
    end if
  end for
end for
Output: Image matrix R after differential privacy based on the Laplacian mechanism.

4.2 | Iris similarity verification approach

Picture similarity detection is used to extract the features from different photos and compare them. If they closely resemble each other, these pictures can be considered to be similar. The algorithms of picture similarity detection mainly include the average hash(aHash) algorithm, perceptual hash(pHash) algorithm, and deference hash(dHash) algorithm [34,35].

Algorithm 2 Iris de-identification based on the Gaussian mechanism

Process begins;
Input: ε; S_f; iris image matrix I; image pixel value $I_{s,t}$, where the row is s and the column is t, $s = 1, 2, 3, \cdots, k$, and $t = 1, 2, 3, \cdots, l$;
$b = S_f/\varepsilon$;
Generate the matrix, ζ and ξ consisting of random numbers following a uniform distribution, Uni$(0, 1)$; their dimensions are the same as that of matrix I.
for s := 1 to k do
  for t := 1 to l do
    $J_{s,t} = b \times sqrt(-2lg(\zeta_{s,t})) \times cos(2\pi(\xi_{s,t}))$;
    $Z_{s,t} = 255 * (I_{s,t}/255 + J_{s,t})$;
    if $Z_{x,y} > 255$ then
      $Z_{x,y}$=255;
    end if
  end for
end for
Output: Image matrix Z after differential privacy based on the Gaussian mechanism.

The aHash algorithm is based on a pixel domain design that takes advantage of the low-frequency components in the picture. First, the high-frequency components in the picture are culled by zooming out the image, thereby preserving the low-frequency information in the picture. Second, the-high frequency components in the picture are further removed by grayscale processing. Then, the hash value of the image needs to be calculated, and the size between each pixel and the average value of the pixels in the grayscale image are compared. If a single pixel in the grayscale image is larger than or equal to the mean value, it is recorded as 1; otherwise, it is 0. The resulting binary string is the aHash value of the image. The image size scaling has less influence on the image hashing value.

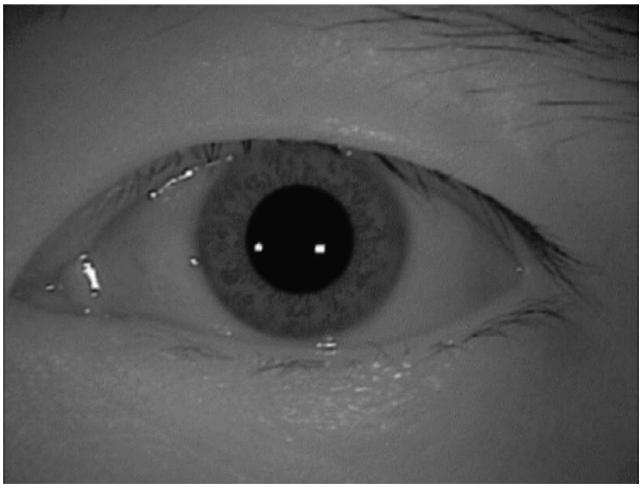


FIGURE 2 Original iris

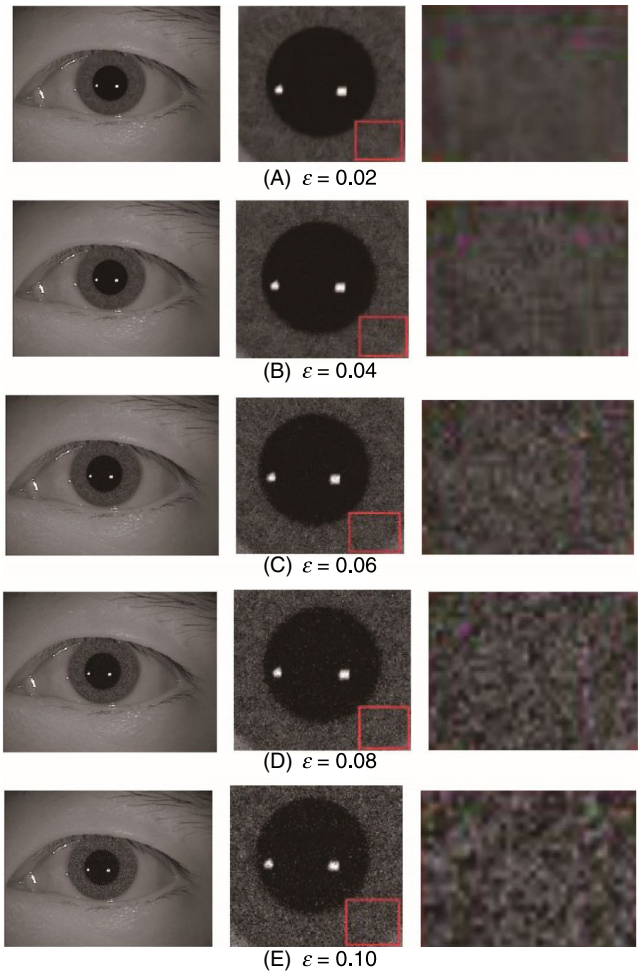


FIGURE 3 Iris image after adding Laplacian noises with different noise parameters ε

The pHash algorithm is based on the frequency-domain implementation. In specific, the algorithm sees an image as a superposition of the different frequency components. The image is first converted to the frequency domain by a DCT. It can be seen that the smaller the coefficient of the frequency component is, the higher is the proportion of the picture coverage it occupies. This applies in the same way in opposite scenarios.

The coefficient matrix element values show a decreasing trend along the diagonal direction from the upper left to the lower right corner. Moreover, the upper left corner element of the matrix is used to calculate the harsh value as well as the size between each element on this corner compared to the average value of the total elements. If the single element in the coefficient matrix of the upper left corner is either larger than or equal to the mean, it is recorded as 1; otherwise it is 0. In addition, the frequency component values with large coefficients are usually concentrated on the upper left corner of the coefficient matrix. The obtained binary string is the pHash value of the image. The DCT significantly preserves the low-frequency components of the picture. As long as the overall structure of the image does not change, the hash value of the image can remain unchanged.

Finally, the dHash algorithm is constructed based on the pixel domain design. In particular, the picture hash value is calculated from the difference between many adjacent pixels. First, the reduced image is converted into a grayscale image by grayscale processing. Second, the size relationship between the adjacent pixel values is compared with regard to the same line performance on the pixel matrix. If the pixel value on the left is larger than the pixel value on the right, it is recorded as 1; otherwise, it is recorded as 0. The closer the relationship between the pixels of two images, the higher the similarity between them. Therefore, the hash value of the image can be obtained by comparing all the rows of the pixel matrix.

To assess their potential and advantages, three similarity detection algorithms are compared, and the following results are obtained. First, the pHash algorithm is optimal in terms of the recognition effect, and the dHash algorithm is better than the aHash algorithm. Second, in terms of the implementation speed, the aHash algorithm is the fastest, and the dHash algorithm works better than the pHash algorithm. Third, the dHash algorithm is in the middle position in terms of both the recognition effect and implementation speed.

Therefore, in this study, the pHash algorithm is used to verify the similarity between the iris image of the differential privacy protection and original images. The detailed processing steps are as follows:

1. Reduce the size of the image: The size is decreased quickly to remove the high-frequency and detailed information of the image. Only the structure and brightness of the image are preserved. This can exclude the difference between the different sizes and different proportions of the image;
2. Simplify the color of the image: Grayscale processing is performed on the image, and the influence of the color difference on the processing result is eliminated. In addition, the operation can also significantly improve the efficiency of the subsequent algorithms;
3. DCT: This transform further compresses the image to be processed. After DCT, the DCT coefficient energy of the image is mainly concentrated in the upper left corner of the image so that only the area of the upper left corner, 80×80, needs to be retained. Finally, the DCT coefficient mean is obtained;
4. Obtain a hash sequence: Comparing the pixels in the region with the mean value of the DCT coefficient, the position of the pixel larger than or equal to the mean is recorded as 1. Then, the number of different hash sequences in the image to be detected and image template is compared. The number represents the Hamming distance. Finally, the obtained Hamming distance is saved to provide the basic data for setting the subsequent discriminant threshold;

5. Compare the Hamming distance: The Hamming distance between the iris images is obtained by the image hashing technique, and the original image is denoted as h. The smaller the Hamming distance, h, the more similar the two images are.

5 | RESULT AND DISCUSSIONS

To show the privacy protection effect, we present numerical examples in this section. Figure 2 is an iris picture taken from the iris database of the Chinese Academy of Sciences [36]. In our simulation examples, there exists differential privacy based on two noise mechanisms to hide the iris features. The left images of Figure 3 show the iris images after adding Laplacian noises with different noise parameters, ε. Meanwhile, the enlarged local iris images after adding Laplacian noises with different noise parameters ε are presented in the middle pictures of Figure 3. For a clearer display, the images on the right in Figure 3 magnify the images in the red box. Figure 4 presents the iris images and enlarged local iris images after adding Gaussian noises with different noise parameters, ε. According to the simulation results, it can be seen that the iris image after the differential privacy protection based on the Laplacian noise and Gaussian noise mechanism hides the features of Figure 2. As the noise parameter, ε, increases, the effect of the iris feature being hidden is better.

This study uses MATLAB to simulate 50 iris images of with 640×480 pixel values taken from the Chinese Academy of Sciences iris database. Some details of the iris images will be hidden when the iris image information is scaled to 80×80 dimensions. The 0 and 1 sequence values generated by an iris image are the hash values of the image for a total of 6400 bits. Figure 5 shows the magnitude of the hash difference between the iris image after the privacy protection based on the two noise mechanisms and the original image when the noise parameters are $\varepsilon = 0.02$, 0.04, and 0.06. When the hash difference is larger than 100, it implies that the two pictures are not completely similar. When the Laplacian noise parameter value is $\varepsilon = 0.02$, we can see that the corresponding hash difference is above 100, which verifies that our de-identification method can well protect the privacy characteristics of the iris. From the results, it can be seen that the image differential privacy of the Gaussian noise is slightly better than that of the Laplacian noise under the same noise parameters.

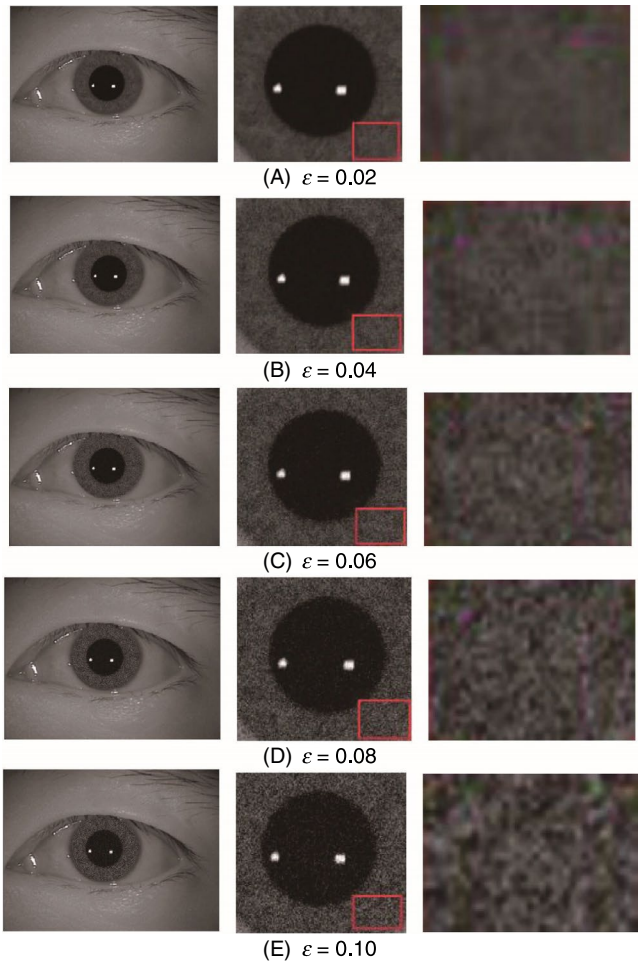


FIGURE 4 Iris image after adding Gaussian noises with different noise parameters ε

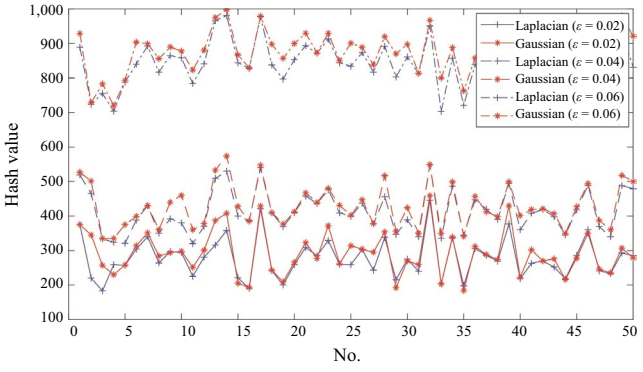


FIGURE 5 Comparison of the hash differences between 50 iris privacy-protected images and original images based on the two noise mechanisms

6 | CONCLUSION

This paper proposes a privacy-preserving method based on a differential privacy model to protect the privacy information of iris features, and achieves a good iris feature hiding effect. Specifically, we employ the Laplacian mechanism and Gaussian mechanism to hide the iris biometric features in the images when the privacy requirement parameter is given. As the noise parameters increase, the privacy protection level becomes stronger. We verify the performance of the two mechanisms by simulation. The simulation results show that the privacy protection based

on the Gaussian noise is slightly better than that based on the Laplacian noise for the same noise parameter. Our future work is to design a mobile applet with the proposed algorithm, in this paper, to avoid the illegal use of iris-sensitive information.

ORCID

Wenming Jiao https://orcid.org/0000-0003-2644-5174
Heng Zhang https://orcid.org/0000-0002-4201-3892
Qiyan Zang https://orcid.org/0000-0001-9464-9887
Weiwei Xu https://orcid.org/0000-0002-3239-0483
Shuaiwei Zhang https://orcid.org/0000-0002-2407-8457
Jian Zhang https://orcid.org/0000-0001-5764-9351
Hongran Li https://orcid.org/0000-0002-7437-7359

REFERENCES

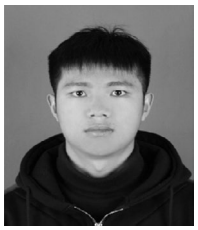
1. T. Root et al, *Fingerprints of global warming on wild animals and plants*, Nature **421** (2003), no. 6918, 57–60.
2. Y. Zheng, D. K. Pal, and M. Savvides, Ring *loss: Convex feature normalization for face recognition,* in Proc. IEEE Conf. Comput. Vis. Pattern Recogn., Salt Lake Sity, Canada, June. 2018, pp. 5089–5097.
3. M. Mottalli, M. Mejail, and J. Jacobo-Berlles, *Flexible image segmentation and quality assessment for real-time iris recognition,* in Proc. IEEE Int. Conf. Image Process. Cairo, Eqypt, Nov. 2010, pp. 1941–1944.
4. L. E. Ali, J. Luo, and J. Ma, *Iris recognition from distant images based on multiple feature descriptors and classifiers,* in Proc. IEEE Int. Conf. Signal Process., Chengdu, China, Nov. 2016, pp. 1357–1362.
5. K. Wang and K. Ajay, *Cross-spectral iris recognition using cnn and supervised discrete hashing*, Pattern Recogn. **86** (2019), 85–98.
6. Z. Zhang et al, *Bilateral privacy-preserving utility maximization protocol in database-driven cognitive radio networks*, IEEE Trans. Depend. Secure Comput. (preprint), https://doi.org/10.1109/TDSC.2017.2781248.
7. J. Fridrich, *Image encryption based on chaotic maps,* in Proc. IEEE Int. Conf. Syst. Man, Cybernetics, Orlando, FL, USA, Oct. 1997, pp. 1105–1110.
8. J. Fridrich, *Symmetric ciphers based on two-dimensional chaotic maps*, Int. J. Bifurcat. Chaos **8** (1998), no. 6, 1259–1284.
9. K. Simoens et al, *A framework for analyzing template security and privacy in biometric authentication systems*, IEEE Trans. Inf. Forensics Secur. **7** (2012), no. 2, 833–841.
10. W. A. A. Torres, N. Bhattacharjee, and B. Srinivasan, *Effectiveness of fully homomorphic encryption to preserve the privacy of biometric data,* in Proc. Int. Conf. Inf. Integ. Web-based Applicat. Serv., Hanoi, Viet Nam, Dec. 2014, pp. 152–158.
11. J. Bringer et al, *Faster secure computation for biometric identification using filtering,* in Proc. Int. Conf. Biometrics, New Delhi, India. 2013, pp. 257–264.
12. B. Hayes, *Cloud computing*, Web Sci. **51** (2008), no. 7, 9–11.
13. J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, *A survey of recent results in networked control systems*, Proc. IEEE **95** (2007), no. 1, 138–162.
14. H. Zhang et al, *Privacy and performance trade-off in cyber-physical systems*, IEEE Netw. **30** (2016), no. 2, 62–66.
15. N. Srichumroenrattana, R. Lipikorn, and C. Lursinsap, *Stereoscopic face reconstruction from a single 2-dimensional face image using orthogonality of normal surface and y-ratio*, Int. J. Pattern Recognit. Artif. Intell. **30** (2016), no. 2, 1–27.
16. B. Benjamin et al, DP-finder: *Finding differential privacy violations by sampling and optimization*, in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Toronto, Canada, Oct. 2018, pp. 508–524.
17. A. Martin et al, *Deep learning with differential privacy*, in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Vienna, Austria, Oct. 2016, pp. 308–318.
18. C. Thee et al, *MVG mechanism: differential privacy under matrix-valued query*, in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Toronto, Canada, Oct. 2018, pp. 1–17.
19. A. Bhowmick et al, *Protection against reconstruction and its applications in private federated learning*, Mach. Learn. **1812** (2018), 1–45.
20. R. Venkatesan, S.-M. Koon, and M. Jakubowski, *Robust image hashing,* in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2000, pp. 664–666.
21. T. Kalker, J. Haitsma, and J. Oostveen, *Issues with digital watermarking and perceptual hashing,* in Proc. Int. Symp. Converg. IT Commun., Denver, CO, USA, 2001, pp. 189–197.
22. J. Fridrich and M. Goljan, *Robust hash functions for digital watermarking,* in Proc. Int. Conf. Inf. Technol. Coding Comput., Las Vegas, NV, USA, Mar. 2000, pp. 1–6.
23. L. Chun-Shien et al, *Robust mesh-based hashing for copy detection and tracing of images,* in Proc. IEEE Int. Conf. Multimedia Expo, Taipei, Taiwan, June 2004, pp. 731–734.
24. S. Kozat, R. Venkatesan, and M. K. Mihcak, *Robust perceptual image hashing via matrix invariants,* in Proc. Int. Conf. Image Process., Singapore, Oct. 2004, pp. 3443–3446.
25. Z. Tang et al, *Robust image hashing using ring-based entropies*, Signal Process. **93** (2013), no. 7, 2061–2069.
26. H. Wei, J. X. Yu, and C. Lu, *String similarity search: a hash-based approach*, IEEE Trans. Knowl. Data Eng. **30** (2018), no. 1, 170–184.
27. Z. Liu et al, *Contextual hashing for large-scale image search*, IEEE Trans. Image Process. **23** (2014), no. 4, 1606–1614.
28. M. De Marsico et al, *Firme: face and iris recognition for mobile engagement*, Image Vis. Comput. **32** (2014), no. 12, 1161–1172.
29. W. Boles, A *security system based on human iris identification using wavelet transform,* in Proc. Int. Conf. Convent. Knowl. Based Intell. Electron. Syst., Adelaide, Australia, May 1997, pp. 533-541.
30. C. Dwork, *Differential privacy,* in Proc. Int. Colloquium Automata Lang. Program., Venice, Italy, July 2006, pp. 1–12.
31. J. Soria-Comas et al, *Individual differential privacy: a utility-preserving formulation of differential privacy guarantees*, IEEE Trans. Inf. Forensics Secur. **12** (2017), no. 6, 1418–1429.
32. S. Goryczka and X. Li, *A comprehensive comparison of multiparty secure additions with differential privacy*, IEEE Trans. Dependable Secure Comput. **14** (2017), no. 5, 463–477.
33. F. Liu, *Generalized gaussian mechanism for differential privacy*, IEEE Trans. Knowl. Data Eng. **31** (2019), no. 4, 747–756.

34. Y. Feng et al, *Visual tracking via multi-experts combined with average hash model*, Proc. Asian Conf. pattern recognition. (2016), 331–335.
35. X. Niu and Y. Jiao, *An overview of perceptual hashing*, Acta Electronica Sinica **36** (2008), no. 7, 1405–1411.
36. G. Vrcek and P. Peer, *Iris-based human verification system: a research prototype,* in Proc. Int. Conf. Syst., Chalkida, Greece, June 2009, pp. 1–4.

AUTHOR BIOGRAPHIES

Wenming Jiao is currently a masters student at Jiangsu Ocean University and is also pursuing a Masters degree at the China University of Mining and Technology, Xuzhou, China. His current research interests include image processing, privacy protection, and intelligent optimization.

Heng Zhang received his PhD in control science and engineering from Zhejiang University, Hangzhou, China, in 2015. He is currently an Associate Professor with the School of Science, Jiangsu Ocean University, Lianyungang, China. He was a Research Fellow with Western Sydney University, Penrith, NSW, Australia. His current research interests include security and privacy in cyber-physical systems and control and optimization theory. Dr. Zhang is an editorial board member of several academic journals, including IET Wireless Sensor Systems, the EURASIP Journal on Wireless Communications and Networking, and the KSII Transactions on Internet and Information Systems. He also serves as a Guest Editor for the Journal of the Franklin Institute and Peer-to-Peer Networking and Applications.



Qiyan Zang received his Bachelor of Science degree from Jiangsu Ocean University, Lianyungang, China. His current research interests include machine learning, deep learning, and data mining.

Weiwei Xu is currently a masters student at Jiangsu Ocean University and is also pursuing a Masters degree at the China University of Mining and Technology, Xuzhou, China. His current research interests include image processing and control theory.

Shuaiwei Zhang is currently pursuing a Bachelor of Science degree at Jiangsu Ocean University, Lianyungang, China. His current research interests include big data analysis and image processing.

Jian Zhang received his Bachelor of Science degree in educational technology from Qufu Normal University in 2001. He received his Master of Science degree in computer science from Bohai University in 2006 and a PhD from Nanjing University of Science and Technology (NUST), in pattern recognition and intelligence systems in 2015. From 2016 to 2017, he was a Postdoctoral Fellow at the School of Applied Science and Textiles, Hong Kong Polytechnic University. Currently, he is an Associate Professor with the School of Computer Science and Engineering, Jiangsu Ocean University. He is the author of more than 30 scientific papers on pattern recognition and computer vision. His research interests include pattern recognition, computer vision, and machine learning.

Hongran Li received his Bachelor of Engineering and Master of Engineering degrees in electronics and computer engineering from Kinki University, Fukuoka, in 2012 and 2014, respectively, and his PhD from Kanazawa University in 2017. In 2017, he also joined the Jiangsu Ocean University as an Associate Professor. His research interests include control theory and control security and its applications.