Wang and Meng *EURASIP Journal on Image and Video Processing* (2018) 2018:92
https://doi.org/10.1186/s13640-018-0335-1

EURASIP Journal on Image and Video Processing

RESEARCH Open Access

Digital image information hiding algorithm research based on LDPC code

Zhong-xun Wang and Xiang-cai Meng*

Abstract

LDPC (low-density parity-check code) is a parity check code, and its performance is very close to Shannon limit. It is a sort of good channel code which has good ability of error correction. The coding can be introduced to an information-hiding algorithm because of its functional advantages. This way can improve robustness of a system in the process of information hiding, and it has a good application prospect. In this paper, a new algorithm is proposed which concludes two steps. Firstly, the encryption information needs to be implemented scrambling dispose; secondly, LDPC codes and modulation are used in the algorithm, and the encryption information is embedded into the carrier image, so the process of watermark embedding is completed. The method realizes the double encryption of information, and it improves the system's stability and security. Under the test of MATLAB emulation, the application of LDPC code in encryption algorithm is fully verified.

Keywords: Encryption algorithm, LDPC code, Chaos sequence, Digital watermarking

1 Introduction

Nowadays, the Internet and communication technologies have made great development. Data and digital media technologies are also increasingly prosperous. In the context of big data, the concept of "Internet Plus" is proposed which has caused a new wave of Internet communications. Under the leadership of the 5G era of mobile communications, the technology has entered a new peak. At the same time, the development of big data and communications has made people put forward higher requirements on the speed and quality of communications. In the new period, the main target and requirement is that improving the validity and reliability of information.

In the era of big data information, people realized the convenience of information circulation. However, under the premise of obtaining a large amount of information, a series of information security problems have also emerged. For example, digital information is stolen, altered, copied, and information's copyrighted is infringed, etc. [1] These problems have become increasingly prominent which have made information security research and development become more and more urgent. In the transmission process, information needs to pay more attention to the security and confidentiality issues. Therefore, information encryption technology has become a hot topic in the field of communication security, and it also has received widespread attention.

In the field of information hiding, the research of digital watermarking technology is relatively extensive. The main idea of digital watermarking is to add confusing visual digital watermarks to the transmission objects so that the data information can be protected. However, this primary encryption operation is relatively simple and the encryption information can be easily found in the process of transmission. And on the other hand, the encryption operation's effect is not ideal due to the interference caused by the loss of a large amount of information. The researchers found that the watermarking system and the communication system are very similar in some aspects [2]. Therefore, the channel coding can be introduced into the watermarking algorithm. The error correction performance of the channel coding is very good, and it can help the information resist the interference and improve the robustness of the system.

In the currently known channel coding, low-density parity check (LDPC) code is a very good code with excellent performance, especially after combining with high-efficiency modulation, which is very close to the Shannon limit [3]. It has a strong error correction and

* Correspondence: ytwzx3@126.com; ytumxc@163.com
Institute of science and technology for Opto-Electronics information, Yantai University, Yantai, China

detection capabilities that can enhance the reliability of information transmission. At present, the code has been widely applied to the digital watermarking systems, and it provides a powerful guarantee for information encryption.

In summary, it can be seen that under the background of the era of communication, it is very necessary to hide and encrypt information and protect personal privacy. The research of watermark encryption algorithm is a very practical significance.

1.1 Research status of LDPC codes

The LDPC code was first proposed by Professor Gallager of the USA in 1962 [4]. Since its performance is closest to the Shannon limit which is only 0.0045 dB, it has become one of the talked-about in error correction code, and it is also listed as the mainstream of the next generation of mobile communication error-correcting code. However, the code was not widely publicized at the time because there was no effective theoretical support. Until 1996, Mackay, Spielman, and Wiberg found that LDPC code has excellent performance and distance characteristics. Both theoretical and practical have great potential for development [5].

In recent years, LDPC codes have made great development and achievements. In the coding construction method, the original random structure is transformed into algebraic structure, such as geometric method, graphic method, and experimental method [6]. From a certain extent, these various construction methods increase the code loop and optimize the node distribution. At the same, the methods reduce the complexity of the encoding, while improving the excellent performance of the LDPC code.

M. Gluby et al. proposed that searching for non-regular codes could enhance the function in the binary finite filed [7]; Mackay et al. put forward a two-step selection method on the basis of non-regular codes to achieve external to internal choice [8]; T J Richardson et al. proposed a method to solve the problem of sparse matrix and find a way to reduce the number of structures to approach the Shannon limit [9]; DA Spielman developed a method to find the distribution of irregular LDPC codes degree, which is namely the heuristic method, and this approach results in a low BER at low SNR, which leads to construction of a minimum ring length LDPC code [10]. In addition, Y. Kou and S. Lin et al. also proposed the coding method on based on geometry construction [11].

LDPC code is a very excellent code which can meet the current high-speed and high-quality transmission requirements. It has a very good spot with the current era of network communications 4G and even 5G, and has made a great contribution for the growth of communication technology. Nowadays, LDPC code has been adopted by satellite digital video broadcasting standard DVB-S2, which has become the highlight of the company's plan and plays more important role in the coding filed.

1.2 Development status of image encryption algorithm

With the continuous development of Internet technology, the requirements for information security are getting higher and higher. The image encryption algorithm has attracted the attention of many people. It generally includes adaptive image encryption algorithm, chaotic system encryption algorithm, and the blind source separation algorithm and some important digital watermark encryption algorithm.

Image encryption algorithm is derived from the earliest cryptography, which is an important branch of the ancient steganography. Its main content is to hide the information that needs to be kept secret in the carrier and transmits the secret information through the transmission of the carrier to complete the confidential work. Thus, the obtained information can be prevented from illegal people. According to the characteristics of the carrier itself, it can be divided into spatiotemporal domain encryption and transform domain encryption.

At present, many kinds of image encryption algorithms have been proposed at home and abroad, such as using LDPC non-regular codes and using wavelet packet transform (DWT) and singular value decomposition (SVD) methods, to reduce the bit error rate of transmission [12]. The watermarking image is embedded through the way of random mapping and LDPC encoding compression [13]. Another digital watermarking algorithm uses the transmission rules of LDPC codes and images to achieve watermark extraction [14]. There is also the use of LDPC in constellation mapping rule to realize the hiding of watermark information and the encryption algorithm [15].

The above algorithms are put forward with the aid of the error correction property of LDPC coding to embed the watermark information in the carrier image. Combing with certain methods such as compression and mapping, the encryption algorithm of the watermark is implemented. However, there are still some problems such as information distortion, transmission instability, and other issues in the process of algorithm implementation. LDPC code has good performance of error correction, which also can enhance the anti-jamming capability, but its concealment and imperceptible ability are equally important, and there are still some deficiencies in the algorithm.

This paper integrates the advantages and disadvantages of all kinds of encryption algorithms, and on the basis of LDPC coding, which makes some improvements. Chaotic processing is performed on the encrypted signals to achieve double encryption of information. The processing

ensures the privacy and imperceptibility, while reducing the error rate and improving transmission speed.

2 Chaotic sequence encryption

2.1 The introduction of chaotic encryption

In 1989, Matthews published a new algorithm for chaos encryption [16]. In cryptography, chaos encryption and chaos system are more important topics. The characteristics of chaotic system include nonlinearity, randomness, and complexity, which provide a good precondition for encryption. The information in an image can be scrambled after obtaining a pseudo-random sequence, especially the key is added. So the process brings the good performance of cryptograph. This series make chaotic cryptograph a hot system, and there are many people conduct in deep research on it, which has injected fresh vitality into confidential communications.

The chaotic secure communication method is a process of encrypting image information though the chaotic sequence and the key together. Since the process adds the key, the encrypted signal is difficult to be deciphered. The key itself calculated by complex equation, and it cannot be simply derived from the plaintext, so the process is almost impossible to be decrypted under the premise of unknowing the key, which is showing a strong encryption. The hardware implementation of the chaotic encryption algorithm is relatively simple and feasible, and this cryptology system has also developed rapidly.

Chaotic sequence encryption belongs to a sequence cryptosystem. Its main part is the origin of this kind of chaotic sequence. Traditional sequence encryption methods generate chaotic sequences by means of shift register. The new algorithm generates the key sequence directly through chaotic systems which has better confidentiality. Using chaotic system to place the original pseudo-random sequence generator is hard to be deciphered. The specific block diagram is shown in Fig. 1.

The specific relationship in the above figure can be described as follows: the sequence generator is generated through the key stream, and the process of encryption and decryption needs to rely on the key stream to complete, which also can be converted to each other.

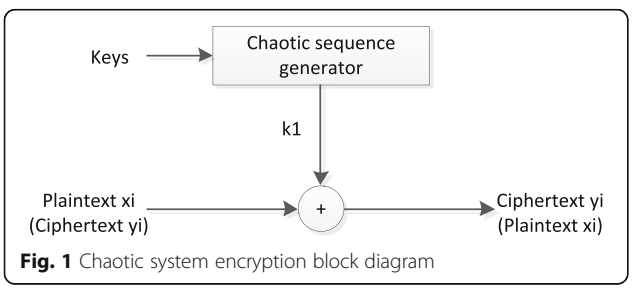

Fig. 1 Chaotic system encryption block diagram

The expressed as a. The formula can be expressed as the following:

Encryption process:

$$Y = X \oplus K \tag{1}$$

Decryption process:

$$X = Y \oplus K \tag{2}$$

In the above two processes, encryption or decryption is performed through an exclusive-OR operation, all of which require the participation of keys, where K represents a key that generates a chaotic sequence. This kind of chaotic encryption algorithm has good data confidentiality and controllability, so it is very practical and has been widely used.

2.2 Chaotic mapping system characteristics

Chaos is widespread in nature and has been studied by more and more scholars. In the process of research, people have discovered a lot of chaotic dynamic models, which are between theory and practice and also have very good representativeness. So it is also called chaotic dynamical system.

Chaotic model is divided into the following categories: discrete chaos model, continuous chaotic model, and so on [17]. Discrete chaos model mainly include Logistic, tent, Henon, and TD-ERCS mapping. Continuous chaotic models mainly include the Duffing oscillator, van der Pol oscillator, Lorenz system, Rossler system, Chua's circuit, Chen system, and united chaotic system.

Among them, logistic chaotic map is a kind of chaotic system which is widely used today. It is a kind of nonlinear system and is also the key system of our research. The logistic chaotic mapping has the following equation:

$$x_{n+1} = f(x_n) = \mu x_n(1-x_n) \tag{3}$$

In the formula, the value of each symbol presents the range of data as follows, $\mu \in (0, 4]$, $x_n \in (0, 1)$. Logistic chaotic mapping system Lyapunov exponent with the parameters of state is shown in the Fig. 2.

As can be seen from the diagram, when the map is in a chaotic state, in other words, the data of$\mu \in (3.5714, 4]$, the state is what we need in the encryption process, which is very suitable for encryption transmission.

The bifurcation diagram of the logistic chaotic mapping system with changes in parameters is shown in Fig. 3.

From the figure, we can see that the time series has experienced four transitions with the change of parameters. The four transitions include stable fixed point, unstable fixed point, period, and chaos. When the data requires$\mu = 4$, the system will become the most chaotic state.

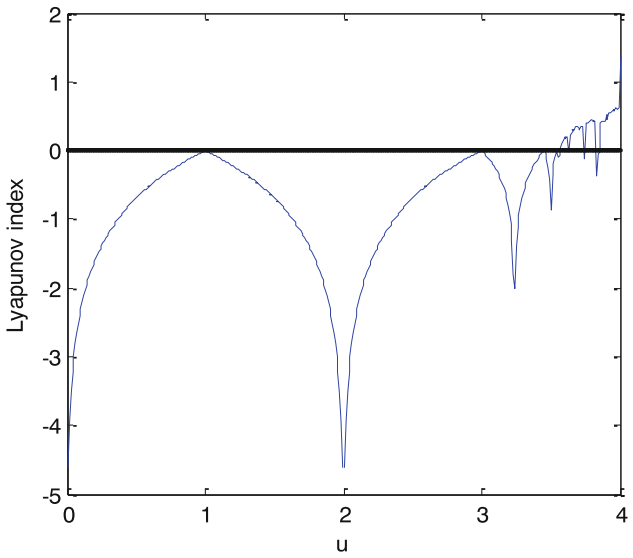

Fig. 2 Logistic map with parameter variation

From the above two diagrams, the final conclusion can also be drawn. When the parameters requireμ = 4, the logistic chaotic system reaches the most complex and the state of the chaos. At this time, the generated chaotic sequence has similar statistical characteristics to the white noise in communication system. It not only has good sensitivity to the initial value, but also has excellent aperiodicity. The generated information sequence is very reliable and safe which is a chaotic sequence that we need and use in our new algorithm.

2.3 Chaotic map encryption algorithm

Logistic map chaotic characteristics are used to generate chaotic sequence which has good aperiodicity and important applications in chaotic mapping algorithms. The sequence has a strong sense of numerical inception and the same statistical characteristics as white noise. The introduction of this sequence into digital watermarking has become a key component.

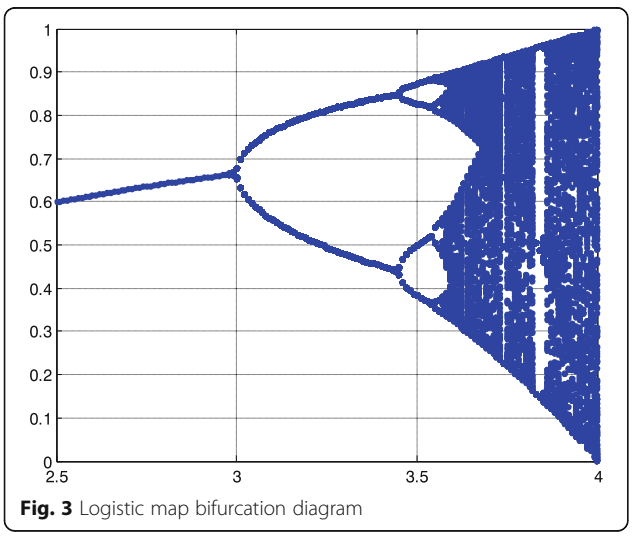

Fig. 3 Logistic map bifurcation diagram

The specific application of chaotic sequence in digital watermarking is manifested in two aspects: First, the digital watermarking information need to be operated by preprocessing before operation which mainly includes directly encrypting or scrambling the watermark information with the generated pseudo-random sequence. Second, select the embedding strength and coefficient in the process of watermark entry, etc.

Our main application is to preprocess the watermark information before the watermark is embedded. The advantage of this method is that the robustness and security are improved and it has stronger robustness after the watermark is preprocessed. Even if the information is stolen during transmission, it cannot be recovered easily after the information is scrambled, and meanwhile, the security of the system is extremely high.

Image scrambling is an important part of chaotic mapping encryption [18]. Its main function is to change the position of each pixel in the image, which can be called position scrambling. Another function is to change the gray value of pixel in the image, which can be called grayscale scrambling. Both of these methods hide the image information and render the image invisible. The image used in this paper is a binary image which has two pixel values that are 0 and 1. Therefore, we can adopt the method of grayscale scrambling.

3 The research method—application of LDPC code in hiding algorithm

3.1 The overview of LDPC code

LDPC code is a kind of linear block code, its function can be reflected through the check matrix (we also call it H matrix), and its most important feature is sparse [19]. The specific performance of the feature is that the internal elements are almost made of zero elements, in other words, the number of "1" in the elemental components is far less the number of "0." In the H matrix, the row weight refers to the number of "1" in each row, and the column weight refers to the number of "1" in each column. Due to the sparseness of the H matrix, the number of elements "1" in the matrix is particularly little, so the row weight and the column weight are very small numbers, and the number of overlaps of any two rows must be less than 1.

The LDPC code can be generally expressed as (n, r, g). The specific definition is that n represents the code length, r represents the line weight, and g represents the column weight. According to the size of relationship between r and g, the LDPC code can be classified two types. If they are equal, it is called regular code; if they are not equal, it is called irregular code [20].

In order to be able to achieve sparseness, the H matrix needs to meet the following conditions:

$$\begin{aligned} &r \geq 3, g > r, (N-K)g = Nr, \\ &\mathrm{r} \ll N-K, g = N \end{aligned} \tag{4}$$

where K represents the information bit and N represents a constant.

LDPC check matrix can also be expressed by a Tanner bidirectional graph. A node corresponding to each column element in the matrix is called a variable node, which also can be called information node. It is displayed as the following N nodes in the bidirectional graph, which can be specifically expressed as $\{x_j, j = 1, 2, \cdots N\}$. The node corresponding to each row element is called a check node, and it is displayed in the bidirectional graph as the above M nodes, which can be specifically represented as$\{x_i, i = 1, 2, \cdots M\}$. The next adjacent element corresponding to the "1" element in the matrix, which we call an adjacent node, is shown in the bidirectional graph as connected edges between two nodes. The number of connected edges around these nodes has a certain amount, which we call degree distribution.

For example, the parity check matrix and bidirectional graph of (10, 2, 4) LDPC codes are shown in Fig. 4.

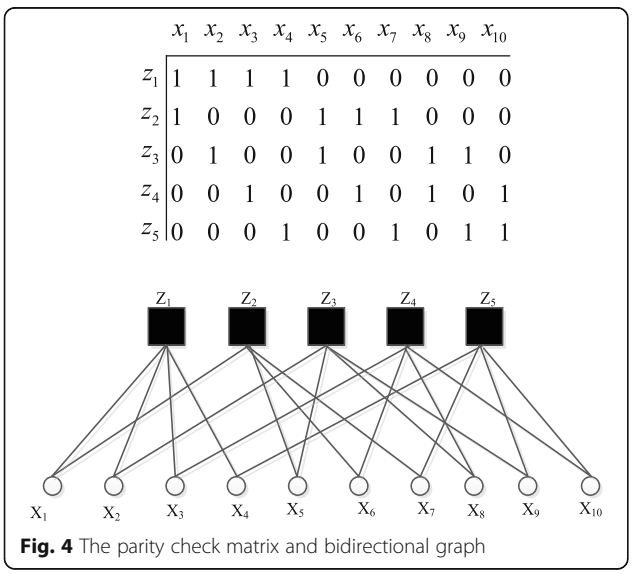

Fig. 4 The parity check matrix and bidirectional graph

3.2 The model of image digital watermark

Digital watermarking is an important technology for information confidentiality. Its basic idea is to embed a series of information that needs confidentiality into digital media through signal processing. During the process, the information cannot be easily found because of the blind spots of human vision and hearing, but it can be extracted from the digital media through an extraction algorithm. The operation realizes copyright protection and covert communication. Digital watermarking technology plays an important role in information security. Therefore, what we need to do is to ensure the robustness, security, and undetectability of digital watermarking.

The specific requirements of the digital watermark development process are as follows: there is no obvious change in the watermark before and after the image carrier is embedded; the watermark cannot be extracted by unauthorized person; the watermark operation process cannot destroy the original carrier. The process of digital

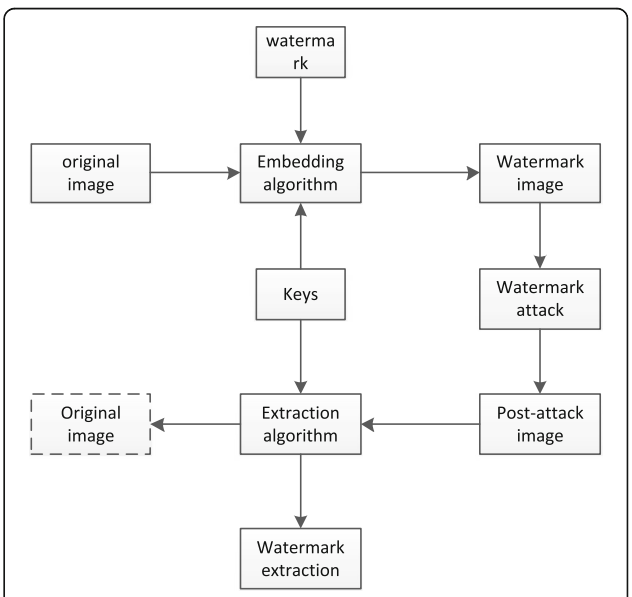

Fig. 5 Image watermarking model

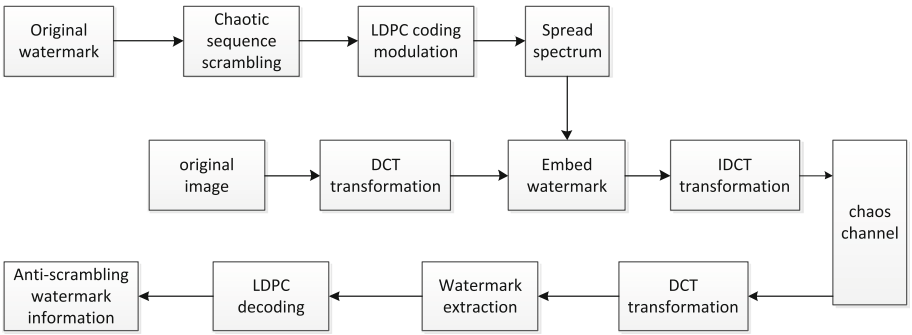

Fig. 6 Improved algorithm flow chart

watermarking encryption is very similar to the process of communication system. We can use the similarity of the two to obtain a preliminary watermark model. The specific process of image digital watermarking should include watermark embedding, attacks, watermark extraction, and detection steps [21]. The specific model is shown in Fig. 5.

The main consideration in watermark embedding is the choice of embedding domain. At present, the most popular choice is to embed in the discrete cosine transform (DCT) domain and DWT domain and to obtain the correlation coefficients of the watermark and the embedded image, respectively. It is necessary to ensure the unity between robustness and invisibility.

The watermark attack link mainly involves various damages to the carrier image during the transmission process, such as movement, geometry, password, and protocol attacks. Therefore, the most important point of the watermarking technology is to ensure the anti-interference ability of the entire system so that it can withstand various types of attacks.

Watermark extraction is the inverse process of embedding [22].

Watermark detection link is mainly to ensure that the watermark can safely reach the destination after operating transmission, and the relationship between the transmitted watermark and the original watermark is compared with the value of the size; according to the pipe between the two, it can be concluded how much the specific accuracy is. The basis of watermark detection includes the following two aspects:

First, the difference coefficient between the extracted watermark and the original watermark estimate.

$$\gamma = \frac{X \cdot X'}{\|X\| \cdot \|X'\|} = \frac{\sum_{i=1}^{N_x} x(i) \cdot x'(i)}{\sqrt{\sum_{i=1}^{N_x} x^2(i)} \sqrt{\sum_{i=1}^{N_x} x'^2(i)}} \tag{5}$$

In the formula, X and X' are the estimated values of the extracted new watermark and the original watermark, respectively. N represents the size of the watermark. When the coefficient size reaches a certain value, we believe that the watermark information achieves successful transmission.

Second, the important data is the bit error rate of the extracted watermark compared with the original watermark.

$$BER = \frac{1}{N_x} \sum_{i=1}^{N_x} x(i) \oplus x'(i) \tag{6}$$

For a binary watermark sequence, the value of the BER satisfies a certain limit to prove the presence of the watermark.

4 Improved encryption algorithm based on LDPC code and chaotic sequence

In order to enhance the accuracy and security, the LDPC code is introduced into the digital watermarking. The stability of the watermarking system can be enhanced through coding and modulation. At the same time, we are inspired by the chaotic encryption algorithm, so that the pseudo-random sequence with chaotic properties is used to operate scrambling processing watermark information. It is also an important choice for watermarking systems.

The new algorithm is proposed in this section. Firstly, a pseudo-random sequence of chaotic nature is

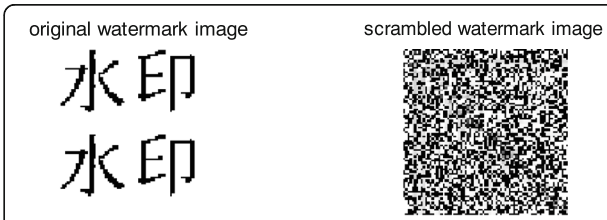

Fig. 7 watermark scrambling

Fig. 8 original image and watermarked image after embedding

generated in a logistic chaotic system. The digital watermark information is subjected to scrambling operation processing using grayscale scrambling preprocessing. Secondly, the watermark information is LDPC-coded and modulated. And then, the watermark information is embedded into the original image to achieve double encryption. The entire algorithm process improves the anti-jamming capability of the watermark encryption system and enhances the stability of the system.

The flow chart of the entire new algorithm can be represented by Fig. 6.

The specific algorithm steps in the above improved algorithm can be described as follows:

1. The chaos characteristic of logistic system can generate a pseudo-random sequence with chaos. The gray-scale scrambling is used to preprocess the original watermark information, which makes the order of gray values inside the watermark information upset, and the watermark after scrambling has obvious invisibility. The whole process achieves one-level encryption of watermark information.
2. The LDPC encoding and BPSK modulation of the watermark information can be operated after scramble, which can perform error correction and error detection, reduce the bit error rate, achieve accurate transmission of watermark information and enhance the interference ability, and then carry out the spread spectrum processing. The watermark information is changed into a watermark sequence to be embedded, and the two-stage encryption process of the watermark information is realized.
3. Watermark embedding process: block processing is performed on the original host carrier, and discrete

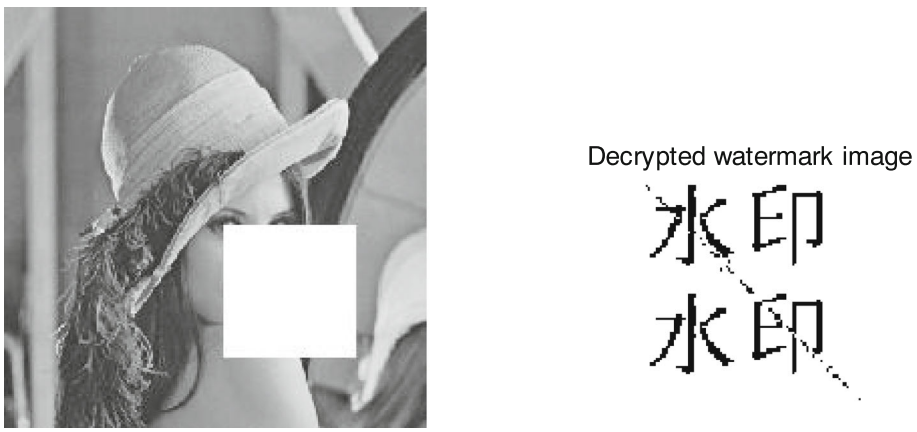

Fig. 9 cut attack and decryption watermark

Fig. 10 Image highlighting and decryption of the watermark

cosine transform (DCT) is performed on each block. According to the characteristics of human visual impairment, the watermark embedded in the intermediate frequency coefficient can be obtained and the watermark embedded operation can be completed. Among them, the DCT domain embedding formula is as follows:

$$\begin{cases} X = DCT(\tilde{X}) \\ X_i^{mz} = X_i^m(1 + aW), (0 \le i < K) \\ X = IDCT(\tilde{X}) \end{cases} \tag{7}$$

In the formula, $\tilde{X}$ indicates the decomposition layer coefficient, X indicates the DCT domain coefficient, X_i^{mz} indicates the maximum embedding amplitude of the watermark, and W indicates the pretreatment of the watermark sequence, a indicates the embedding strength.

4. Watermark extraction process is the inverse process of the embedded process. It is necessary to perform block DCT transform on the entire transmitted image and extract the watermark information from the intermediate frequency domain to complete the process.
5. After the watermark information is extracted, the extracted watermark is decoded by an iterative decoding process of the LDPC code, and then the anti-scrambling operation of the watermark is performed using the key to obtain the estimated watermark information.

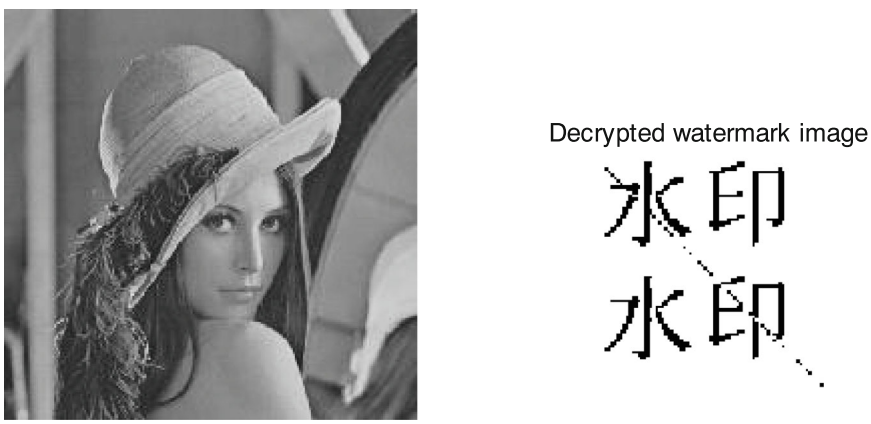

Fig. 11 Image darkening and decrypted watermark

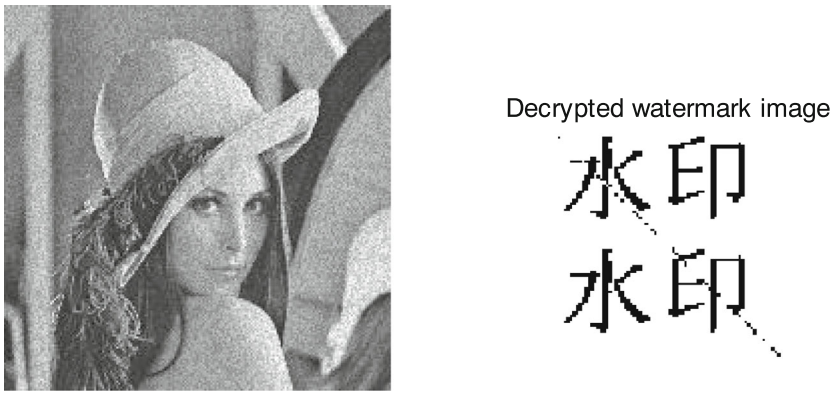

Fig. 12 Add product noise and decrypted watermark

The highlight of the entire algorithmic process is the double encryption of the watermark information, which combines the advantages of the two encryption algorithm. The whole system has good encryption, anti-jamming capability, and good robustness. The application of the proposed algorithm in the image encryption has a good implementation.

5 Analysis of simulation experiments results and discussions

5.1 Simulation diagram analysis

When the watermark information is embedded and extracted, the index parameters used are presented by the peak signal to noise ratio (PSNR). This parameter value can represent the quality of the watermark image, pass the size of the PSNR value, and reflect the invisibility of the watermark image. Usually, in order to ensure the normal concealment of the watermark, the PSNR value has a certain setting, which should be greater than 38 dB.

The PSNR calculation can be expressed as follows:

$$PSNR = 10\ \log \frac{M^2 g_{\max}^2}{\sum_{x=1}^{M}\sum_{y=1}^{M}\left[\hat{g}(x,y)-g(x,y)\right]^2} \tag{8}$$

In the formula, M^2represents the size of the watermark image, $g_{\max}$represents the maximum value of the image, $\hat{g}(x,y)$represents the image value after the watermark is embedded, and $g(x,y)$represents the original image value.

The original image used in this paper is a Lena black-and-white image, which is very typical. The LDPC code used has a code length of 1024 and a code rate of 1/2. In order to facilitate calculation and encoding, the Mackay construction method is the method of selection. The decoding algorithm uses a soft-decision decoding

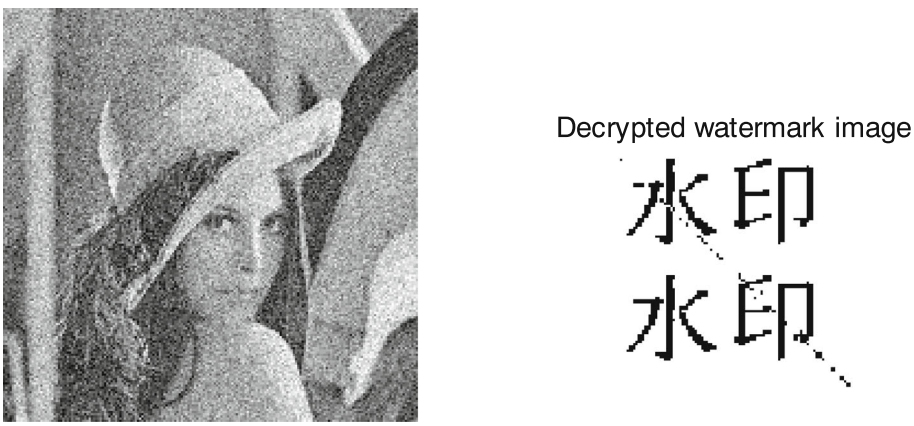

Fig. 13 Add Gaussian noise and decrypted watermark

Fig. 14 Histogram equalization attack and decrypted watermark

method with better performance advantages, and the maximum number of iterations is 1000, until the decoding is completed and the result appears.

Start the MATLAB simulation, and the resulting simulation diagrams for each stage are shown in the following series of image.

We can conclude from Fig. 7 which shows the simulation diagrams of the original watermark and the scrambled watermark. The original watermark is scrambled with the chaotic sequence. It can be seen from the above simulation diagrams that the effect of scrambling through the chaotic sequence encryption is very good. The watermark information has been changed beyond recognition. It can no longer be easily identified, and it achieves very good encryption processing.

We can conclude from the Fig. 8 that the watermark is scrambled and LDPC encoded and modulated; after that, the watermark information is embedded in the original image so that we can decrypt it with the encryption. The images are compared to verify the correctness of the algorithm simulation. It can be seen that the image after embedding the watermark is compared with the original image. In comparison, there is no visible change, and it is well concealed. The watermark information after scrambling is well hidden.

5.2 Attack test analysis

After the completion of encryption and embedding of watermark information, the process of image information transmission is required. In order to verify the robustness and encryption of the algorithm proposed in this paper, the attack information analysis of the image information embedded in the watermark information is performed to verify the excellent algorithm. By observing the correlation coefficient between the original watermark

Fig. 15 Rotate 45 rotation and decryption watermark

and the extracted watermark, we can infer the effectiveness of the attack experiment.

Here we will attack the watermark image separately from several different aspects. The simulation image obtained is shown in the following image.

1. Cut attack

The cut attack is mainly an attack processing that needs to directly cut the image. After the attack test, we can also get the correlation coefficient is 0.9551, and the specific simulation image is shown in the Fig. 9.

2. Brightening and darkening attack

This is a pair of opposite processes, which mainly to change the brightness parameters of the image to test the robustness of the watermark information. After the attack test, we can obtain the coefficient. The brightening attack can obtain correlation coefficient is 0.9581; the darkening attack can obtain correlation coefficient is 0.9656. The specific simulation image is shown in the Figs. 10 and 11.

3. Add noise processing attack

The processing of adding noise is the closest approach to the communication system. Through noise attack, it can directly reflect whether the encryption system has excellent robustness. In the simulation, it mainly concludes product noise and Gaussian noise. After the attack test, we can obtain the coefficient respectively. The product noise can obtain a correlation coefficient of 0.9637; the Gaussian noise can obtain a correlation coefficient of 0.9601. The specific simulation image is shown in Figs. 12 and 13.

4. Histogram equalization attack

The attack refers to flattening the image's histogram to show a flat trend. It is a normalization process that can increase its contrast. The correlation coefficient is 0.9574. The specific simulation image is shown in Fig. 14.

5. Image rotation processing attack

The attack is mainly the stability of the test image in the transmission. The processing done here is a 45° test attack on the image rotation. The rotate 45 rotation has a correlation coefficient of 0.9478. The specific simulation image is shown in Fig. 15.

From the above Figs. 9 to 15 simulation images, it can be seen that the watermark which contains a carrier image does not show a huge loss. The image can still be clearly visible, and the correlation coefficient is very close to one. The specific image content and watermark information can be distinguished after deciphering. The information did not receive much destruction. The new algorithm proposed in this paper does improve the robustness of the system and make up for the insufficiency of the single-layer encryption algorithm, and has a very good implementation.

6 Conclusions

In this paper, a new algorithm is proposed for the robustness and invisibility of the transmission system. First, the chaotic sequence is used to scramble the watermark and break its internal arrangement. Second, the scrambled watermark information can be encoded and modulated by the LDPC code. Under the double encryption, the stability and confidentiality of the system have been effectively improved. Then the new algorithm is simulated by a MATLAB simulation software. The results indicate that the encrypted information image can still maintain the integrity of the original image information and watermark information after various attack experiments.

Abbreviations

DCT: Discrete cosine transform; LDPC: Low-density parity-check code; SVD: Singular value decomposition

Author details

Institute of science and technology for Opto-Electronics information, Yantai University, Yantai, China

Availability of data and materials

Data and materials are available upon a request from the authors.

About the authors

Zhongxun Wang was born in Yantai, Shongdong, 1964. He received the Ph.D. degree in Naval Aeronautical Engineering Institute, in 2009. His research interest is source channel coding in wireless communication. Meng Xiangcai, female, was born in 1992, a master degree candidate of Yantai University, and her research direction is application of LDPC coding in the filed image encryption.

Author's contributions

W is the first author, and M did some parts of the experiment. Both authors read and approved the final manuscript.

Ethics approval and consent to participate

Agreed.

Consent for publication

Agreed.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Received: 11 June 2018 Accepted: 10 September 2018
Published online: 21 September 2018

References

1. F. Ian, W.S. Akyildiz, Y. Sankarasubramaniam, et al., A survey on sensor networks. IEEE Commun. Mag. **40**(8), 102–114 (2002).
2. S. Myung, K. Yang, J. Kim, Quasi-cyclic LDPC codes for fast encoding. IEEE Transactions Information **51**(8), 1038–2901 (2005).
3. S. Li, H. Li, K. Li, in *2011 IEEE International Conference on Information Theory and Information Security*. Research of image watermark algorithm based on LDPC code and wavelet packet transform (2011), pp. 840–844 Moon T K. Error Correction Coding: Mathematical Methods and Algorithms [M]. Wiley-Interscience, 2005.
4. Y. Zhao, Y. Xiao, The necessary and sufficient condition of quasi-cyclic LPDC codes without girth four. IEICE Tansact Commun **92**(1), 306–309 (2009).
5. W. Xijin, L. Fan, in *2010 International Conference on Future Information Technology and Computing (FITC 2010)*. The application research of MD5 encryption algorithm in DCT digital watermarking (2010), pp. 182–184.
6. Y. Xiao, K. Kim, *Alternative good LDPC codes for DVB-S2[C]*, International Conference on Signal Proceeding (2008), pp. 1959–1962.
7. H. Xiao, A.H. Banihashemi, Improved progressive-edge-growth (PEG) construction of irregular LDPC codes. Commun Letters IEEE **8**(12), 715–717 (2004).
8. Y. Zhang, X. Chen, *Current status of color image watermark methods*, 2011 Chinese Control and Decision Conference(CCDDC) (2011), pp. 4074–4079.
9. M. Sipser, D. Spileman, Expander codes. IEEE Trans Inf Theory **42**(11), 1710–1722 (1996).
10. D.J.C. Mackay, S.T. Wilson, M.C. Davey, Comparison of constructions of irregular Gallager codes. IEEE Trans. Commun. **47**(10), 1449–1454 (1999).
11. R.G. Gallager, *Low-density parity check codes* (MIT Press, Cambridge, 1963).
12. Z. Chen, Z. Liang, Application of irregular LDPC code in digital watermarking. Comput Eng App, 154–160 (2010).
13. Y. Zhou, L. Zhou, Research of image watermark algorithm based on compressive sensing and LDPC. J Chinese Comput Syst, 215–219 (2011).
14. Z. Lu, G. Feng, Design of robust digital watermarking algorithm based on LDPC and image scrambling transformation. J Kunming Univ, 68–72 (2010).
15. Y. Kou, S. Lin, M.P.C. Fossorier, Low-density parity-check codes based on finite geometries: a rediscovery and new results. IEEE Trans. Inf. Theory **47**(7), 2711–2736 (2001).
16. M. Hénon, A two-dimensional mapping with a strange attractor. Commun. Math. Phys. **50**(1), 69–77 (1976).
17. A. Gautam, R. Gupta, Enhancement of steganography scheme based on QC-LDPC codes. Int Conf Signal Processing, 10–13 (2015).
18. N.M. Makbol, B.E. Khoo, T.H. Rassem, Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. Inst Eng Technol, 34–52 (2016).
19. T. Richardson, R. Urbanke, The capacity of low-density parity-check codes under message-passing decoding. IEEE Trans Inform Theory, 599–618 (2001).
20. Z.P. Shi, J. Tiffany Li, I.P. Zhongpei Zhang, Joint nonbinary LDPC code and modulation diversity over fading channels. J. Appl. Remote. Sens., 1–13 (2010).
21. S.T. Brink, G. Kramer, A. Ashikhmin, Design of low-density parity-check codes for modulation and detection. IEEE Trans Commun, 670–678 (2004).
22. N.M. Makbol, B.E. Khoo, Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. Int. J. Electron. **67**(2), 102–112 (2013).