EURASIP Journal on Image and Video Processing

RESEARCH Open Access

Research on iris image encryption based on deep learning

Xiulai Li[1,2], Yirui Jiang[1], Mingrui Chen[1*] and Fang Li[3]

Abstract

With the development of information technology, the demand for information security is increasing. For more convenient and safer needs, the encryption technology based on biometrics has developed rapidly. Among them, iris technology has become an important research object of information security research due to the stability of iris characteristics and its difficulty in forgery. In this paper, the iris feature encryption technology based on the iris is studied by using the method of deep learning as the feature classification method and the iris feature as the research object. The simulation experiment is carried out by using the common iris database. The results show that the method can greatly improve the consistency of iris encryption and improve the security of encryption and decryption process.

Keywords: Image analysis, Iris, Deep learning, Image encryption

1 Introduction

With the development of technology, people have entered the era of big data, Internet technology and computer technology have developed rapidly, the popularity of the network is very extensive, and information interaction technology is becoming more and more mature. While people generally use the network to transmit information, it also breeds many information security issues. As the network enters various fields, the security of information transmission increasingly affects the security of individuals, enterprises, and even countries.

The image has a very good expression effect on the contained information because of its visual characteristics. It is widely used in information interaction, so many information expressions are more favored for images. Owners with important value images often use the Internet to achieve auctions or publish their own image information. This method overcomes the limitations of geographical conditions such as geography and is not only convenient and fast, but also reduces economic costs. However, in the process of network transmission, the insecurity factors of image information give the malicious attack the opportunity to attack, and the original image information may be attacked and lead to information leakage or information destruction. Image encryption algorithm aims at improving the security of image information, reducing the probability of information leakage and destruction, and ensuring the safe transmission of original information. In some special circumstances, image data must be encrypted to transmit. For example, in medical image transmission, in order to protect patient privacy, these pictures need to be encrypted before they can be transmitted over the Internet. The security of image information involves a wide range of social sectors, ranging from individuals to countries. Attacks such as malicious destruction and information theft by the criminals frequently occur, and image encryption technology is developing rapidly. How to improve image security, anti-attack capability, and key transmission security is an urgent problem to be solved [1].

The rapid development of information technology, the increasing need for information security transmission, and the biometric-related technology are developing rapidly. Human biometrics refer to the information features produced by human tissue structure, including the iris [2–4], face [1, 5], fingerprint [6–8], voice [9–11], DNA [12–14], and palm postures [15]. The biological characteristics of human body are widely used in identity recognition and other fields because of their uniqueness. Iris recognition technology is used to extract the characteristics of the iris. By comparing with the iris database image to calculate the similarity, the identity decision is finally

* Correspondence: 17786967707@163.com
[1]Hainan University at Meilan, No. 58 People' Rd. Meilan District, Haikou, China
Full list of author information is available at the end of the article

realized. It belongs to the human biological feature extraction technology and has a very excellent quality. Compared with other human biological characteristics, the iris has more excellent characteristics. It is more suitable for image encryption to improve the security and anti-attack ability of the algorithm. Academic and business circles pay more attention to identity recognition technology based on iris feature extraction. It has a wide application prospect and is gradually applied to some departments which need high security requirements, such as banking system, secrecy, and so on.

The target information contained in the image is filtered by feature extraction to perform information processing according to the user's needs. The biggest disadvantage of traditional machine learning is that many parameters need to be set manually during the learning process. This shortcoming is especially noticeable when dealing with big data and high-dimensional complex data. Deep learning technology belongs to machine learning [16–20], based on artificial neural network for data feature extraction. The original information is expressed as a feature vector through feature learning, input into a sub-learning system (such as classifier, decision maker), and then the sample is classified or detected. Feature learning is a means of detecting and classifying input samples. Through feature learning of input samples, feature extraction is automatically realized.

Deep learning uses a nonlinear neural network model to transform original data into higher-level abstract representations through nonlinear transformations. Deep learning uses an artificial neural network structure. After multiple linear transformations and nonlinear transformations, complex functions are constructed. The principle of sample classification is to strengthen the ability to discriminate data and weaken irrelevant factors by high-level expression of original data, illustrated by an example: The image is a matrix composed of many pixels. The first layer of the model expresses the features of the edge and position of the image. The second layer will display the features such as edges on the basis of the features extracted by the first layer to detect the pattern, while the interference item will be ignored. The third layer may further splicing and combining the detected images to show the part that has obvious detection or classification help for the target. Thus, as the number of layers increases, the target to be detected is gradually formed. Traditional machine learning is based on manual feature setting and machine learning algorithm is used to screen. The core of deep learning is automatic feature setting in each layer. Model training is realized through continuous feedback, and features are constantly learned from data. There are also some relevant research results on this aspect of research, which proves that relevant research is feasible [21, 22].

Image encryption has higher security requirements. Iris features are more suitable for extracting feature from deep learning algorithm and applying it to image encryption. Compared with other biometrics, it is more effective to improve encryption security. The traditional iris image encryption technology, the iris feature extraction method which uses machine learning algorithm, presents some problems of lack of feature learning and low efficiency, such as image preprocessing trouble, high quality of iris image quality, and the need to repeat the iris image acquisition in the process of decryption in order to achieve a correct decryption operation. In recent years, deep learning has solved many unsolved problems in the field of artificial intelligence with its excellent feature learning ability and has achieved rapid development. Research shows that deep learning is superior to other learning algorithms in many fields, especially in feature learning on high-dimensional complex data and big data, and has been applied in commercial, economic, and government fields. The reason why deep learning can be applied to image encryption technology is that it exhibits excellent learning ability for dealing with a large amount of data, accurately extracts essential features, and satisfies the high security requirements of image encryption.

In this paper, the deep learning algorithm is introduced to extract the iris image. Based on the original iris image encryption algorithm, a new iris image encryption algorithm based on deep learning is proposed. The image encryption function is realized by training the sample. The simulation experiments on the iris samples of the public iris database show that the proposed method can solve the inconsistency of iris features and improve the confidentiality of the encryption and decryption process.

2 Proposed method

2.1 Iris feature extraction

The structure of the human eye mainly includes the pupil, the iris, and the sclera (as shown in the upper left of Fig. 1). The pupil is an approximately circular black structure in the center of the eye. The white area around the eyeball is the sclera. The iris is located in the annular region between the pupil and the sclera. The texture information is very rich. The details of the iris are mainly stripes, wrinkles, crypts, stains, and so on (as shown in the lower left of Fig. 1). The best choice for biometric technology is the iris. The reason is that the iris has the advantages of highest uniqueness, high recognition accuracy, high speed, strong biological activity, strong anti-counterfeiting ability, and lifelong stability compared with other biological features.

It can be seen from the structure of the iris that the iris area of the human eye has a very rich texture feature. The iris is formed in the stage of human embryo

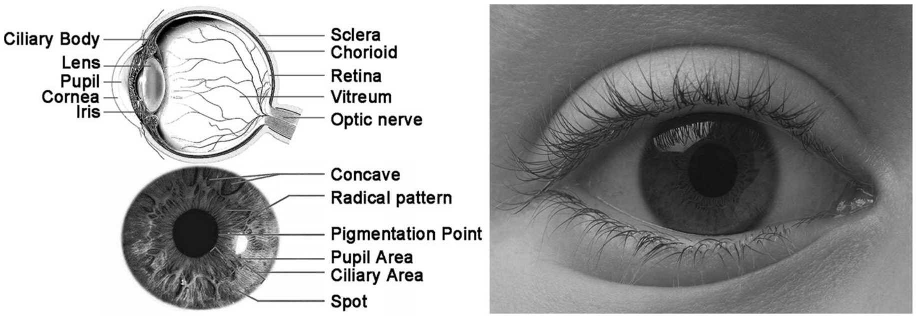

Fig. 1 Human eye structure and human eye sample

development, and the cell tissue grows randomly, resulting in a series of differences in shape, color, and gray in the iris area. These differences constitute iris texture features. The different shapes of scars, different gray areas, and randomness of features make the difference between iris very large. Texture is not affected by gene regulation, even though the iris texture of the right and left eyes of the same person varies greatly. After iris localization and human eye image segmentation, how to effectively extract the texture features contained in the iris is the most important step in the whole iris recognition system. Iris feature extraction refers to extracting the rich texture information contained in the iris as the feature code of the iris for subsequent matching recognition, and the distance measurement function determines the similarity between the two iris images. Iris recognition technology uses the invariance of the iris and the difference of features to achieve individual identification.

Individual identity is determined by comparing the similarities between features of the iris image. Image processing, pattern recognition, and other methods are used to describe and match the characteristics of the iris to automatically identify the identity. Typical iris recognition systems include iris image acquisition, preprocessing, feature extraction, and recognition. According to the above description of iris recognition technology, the iris recognition system framework is shown in Fig. 2.

As an important branch of pattern recognition, feature extraction and pattern classification of iris recognition are two important tasks. From the perspective of feature extraction, the existing iris recognition algorithms can be roughly divided into three categories: based on phase method, zero crossing representation method, and texture analysis method. From the perspective of the classification mechanism of iris samples, the existing algorithms can be divided into three categories: the algorithm based on the distance classification, the method of using the correlation analysis, and the classification algorithm through machine learning. There are few algorithms for classifying using machine learning. The most popular is the use of learning vector quantization (LVQ) in the classifier.

The iris contains rich features, and it is suitable for recognition, encryption, and other fields because of its excellent quality. How to extract high-efficiency and strong distinguishing features from iris images is a key part of iris application. Iris preprocessing mainly includes iris dryness, filtering, localization, and normalization.

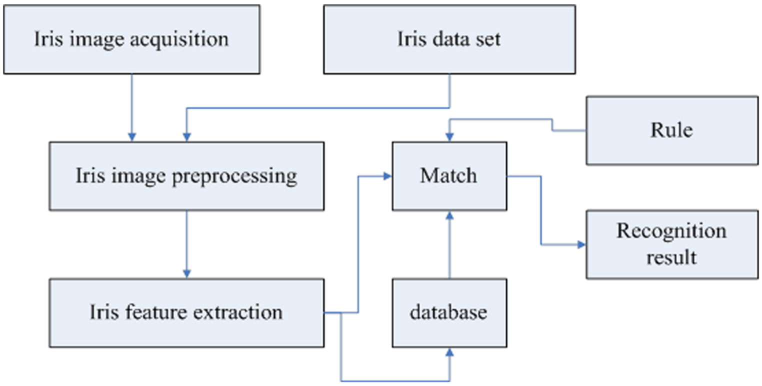

Fig. 2 Iris recognition system framework

There are many kinds of noise in the image, and the main purpose of image smoothing is to reduce noise. Their effect on the amplitude and phase of the image signal is very complex. Common noise includes additive noise, multiplicative noise, quantization noise, and "salt and salt noise." In the frequency domain, due to the high-frequency domain of the noise spectrum, various forms of low-pass filtering can be employed to reduce noise in the spatial domain. Image noise is often intertwined with signals, especially multiplicative noise, but the basis of smoothing is details such as edges and blurred contours, so smoothing noise removal is maintained as much as possible while maintaining image detail.

Smoothing usually uses Gaussian template for digital image processing. It removes point mutations for fixed point and several surrounding points to remove certain noise. The Gaussian template used in this paper is as follows:

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

In the case where the noise is not obvious, the smoothness does not contribute much to the segmentation and matching of the image, but it becomes difficult to find the edge point boundary due to the problem of blurring. The purpose of sharpening the image is to make the edges and outline blurred images clear and the details clearer. From a spectral point of view, the average or integral operation of the reverse operation (such as differential operation) is usually used. The essence of the image blur is the attenuation of the high-frequency component, which can make the image clear by the high-pass filter. It should be noted that sharpening of the image must require a higher signal to noise ratio, generally eliminating or reducing noise prior to sharpening. The difference method is one of the common methods of image sharpening, and the difference method is divided into two methods: first-order differential and second-order differential. Second-order differential operators are more sensitive to noise and tend to enhance noise components, so smoothing operations usually use second-order differentiation. Although the edge of the sharpened image is enhanced, the increase in noise is more serious, and image smoothing can effectively reduce noise.

The iris feature includes a lot of noise data, although the noise reduction method can reduce the noise, but it cannot remove all the noise. For the eye sample selected in this paper (as shown in the right of Fig. 1), in order to better extract the eye features, iris inner edge positioning and outer edge positioning method are used in this paper.

The inner edge of the iris is positioned using the gray projection method. The center and radius of the pupil are determined based on the gray scale distribution of the image. The gray scale distribution of the human eye image has certain characteristics. The gray scale distribution of the pupil, sclera, and iris is different, so the inner edge of the iris is defined by gray. In the imported image, find the sum of the pixels of the x and y axes, respectively, and find the point with the smallest pixel. Finally, use the traverse method to find the boundary point of the pupil.

The outer edge of the iris is positioned by the calculus operator method. Based on the gray scale characteristics of the human eye, the sclera is white, and the iris is darker. In the image, the gray scale contrast is large, so the detection of the outer boundary of the iris needs to be treated as follows on every point on the image.

(1) According to the length and width of the input image, the circle detection range of the center and the corresponding radius is determined. According to the circumferential parameters of the rough location of the outer iris boundary, the range of the value is narrowed and the positioning speed is accelerated.
(2) For all possible radii, count the gray scale average of the points on the circumference.
(3) Find the gray scale gradient of two adjacent circles.
(4) Find the radius of the gray gradient jump value.

The inner and outer edges of the iris are positioned as shown in Fig. 3. The left side of Fig. 3 is the inner edge, and the right side is the outer edge.

2.2 Deep learning theory

Deep learning is a popular research direction in recent years. Due to its unique network structure, its deepening in academic and industrial fields is often referred to as deep neural network. The deep learning network itself is an artificial neural network model, but it has improved in terms of network structure and learning algorithms than traditional artificial neural networks.

Deep learning is a new field of machine learning research. By establishing an artificial neural network model, it simulates the working mode of the human brain, so that it can make a correct judgment on the input information. After the deep learning network model is established, continuous learning is needed to optimize the training network model and improve the decision-making results. It is similar to human beings who need continuous learning after birth to make more accurate judgments.

Deep learning is used to construct a network structure with multiple hidden layers. The entire network training has a large amount of training data, and the deep

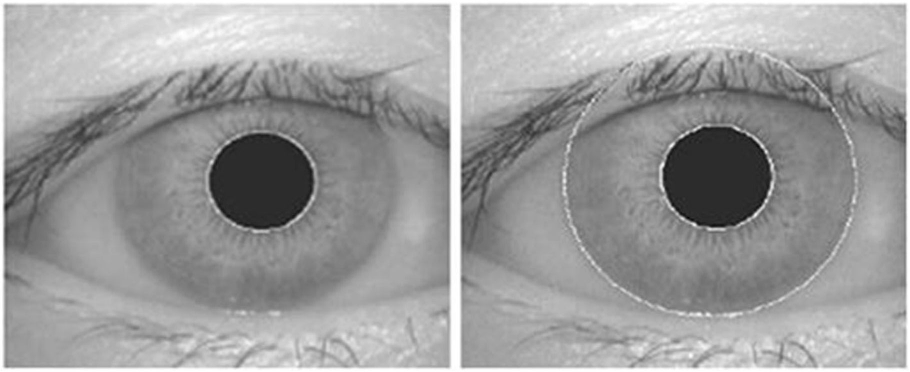

Fig. 3 Inner and outer edge location

network structure is used to extract features. Regardless of the human brain's visual mechanism or its mathematical properties, the characteristics of the deep model are far superior to the shallow model extraction feature, and the use of this feature is very good for classification and recognition. In this process, the depth of the multi-layer hidden layer model is a method, and feature extraction is the purpose of deep learning.

The convolutional neural network (CNN) is proposed by Yan Lecunn and his team. It belongs to a multi-layer neural network. The original CNN is mainly for the data processing of images and other data and has achieved very advanced results. The CNN structure has three special structures: convolution, downsampling, and weight sharing. The network structure of CNN makes it very few in terms of the number of parameters relative to other network structures. Each computing layer of the network consists of multiple feature maps, each of which is mapped into a plane with a higher distortion tolerance for the input samples in the recognition.

The CNN algorithm mainly includes two stages of forward propagation and back propagation, which are divided into four steps:

The first stage, the forward transmission phase:

(1) Extract a sample (X, Y_p) from the sample set and enter X into the network (X, Y);
(2) Calculate the corresponding actual output O_p.

In the forward propagation phase, information is converted from the input layer to the output layer, and the network performs the training process after completing normal operations. In this process, the network is implementing the calculation (actually, the input weight matrix is multiplied by each phase point, and the final output):

$$O_p = F_n\left(\dots\left(F_2\left(F_1\left(X_p W^{(1)}\right) W^{(2)}\right)\dots\right) W^{(n)}\right) \qquad (1)$$

The second stage, the backward propagation phase:

(1) Calculate the error of the network layer output O_p and the ideal output Y_p;
(2) The weight matrix is adjusted by inverse propagation according to the algorithm such as gradient descent, and the parameters are optimized.

CNN recognizes two-dimensional graphics with distortion invariance in the form of displacement and scaling. The feature detection layer of CNN is learned from training data, avoiding explicit feature extraction, and learning from the training data implicitly when using CNN. In addition, the weights of neurons on the same feature mapped surfaces can be studied in parallel, which is one of the advantages of CNN relative to the neurons connected to each other. CNN has a unique advantage in speech recognition and image processing. It has a special structure with local weight sharing, and the layout is closer to the actual biological neural network. The sharing of weight reduces the complexity of the network, especially for high-dimensional data. The input vector image can be directly input to the network feature to avoid the complexity of data reconstruction in feature extraction.

2.3 Iris feature extraction method based on deep learning

Deep learning can learn by unsupervised, semi supervised, or supervised methods of the original data, and extract the advanced features contained in the information. It can be used for pattern recognition, classification, and other scenes. Compared with the traditional feature extraction methods, it can produce better accuracy and achieve better application results. It is necessary to extract the feature of the iris image by using the iris to generate the image encryption key. However, the traditional feature extraction method is based on the image processing or shallow learning, and the operation is cumbersome and the quality of feature extraction is poor. So the feature extraction of iris image is carried out by deep learning. The feature extraction of iris image based on deep learning refers to the calculation of iris image by deep learning and extraction of the feature matrix, which mainly includes iris image acquisition, image preprocessing, feature depth learning, and feature extraction.

The specific process of extracting iris features using CNN can be described as the following steps:

(1) Iris image acquisition of the human eye to obtain an iris image;
(2) Iris image preprocessing to form an iris data set;
(3) Using the deep learning model CNN to learn the collected iris image dataset, including parameter initialization, model selection, and hyperparameter selection, and using the inverse gradient descent algorithm to train the model;
(4) The output matrix of the deep learning model is the extracted iris feature.

2.4 Reed-Solomon error correcting code

In the whole process of image acquisition, preprocessing, and feature extraction of the iris, due to many factors such as the external environment, the iris feature vector obtained by the two feature extractions before and after cannot be exactly the same. Then, in the image encryption algorithm, it is necessary to ensure that the encryption key used by the encryption side and the decryption key used by the decryption side are completely identical, so that the entire process of encryption and decryption can be successfully implemented. This creates a serious contradiction: the contradiction between the inconsistency of the iris feature vector and the strict correspondence of the keys. The error correction code model can well solve this contradiction.

The Reed-Solomon error correcting code (referred to as RS code) consists of two parts: the original code and the check code. The original code contains the original data, and the check code is a data code generated after performing a certain regular operation on the original code. Due to the interference of external factors, when the original code is different, the original code can be corrected by the check code, so that the original source code can be finally obtained. The coding algorithm steps of the RS code are:

(1) Calculate the m query source polynomial table according to the relation $n = 2^m - 1$ to obtain the original polynomial $p(x)$ corresponding to $GF(2^m)$, thereby generating an extension field of $GF(2^m)$ and establishing a correspondence relationship between the domain element d and the m vector.
(2) According to the error correction capability t, the generator polynomial $g(x)$ on $GF(2^m)$ is obtained:

$$g(x) = \prod_{i=1}^{2t} (x - a^t) \tag{2}$$

The $g(x)$ expansion formula is obtained according to the domain operation rule simplification as follows:

$$g(x) = \sum_{i=0}^{2t} a^{k(i)} x^i \tag{3}$$

(3) Encoding the information bit polynomial $M(x)$ according to the relation $C(x) = M(x)g(x)$ to obtain the code word polynomial $C(x)$.

The RS code belongs to the system linear block code, including the information bit and the supervised bit. The block code divides the continuous data bit stream into fixed-length groups, each group being further divided into m-bit symbols, usually taking 3 or 8 bits of data to form a symbol. The K symbols together form a source word, which is linearly encoded after being encoded as a code word called an m-bit symbol block code.

2.5 Iris image encryption and decryption method based on deep learning

The iris image encryption algorithm based on deep learning firstly performs normalization and other preprocessing on the collected iris image dataset and then uses the deep learning neural network model to extract the features of the iris image. The extracted feature vector is used for key generation, and finally, the XOR operation is performed on the key and the pixel value of the original image.

The encryption process can be described as the following steps:

(1) Normalizing the iris dataset and using the iris dataset to train the deep learning neural network model;
(2) The encryption side collects the iris image and inputs the trained deep learning model to extract the feature vector V. The dimension of the feature vector V1 can be adjusted according to the adopted image encryption algorithm;
(3) Using the RS error correcting code to encode the feature vector V, the encryption key Vk1 can be calculated;

(4) Using the encryption key Vk1 and the pixel matrix gray value of the image matrix to perform XOR operation to obtain an encrypted image, the entire encryption process is completed.

The decryption process is performed after the image is encrypted by the encrypting side, and after receiving the image ciphertext and the RS error correcting code transmitted by the encrypting side, the reverse algorithm of the encryption algorithm is used to realize the decryption of the ciphertext to obtain the plaintext. But the algorithm in this paper is not a complete inverse transformation. The decryption process can be described as the following steps:

(1) Performing iris image acquisition on the decryption side, inputting into the trained deep learning model, and realizing iris feature vector extraction V2;
(2) Since V2 and V1 may have different values in some dimensions, the RS error correction code is used to correct the feature vector V2 to obtain the decryption key Vk2;
(3) Using the decryption key Vk2 to encrypt the image matrix corresponding to the gray value of the pixel to perform XOR operation, and get the decrypted image, and then complete the whole process of decryption.

2.6 Evaluation method

Iris image encryption is different from general image encryption algorithms and has different indicators in algorithm evaluation. The evaluation indexes of iris image encryption algorithm mainly include the following.

False acceptance rate and error rejection rate: The false acceptance rate (FAR) is the probability that the wrong key correctly decrypts the original image. The false rejection rate (FRR) is the probability that the original image cannot be correctly decrypted with the correct key.

System security: System security is the most important indicator to measure the encryption algorithm, which restricts the feasibility of the encryption algorithm. It mainly includes indicators such as the probability of being attacked. The specific indicators and their implementation methods will be elaborated in the experiments in the following chapters. There is a probability that the attacked probability pointer will operate on the encryption system and successfully decode the plaintext. Unidirectionality refers to the ability to recover plaintext from all aspects of the encryption process. Discrimination refers to the successful decryption performance of different irises.

3 Experiments and results

3.1 Experimental dataset

In order to improve the credibility and predictability of the algorithm, the experimental iris dataset uses the CASIA iris database public version; CASIA is the first large-scale iris shared database built by the Institute of Automation of the Chinese Academy of Sciences using the self-developed iris image acquisition device. This paper uses the CASIA version 4.0. CASIA Iris Library Version 4.0 has added three distinctive datasets ASIA-Iris-Distance, CASIA-Iris-Thousand, CASIA-Iris-Syn based on version 3.0 and was officially released in March 2009. By the end of November 2010, there were more than 3635 applicants from more than 100 countries and regions, including 522 domestic and 3113 foreign countries, mainly in India (787), China (522), the USA (290), Britain (114), Brazil (82), France (39), and other countries. The database applicants include researchers from internationally renowned universities such as Harvard, MIT, CMU, and Cambridge, and other well-known international institutions, as well as R & D personnel from famous international enterprises such as Microsoft, Philips, BT (British Telecom), Sagem, and other government institutions such as the American Standardization Technology Institute and the US Naval Research Institute.

The deep learning model for feature learning of the iris uses CNN, and the dataset contains 400 images of irises in total, 10 types, 40 images per class. The CNN structure uses a five-layer network layer, the convolution process is a 5×5 convolution filter, and the sampling layer is a 2×2 pooling filter.

3.2 Experimental simulation environment

In this paper, the data simulation is carried out in the MATLAB 2014B environment.The data of each subject is divided into test set and training set according to the tenfold cross validation method. That is, the sample of the subjects was equally divided into ten parts, nine of which were training sets and one was a test set, which were calculated ten times for each sample, and the final results were averaged.

4 Discussion

The feature extraction is performed on the iris as described above. First, the inner and outer edges of the iris are positioned, and then the iris image is encrypted. The encryption process is described in Fig. 4, and the result of Fig. 4 shows that the original inner and outer edge features of the iris are encrypted into a set of encrypted images that are unrecognizable in appearance.

Deep learning is a feature extraction method based on neural network. Training and testing precision after network training are an important indicator to measure the classification results. Figure 5 shows the training and test accuracy comparison with the increase of sample number.

It can be seen from the results in Fig. 5 that as the number of samples increases, the accuracy also increases. The reason is that when the number of samples is too small, the extracted sample features are different, and the learning mechanism does not function. As can be seen from Fig. 5, when the number of samples is above 600, the accuracy is significantly increased. For test and training samples, the result of Fig. 5 shows that the precision of the training sample is higher than that of the test sample, because the training sample is the feature set of the input learning machine fitting, so the precision of the sample is higher than the test sample.

For the same person to perform feature extraction twice, two sets of feature vectors are generated. If two set of feature vectors are defined as A1 and A2, then for the random selected n group features, the difference index between the description feature (the difference degree F value) calculation method is as follows:

$$f=\frac{\sum_{i=1}^{n}\left(\sqrt{\sum_{j=1}^{256}\left(A1_{ij}-A2_{ij}\right)/(A1/2+A2/2)}\right)}{n} \tag{4}$$

where i and j are the number of two sample set.

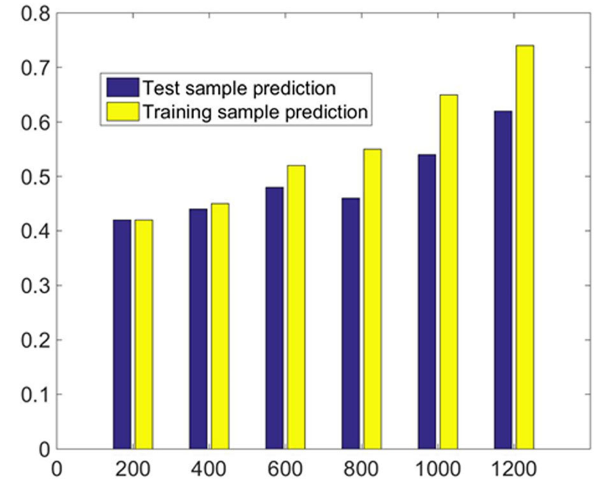

Fig. 5 Prediction results for training and testing samples

Table 1 shows the difference results of the deep learning iris encryption features before and after encoding. From the results of Table 1, the feature extraction difference of the same person collected in different cases is about 9%. The image encryption algorithm requires that the encryption key must be consistent with the decryption key before it can be decipher successfully. It is said that the difference between the feature vectors is 0%, so that can successfully encrypt and decrypt as the key. Therefore, Reed-Solomon error correction code is used to solve this problem. By comparison, the extracted

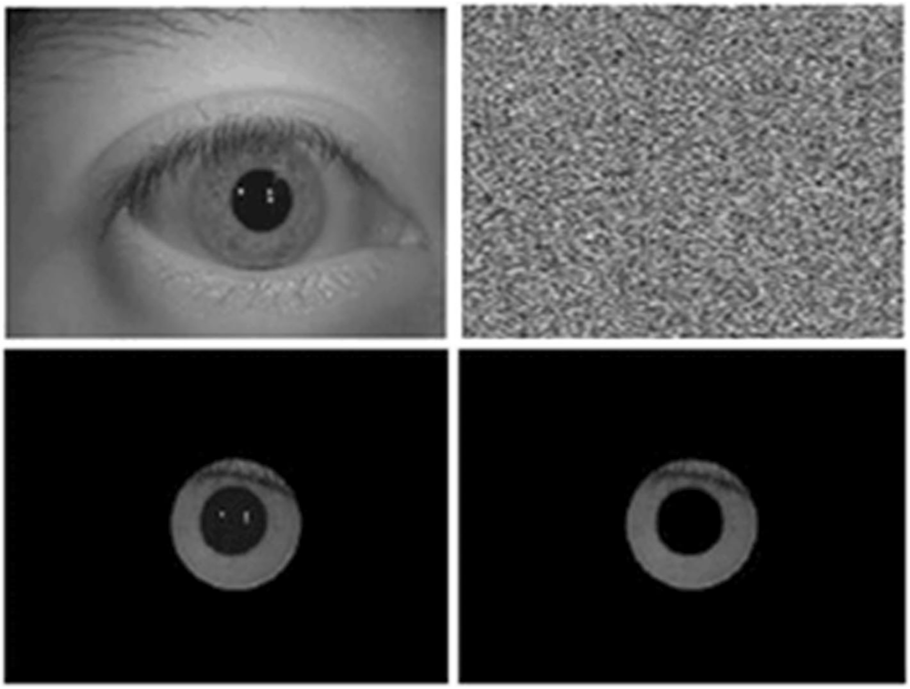

Fig. 4 Encryption of iris image

Table 1 Comparison of iris characteristics

Number of groups	5	10	20	30	40
Before coding	0.93	0.92	0.91	0.89	0.89
After encoding	0	0.01	0	0	0

256-dimensional feature vector is coded and corrected by RS code, then the feature vector selects *n* groups randomly for similarity matching and calculates the similarity between the feature vectors according to the formula, as shown in Table 1. The results were about 0.

Figure 6 shows the results of image encryption and decryption using the iris.

In order to verify the feasibility of the algorithm, this paper evaluates the algorithm from two aspects: decryption accuracy and security. The encryption algorithm requires that an illegal key cannot successfully decrypt the ciphertext, so the FAR must be equal to zero. Due to some unavoidable external interference during image acquisition, the iris image cannot be exactly the same. Therefore, the generated encryption key and decryption key cannot be completely consistent, and the legitimate user cannot be decrypted absolutely successfully, and the repeated operation is required to achieve the successful purpose.

As can be seen from Table 2, at $T = 92$, FAR = 0.003%, FRR = 1.043%, and the RS error correction code is encoded by (440, 256). That is to say, the illegal key cannot be successfully decrypted, and the legitimate key user has 1.043% need to perform two or more decryptions to achieve successful decryption.

After the encryption is completed, the ciphertext and the RS error correction code are transmitted. According to this, the plaintext reply cannot be performed, indicating that the encryption algorithm has unidirectionality. When the key is attacked according to the RS error correction code, only the guess can be made. When $T = 92$, the key with the key length of 256 is attacked by the probability of 2–428, so the deep learning algorithm is introduced to generate the key. It can greatly reduce the chance that the key will be compromised, thus improving the security of encryption.

Table 2 FAR and FRR for different thresholds

Threshold	FAR (%)	FRR (%)
96	0.015	2.045
95	0.014	1.882
94	0.007	1.402
93	0.013	2.206
92	0.003	1.043
91	0.014	1.557
90	0	1.484
89	0.005	1.972
88	0	2.009
87	0	1.237

5 Conclusions

In cryptography, the key is the key to successful encryption and decryption. The security of information depends on the security of the key. The traditional image encryption algorithm cannot resist the attack of malicious key sharing and repudiation. If the key length is too large, it will be easy to lose and it will be difficult to remember. Biometric encryption technology emerged as the times require, trying to solve the problem of poor security of key. The key is generated according to the biometrics of the individual and then applied to the corresponding image encryption algorithm to realize the information encryption. The biological features that can be encrypted should meet the characteristics of uniqueness, stability, non-aggression, and so on. The iris not only satisfies the requirements mentioned above, but also has rich feature information, strong anti-attack ability, and excellent encryption potential. Iris image encryption has become an

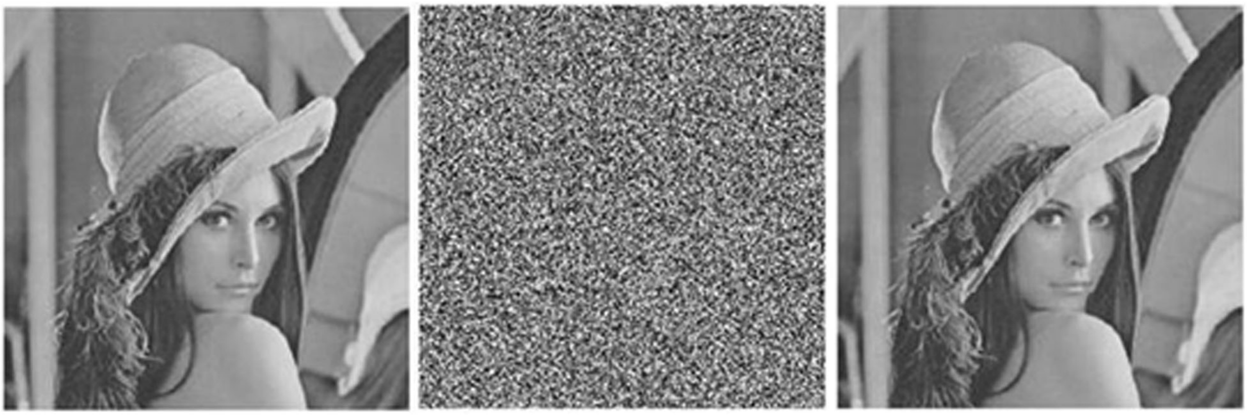

Fig. 6 Encryption and decryption results

important branch of image encryption and plays an important role in image encryption.

In this paper, the iris is taken as the research object, and the image encryption and decryption process based on iris feature is realized. The iris feature extraction algorithm based on deep learning is established. The extracted features are used for image encryption and decryption processing, and the proposed algorithm is objectively evaluated. The simulation results of the public iris database show that the proposed method can achieve image encryption.

Abbreviations

CNN: Convolutional neural network; DNA: Deoxyribonucleic acid; FAR: False acceptance rate; FRR: False rejection rate; LVQ: Learning vector quantization; RS code: Reed-Solomon code

Acknowledgements

The authors thank the editor and anonymous reviewers for their helpful comments and valuable suggestions.

About the authors

Xiulai Li was born in Anqing, Anhui, People's Republic of China, in 1992. He received bachelor's degree from Beijing Forestry University, People's Republic of China. Now, he studies in the College of Information Science and Technology, Hainan University. His research interest includes computational intelligence, cloud security, and information security.

Yirui Jiang was born in Zhumadian, Henan, People's Republic of China, in 1994. She received bachelor's degree from Zhengzhou University, People's Republic of China. Now, she studies in the College of Information Science and Technology, Hainan University. Her research interest includes computational intelligence.

Mingrui Chen was born in Chengmai, Hainan, People's Republic of China, in 1960. She received bachelor's degree from South China Normal University, Hainan, People's Republic of China. Now, he works in the College of Information Science and Technology, Hainan University, His research interests include software engineering, computer science, and information security.

Fang Li was born in Hanchuan, Hubei, People's Republic of China, in 1968. She received bachelor's degree from Tongji Medical University, Shanghai, People's Republic of China. Now, she works in The Maternal and Child Health Hospital of Hainan Province; her research interests include health care and health management during pregnancy and childbirth, Internet Med, and Big data on health.

Funding

This work was supported by the funding project of A study on multiple mapping fusion Chinese and English automatic word alignment system based on multi-preprocessing mechanism takes the establishment of parallel corpus on the Chinese-English translation website of Hainan tourism text as an example (No. 20167238) and the funding project of Construction and application of female health system in Hainan (No. ZDYF2016136).

Availability of data and materials

We can provide the data.

Authors' contributions

All authors take part in the discussion of the work described in this paper. The author XL wrote the first version of the paper. The authors XL and YJ did part experiments of the paper, and MC revised the paper in different versions of the paper, respectively. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details

[1]Hainan University at Meilan, No. 58 People' Rd. Meilan District, Haikou, China. [2]Hainan Hairui ZhongChuang Technology Co. Ltd, Haikou, China. [3]The Maternal and Child Health Hospital of Hainan Province, Haikou, China.

Received: 15 August 2018 Accepted: 15 October 2018
Published online: 16 November 2018

References

1. M. Carcary, K. Renaud, S. Mclaughlin, et al., A framework for information security governance and management. IT Prof. **18**(2), 22–30 (2016)
2. X. Wu, N. Qi, K. Wang, et al., in *Iihmsp '08 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. An iris cryptosystem for information security (IEEE, Elsevier Advanced Technology Publications Oxford, 2008), pp. 1533–1536
3. J. Daugman, Information security technical report - prospectus: recognizing people by their iris patterns. Inf. Secur. Tech Rep. **4**, 29 (1999)
4. W. Abdul, A. Alzamil, H. Masri, et al., Fingerprint and iris template protection for health information system access and security. J. Med. Imaging Health Inform. **7**(6), 1302–1308 (2017)
5. S. Zhou, X. Lu, in *Information Science and Management Engineering*. Fingerprint identification and its applications in information security fields (IEEE, Shaanxi, 2010), pp. 97–99
6. M.M. Mahmoud Musleh, I.I. Ba, K.M.A. Nofal, et al., Improving information security in e-banking by using biometric fingerprint: a case of major bank in Malaysia. Int. J. Comput. Sci. Inf. Secur. **10**(3), 1–4 (2012)
7. J. Shang, H. Huang, in *International Conference on Computer Science and Service System*. Shallow fingerprint identification information security technology in the electronic commerce application (IEEE, 2011), pp. 1684–1687
8. Ryu H. Information security attachment device for voice communication and information security method for voice communication using the same. 2016
9. L.A. Johnson, K.L. Dempsey, D. Bailey, et al., SP 800-128. Guide for security-focused configuration management of information systems. J. Dairy Sci. **77**(6), 1604–1617 (2011)
10. J.G. Chouhan, N.K. Singh, P.S. Modi, et al., Camera and voice control based location services and information security on android. J. Inf. Secur. **07**(3), 195–205 (2016)
11. G. Cui, L. Qin, Y. Wang, et al., in *IEEE International Workshop on Anti-Counterfeiting, Security, Identification*. Information security technology based on DNA computing (IEEE, Xiamen, 2007), pp. 288–291
12. G. Cui, L. Qin, Y. Wang, et al., *Information Security Technology Based on DNA Computing* (2007), pp. 288–291
13. G. Cui, C. Li, H. Li, et al., in *International Conference on Natural Computation*. DNA computing and its application to information security field (IEEE Computer Society, Tianjin, 2009), pp. 148–152
14. Y. Mizuchi, Y. Hagiwara, A. Suzuki, et al., *Monocular 3D Palm Posture Estimation Based on Feature-Points Robust Against Finger Motion* (2013), pp. 1014–1019
15. S. Bhilare, G. Jaswal, V. Kanhangad, et al. *Single-sensor hand-vein multimodal biometric recognition using multiscale deep pyramidal approach[J]. Machine Vision & Applications* (2018) pp. 1-18.
16. Y. Rao, J. Ni, in *IEEE International Workshop on Information Forensics and Security*. A deep learning approach to detection of splicing and copy-move forgeries in images (IEEE, London, 2017), pp. 1–6
17. J. Ye, J. Ni, Y. Yi, Deep learning hierarchical representations for image steganalysis. IEEE Trans. Inf. Forensics Secur. **12**(11), 2545–2557 (2017)
18. M.E. Aminanto, K. Kim, in *International Workshop on Information Security Applications*. Detecting impersonation attack in WiFi networks using deep learning approach (Springer, Cham, 2016), pp. 136–147
19. T.P. Le, Y. Aono, T. Hayashi, et al., in *International Conference on Applications and Techniques in Information Security*. Privacy-preserving deep learning: revisited and enhanced (Springer, Singapore, 2017), pp. 100–110
20. Z. Chen, D.O. Information, Face deep learning technology in the design and implementation of the security in colleges and universities. J. Anyang Inst. Technol. **16**(6),70-75(2017)
21. M. Kumar, Y.H. Mao, Y.H. Wang, T.R. Qiu, C. Yang, W.P. Zhang, Fuzzy theoretic approach to signals and systems: static systems. Inf. Sci. **418**, 668–702 (2017)
22. W.P. Zhang, J.Z. Yang, Y.L. Fang, H.Y. Chen, Y.H. Mao, M. Kumar, Analytical fuzzy approach to biological data analysis. Saudi J. Biol. Sci. **24**(3), 563–573 (2017)