IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 3, 2022, accepted January 31, 2022, date of publication April 11, 2022, date of current version April 15, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3166475

Digital Watermarking Technology Based on LDPC Code and Chaotic Sequence

ZHONG-XUN WANG, KAI-YUE SHA, AND XING-LONG GAO
Institute of Physics and Electronic Information, Yantai University, Yantai 264005, China
Corresponding author: Zhong-Xun Wang (ytdxwzx@163.com)

ABSTRACT The number of ways to obtain information has increased by 5th Generation Mobile Communication Technology commercial. But easier access to information also means more security issues. Digital watermarking is an effective method to solve the security problem of information. Aiming at the problems of one-dimensional single chaotic image encryption algorithm, such as simple structure, small key space, and the invisibility and robustness of traditional information hiding technology cannot be well reconciled. The improved encryption algorithm based on Low Density Parity Check Code and double Logistic chaotic system is proposed, which can expand the key space, reduce the bit error rate, and enhance the security and anti-interference ability of the system. The feasibility, reliability and practicability of the algorithm are verified by MATLAB simulation.

INDEX TERMS LDPC code, chaos encryption, digital watermark, information security.

I. INTRODUCTION

There is an old saying that "one coin has two sides". On the one hand, information digitization and high-speed development of Internet technology make people's life and communication more convenient and colorful. On the other hand, the accompanying security problems of digital image information also make people worried. In particular, with the rapid development of 5G (5th Generation Mobile Communication Technology) bringing convenience to people, problems such as illegal embezzlement of personal documents and software, copyright damage of digital multi-media works and even hacker attacks and illegal theft of business information also appear frequently. These problems remind us that image information security is a problem that must be paid attention to in the present and future long-term development, and the Re-search of its encryption algorithm is also very urgent and necessary.

In this paper, an improved encryption algorithm based on LDPC (Low Density Parity Check Code) code and Logistic chaotic encrypted twice is proposed to solve the problem that the robustness and security of current digital watermarking technology are not perfect. Through MATLAB simulation, it is compared with single chaos encryption algorithm[1] and traditional watermark algorithm in many aspects, which shows that the improved algorithm can enhance stability, anti-interference and security, and well balance the problem of robustness and watermark invisibility.

II. LDPC CODE AND LOGISTIC CHAOS

In this section, we will introduce the basic concept of LDPC code and the overview of logistic chaos.

A. THE BASIC CONCEPT OF LDPC CODE

The transmission of signals in communication is very complicated. Ya T U *et al.* proposed an electric signal recognition based on deep learning [2]. And for the channel transmission signal Yun Lin *et al.* proposed Adversarial Attacks in Modulation Recognition With Convolutional Neural Networks [3]. LDPC codes have excellent characteristics that can approach the Shannon limit. LDPC (Low Density Parity Check Codes) code [4] was first proposed by Gallager in 1963. After decades of continuous research, it has become the coding scheme of data channel in 5G technology. The most prominent ones are the Quasi-cyclic LDPC codes [5], [6] proposed by Myung *et al.* and the Optimization-based decoding algorithms for LDPC convolutional codes in communication systems [7] proposed by Banu *et al.* and the Comparison of constructions of irregular Gallager codes [8] proposed by Mackay *et al.* Compared with the length of the check matrix—**H**, there are a few non-zero number in its ranks, that is, the number of "0" is much more than the

The associate editor coordinating the review of this manuscript and approving it for publication was Jiankang Zhang.

number of "1", so it is also called low-density parity code, which is also based on this unique sparsity to construct its low complexity and high performance characteristics [9], [10]. It is also considered to be one of the most superior error correction codes based on the following ad-vantages:

1) Approximate Shannon limit, for example, irregular LDPC code (r=1/2), in binary input AWGN (Gaussian white noise channel), when the code length is 107, the difference between the distribution of times and Shannon limit is only 0.0045dB [11];
2) Parallel decoding operation and simple implementation;
3) The minimum distance is proportional to the code length;
4) Low error platform;
5) It can detect decoding errors with low error rate.

B. OVERVIEW OF LOGISTIC CHAOS

Chaos is ubiquitous in nature, which can be attributed to the random and irregular motion in a certain system. Chaos is generated by the deterministic equation, which is characterized by extreme sensitivity to the initial value (the minimum difference of the initial value will result in different chaotic orbits), inherent randomness, ergodicity, etc. Ac-cording to the continuity of time, chaotic system can be divided into continuous chaotic system (such as Lorenz system) and discrete chaotic system, such as Logistic system [12].

Although the model of Logistic chaotic system has a single form, it is one of the commonly used chaotic systems. Generally speaking, the iteration is also called logistic mapping. Its one-dimensional mapping definition formula:

$$x_{n+1} = \mu x_n(1 - x_n) \quad n = 1, 2, 3 \cdots \tag{1}$$

System control parameters $\mu \in (0, 4]$, state variable $x_n \in (0, 1)$, n is the number of iterations. When μ increases gradually, the period of system iteration increases slowly. When μ is closer to 4, the value of X is closer to the average distribution in the range of [0, 1]. At this time, the chaotic sequence has the statistical characteristics similar to the white noise - the initial value is extremely sensitive and very good aperiodicity. By using this feature, the initial condition of mapping is regarded as a key, which can improve the security. The mapping bifurcation is as follows: The Lyapunov exponent graph of Logistic mapping is shown in Figure 2:

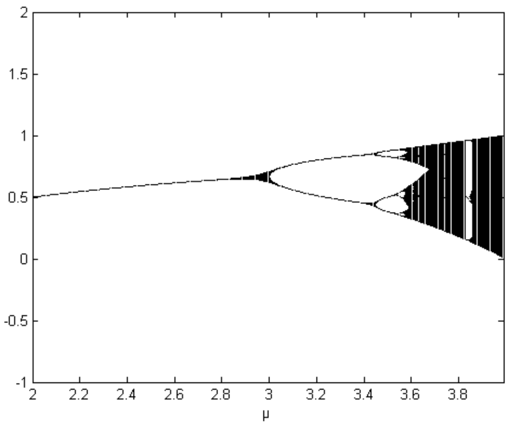

FIGURE 1. Bifurcation diagram of logistic map.

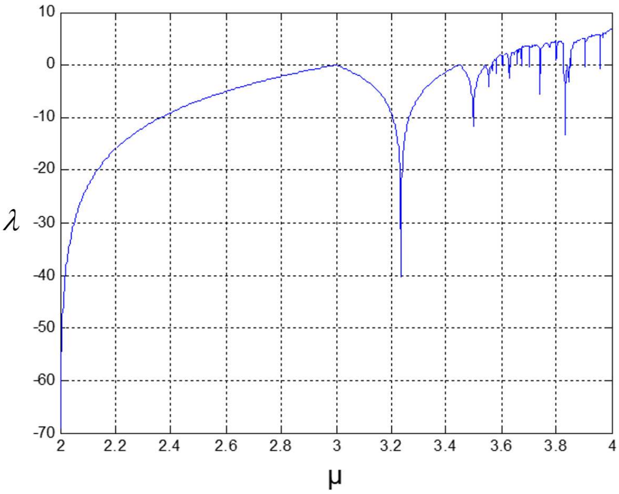

FIGURE 2. The Lyapunov exponent graph of logistic mapping.

From Figure 2, when μ=4, the Lyapunov exponent is positive and the value reaches 0.69, when the complexity of the system is the largest.

The main methods of using Logistic system to generate chaos are:

1) Set the initial condition μ and initial value for the Logistic chaotic system, and perform real-value sampling on the generated trajectory to form a real-valued chaotic sequence.
2) On the basis of generating real-valued chaotic sequence, quantization is performed, such as equations (2) and (3), to obtain a binary sequence with chaotic properties.

$$sign(x_i) = \begin{cases} 0 & 0 \le x_n < 0.5 \\ 1 & 0.5 \le x_n \le 1 \end{cases} \tag{2}$$

$$sign(x_i) = \begin{cases} -1 & 0 \le x_n < 0.5 \\ 1 & 0.5 \le x_n \le 1 \end{cases} \tag{3}$$

On the basis of generating real-valued chaotic sequence $\{x_n, n = 1, 2, 3, 4, \cdots\}$, rewrite x_n into a floating point number of M_bit, that is, $|x_n| = a_0(x_n)a_1(x_n)\cdots a_i(x_n) \cdots a_{M-1}(x_n)$, where $a_i(x_n)$ is the i_{th} bit of x_n, and the resulting chaotic sequence is $a_i(x_n), i = 0, 1, 2, \cdots, M - 1; n = 1, 2, 3, \cdots$.

III. AN IMPROVED IMAGE ENCRYPTION ALGORITHM BASED ON LDPC CODE AND CHAOS

By virtue of the excellent error correction performance of LDPC code and the initial value sensitivity of logistic map, the algorithm of digital image encryption is improved by combining them with digital watermark. It is proposed to combine the creation of pseudo-random sequence with LDPC code by using two logistic codes. Through the coding and decoding of LDPC code, the security of information can be effectively enhanced and the anti-attack of watermark can be improved. Through the second-order chaos and the creation of sequence can enlarge the key space and enhance the security [13] The improved algorithm is mainly divided into two parts, one is the encryption of water-mark image, the other is the encryption of color carrier image. The specific steps are as follows:

1. Binary Logistic chaotic encryption of watermark image

Read the size of watermark image A-M1xN1, design the initial value of the first and second level logistic mapping, select the logistic image pixel value diffusion (substitution) algorithm, set the initial value of chaos $\mu_1 = 3.9889662245452165$, $\mu 2 = 3.9987653246512161$; x1= 0.2; x2= 0.7, and then get two chaotic sequences from the mapping formula. After the following formula, we can get the random sequences Y1 and Y2, and implement the original image Value instead of encryption to enhance its invisibility. At this time, the obtained watermark image is encrypted by two chaotic sequences.

$$y\left(i\right) = \left(1/3.1415926\right) \times asin\left(sqrt\left(x\left(i\right)\right)\right) \tag{4}$$

$$y(i) = \frac{1}{\pi} \times a\sin\sqrt{x(i)} \tag{5}$$

2. LDPC code modulation information

For the watermark image encrypted by chaos, the check matrix **H** is generated by LDPC coding principle, and then the generated matrix **G** is obtained by Gauss elimination method. Then, the symbol C is obtained by BPSK modulation, and then the coded watermark sequence $x_i = c_j p_i$ can be obtained by pseudo-random sequence spread-spectrum, where c_{j} represents the j-th element, and p_i represents the spread-spectrum factor.

3. Embedding watermark

The carrier image I is divided into blocks and each block is transformed by DCT. Due to the characteristics of information loss easily caused by the high frequency do-main in the DCT domain and the sensitivity of the human eye to the low frequency component, the DCT coefficient generally adopts the intermediate frequency coefficient on the carrier image. The formula is as follows:

$$f_i' = f_i(1+\alpha q_i x_i) = f_i(1+\alpha c_j q_i p_i),\ i = 1, 2, \cdots, \gamma \tag{6}$$

For the new integrated image, the DCT coefficients are calculated. f_i and f_i' are the coefficients of original image and embedded watermark, α represents the embedding strength ($\alpha > 0$), q_i represents the size of visual hiding matrix. After embedding the watermark, the inverse transform (IDCT transform) is applied to each block, and the carrier image I' containing the encrypted watermark can be obtained by combining these blocks. Formula for embedding watermark:

$$\begin{cases} X = DCT(\tilde{X}) \\ X_i^{mz} = X_i^{m}(1+\alpha W), \quad (0 \leq i \leq K) \\ X = IDCT(\tilde{X}) \end{cases} \tag{7}$$

4. Encryption of carrier image

The RGB three-layer hierarchical Logistic chaotic encryption is applied to the color carrier image. The initial value of chaos is set here, $\mu_3 = 3.9181689662245452$, $\mu_4 = 3.9975843215678916$; $x_1 = 0.3$; $x_2 = 0.6$. The principle of encryption is the same as that of watermark image, so we can get the carrier image with double encryption. In this way, even if the image is stolen in the process of transmission, we can still extract the watermark to confirm the copyright.

5. Decryption of carrier image and extraction of watermark

Decryption is also divided into two parts, the first is to decrypt the carrier image. The RGB layer of color carrier image is still layered, and then each layer is decrypted and recombined by chaos, then the clear carrier image with watermark can be obtained. The second part is to extract the carrier image with watermark, and then get the original watermark image after LDPC code decoding and the same Logistic chaotic sequence reconstruction and decryption.

Watermark extraction is about to block the image after embedding the watermark in the above process, and then recover the watermark $m\cdot$ by LDPC decoding after IDCT transformation. The formula is as follows:

$$r_j = \frac{1}{\gamma}\sum_i f_i' P_i,\ i = 1, 2, \cdots, \gamma \tag{8}$$

$$X(m,n) = \frac{2}{\sqrt{MN}}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} c(k)c(l)Y(k,l) \times \cos\frac{(2m+1)k\pi}{2M}\cos\frac{(2n+1)l\pi}{2N} \tag{9}$$

r_j is the watermark information extracted after decoding, f_i' is the DCT coefficient after embedding the watermark. When k, l= 0, the values of C (k) and C (l) are taken, otherwise, $1\Big/\sqrt{2}$ is taken.

Min-sum decoding algorithm can be adopted:

1) Initialization

$$Z_{n,m}^{a} = f_n^{a} = \ln\frac{p(x_n = a/y_n)}{p(x_n = 0/y_n)} \tag{10}$$

2) Check node update

$$L_{mn}^{a(k)} = \prod_{n' \in N(m)\backslash m} \operatorname{sgn}(Z_{mn'}^{a(k-1)}) \cdot \min_{n' \in N(m)\backslash m}\left|Z_{mn'}^{a(k-1)}\right| \tag{11}$$

3) Variable node update

$$Z_{mn}^{a(k)} = Z_n^{a(0)} + \sum_{m' \in M(m)\backslash m} L_{m'n}^{a(k)} \tag{12}$$

$$Z'^{a(k)}_{mn} = \begin{cases} (Z_{mn}^{a(k)} + Z_{mn}^{a(k-1)})/2 & \widehat{x}_i^{l} \neq \widehat{x}_i^{l-1} \\ Z_{mn}^{a(k)} & otherwise \end{cases} \tag{13}$$

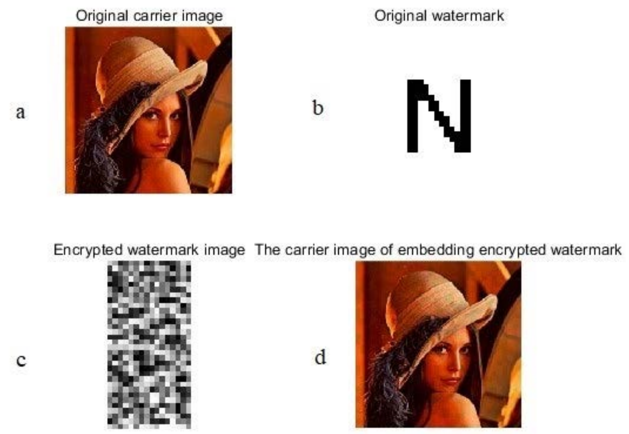
Original carrier image
Original watermark
a
b
Encrypted watermark image
The carrier image of embedding encrypted watermark
c
d

FIGURE 3. Simulation of embedding the encrypted watermark into the carrier image.

4) Decoding decision

$$Z_n^a = Z_n^a + \sum_{m\in M(m)} L_{mn}^a \qquad (14)$$

$$\widehat{x_n} = \arg\max Z_{an}^a(x_n) \qquad (15)$$

Finally, make the following decision on the estimated value x_n given by the codeword. For n=1, 2, $\cdots$, N, if $Z_n > 0$, then judge x_n=0, otherwise x_n=1.

If $H \cdot (x_n)^T = 0$ or the number of iterations exceeds the set maximum number of iterations, the iteration will be stopped, and $x_n(n = 1, 2, \cdots , N)$ will be output as the decoding result. Otherwise, continue to the next iteration.

IV. MATLAB SIMULATION EXPERIMENT AND ANALYSIS

A. SIMULATION RESULTS

Using the MATLAB software of 2018 version and the improved algorithm, experiment the color image of ‘‘lena256bm. BPM’’ with the size of 256 * 256, and set the LDPC code length n=512 and code rate $R = 1/2$. The embedding strength of watermark is a = 0.06; select BP decoding, and the results are shown in Figure:

As shown in Figure 3, after two-level chaotic encryption and LDPC code processing of watermark information, we can’t see the information of the original watermark image, and embedding the encrypted watermark information into the carrier image will not be captured by the human visual system, that is, the invisibility is very good; for the color carrier image, we can create two chaotic sequences to R, G and B layers of the image respectively After layered encryption, the encrypted carrier image is synthesized. As shown in Figure 5, the key information of the carrier image after two-level chaotic encryption processing is completely invisible and has good confidentiality. Similarly, layered decryption of the encrypted carrier image can restore it to Figure 6, which is no different from that before encryption, which proves that the algorithm has good feasibility. After decryption, the key information of the carrier image is completely invisible and has good confidentiality. As shown in Figure 6, the extracted watermark is the same as the original image.

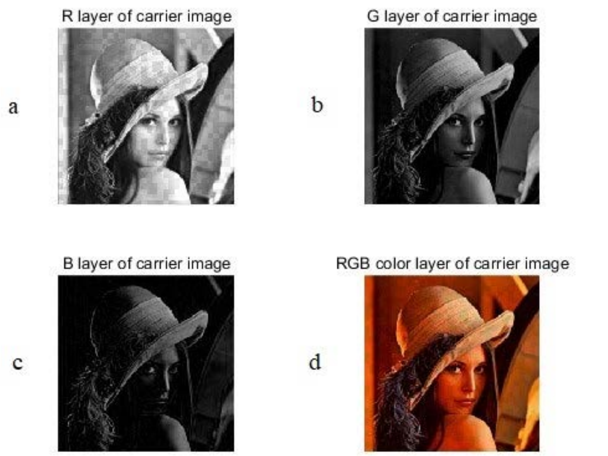

FIGURE 4. Layered simulation of color carrier image embedded with watermark.

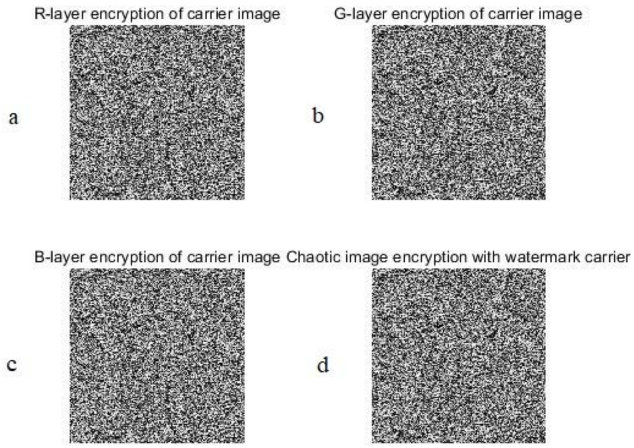
R-layer encryption of carrier image
G-layer encryption of carrier image
a
b
B-layer encryption of carrier image
Chaotic image encryption with watermark carrier
c
d

FIGURE 5. Simulation of layered chaotic encryption of carrier image.

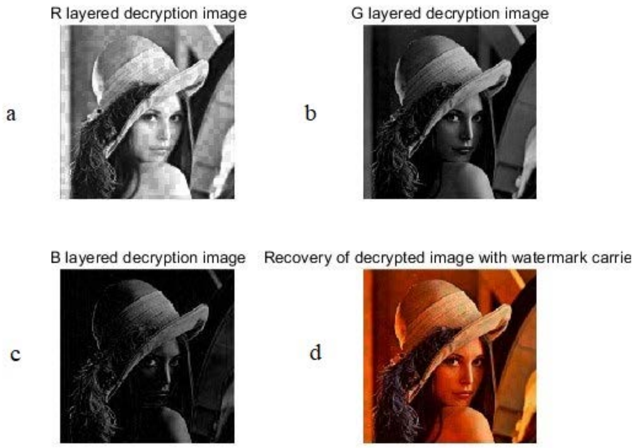
R layered decryption image
G layered decryption image
a
b
B layered decryption image
Recovery of decrypted image with watermark carrie
c
d

FIGURE 6. Recovery of carrier decryption with watermark.

B. HISTOGRAM ANALYSIS

Histogram is a basic statistical feature in digital image analysis, which belongs to the function of gray level. The horizontal and vertical coordinates respectively show the gray level and the number of pixels displayed in any gray level. For color image, we usually separate the three primary colors in the image first and then analyze the histogram separately. Before encryption, the histogram is disordered and uneven. At this time, the image information can be obtained by general analysis [14]. After encryption, if the gray value of the pixel is evenly distributed, it shows that the encryption effect of the algorithm is better, and it can effectively prevent the statistical analysis attack on the encrypted image. In turn, it indicates that the security is not high. Figure 3-9 shows the RGB three layers' histogram of original carrier, single chaos encryption and double encryption:

From the histogram simulation results and pixel contrast images of R, G and B layers of the original carrier image, single chaotic encryption and double encryption respectively, we can clearly see that the pixel distribution of the original carrier image is very irregular and fluctuates greatly. Compared with the original image, the pixel value set of each pixel in the single chaotic encryption carrier image tends to be flat, but still fluctuates. Compared with the former two, the double encrypted carrier image has the smallest amplitude difference, the histogram is smooth and close to the level [15]. It is proved that the encryption of the improved algorithm is very good.

C. EDGE OPERATOR ANALYSIS

Edge (edge) is one of the basic characteristics of an image. Generally speaking, it refers to the discontinuity of some characteristics of an image, such as the sudden change of color, gray level and structure. The basic idea of edge operator detection is to detect the edge points in the image first, and then connect these points to form the segmentation area [16].

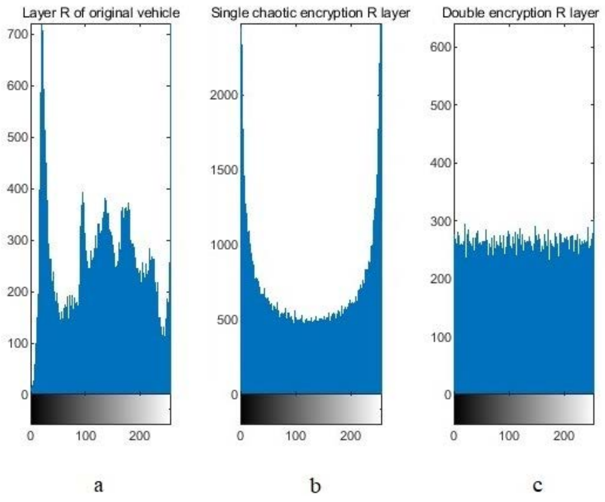

FIGURE 7. R-layer histogram of original carrier, single chaos encryption and double encryption.

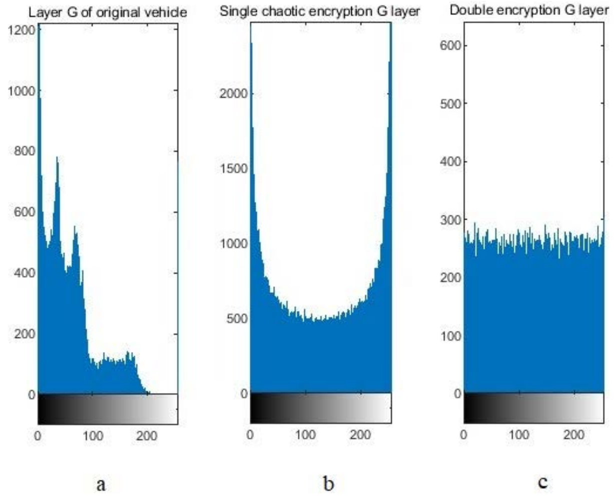

FIGURE 8. G-layer histogram of original carrier, single chaos encryption and double encryption.

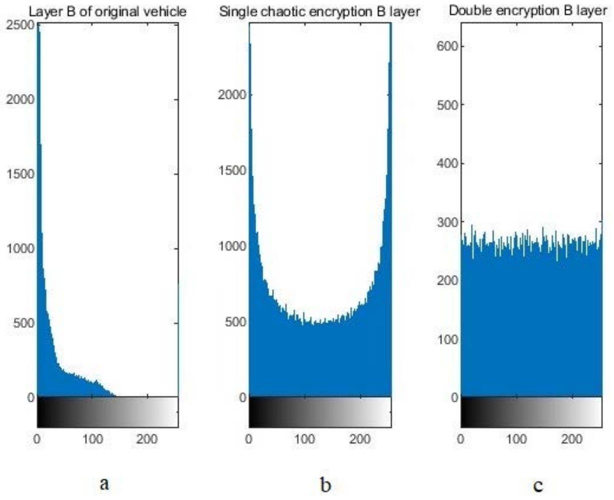

FIGURE 9. B-layer histogram of original carrier, single chaos.

Because the edge is the boundary between the target and the background, edge detection is very important for processing and analyzing image [17]. The application of sparse reconstruction algorithm also has better image effects [18].

Roberts operator is an operator that uses partial difference to search the edge. It calculates the difference between two adjacent pixels on the diagonal to check. It has high positioning accuracy, but it cannot eliminate the interference of noise. Laplacian operator uses the second derivative information to detect the edge according to the sharp zero crossing point generated at the edge, which is isotropic [19].

According to the above figures 10, 11 and 12, the Roberts operator and Laplacian operator of the original image, the embedded watermark and the double encrypted image processed by watermark and chaotic sequence are analyzed and compared as a whole. It can be seen intuitively that the edge of the original image and the image only embedded watermark can be captured by the human eye, while the edge operator of the image after double encryption cannot be extracted

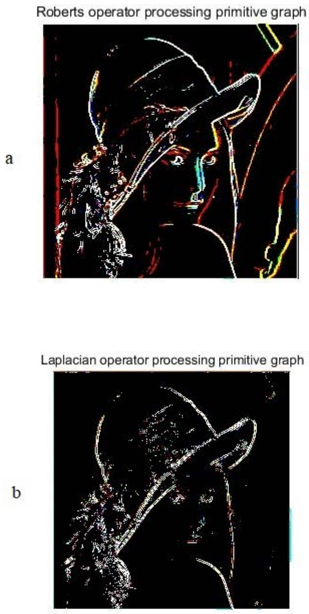
Roberts operator processing primitive graph
a
Laplacian operator processing primitive graph
b

FIGURE 10. Detection results of Roberts and Laplacian operators on the original image.

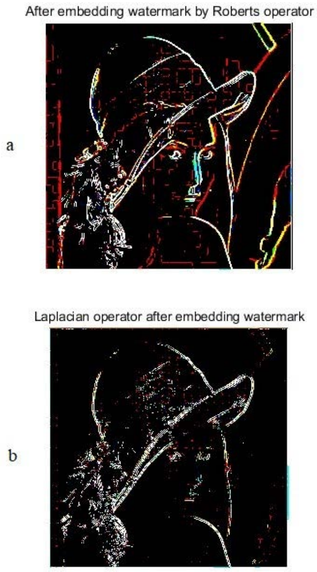
After embedding watermark by Roberts operator
a
Laplacian operator after embedding watermark
b

FIGURE 11. Detection results of embedded watermark by Roberts and Laplacian operators.

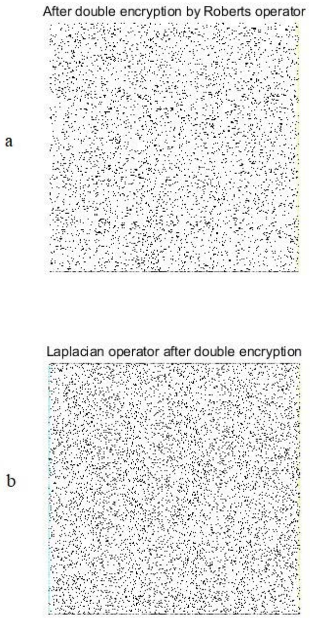
After double encryption by Roberts operator
a
Laplacian operator after double encryption
b

FIGURE 12. Detection results of double encryption by Roberts and Laplacian operators.

basically It has obvious edge features, cannot see the information of the original image, and has good confidentiality.

D. CORRELATION ANALYSIS OF ADJACENT PIXELS

Generally, the correlation of image is very high, close to 1, and the correlation will be cracked to a certain extent after image encryption [20]. Therefore, the smaller the correlation after encryption, the better the encryption of the algorithm, and the stronger the anti-attack of statistical analysis. As shown in Figure 13, the R, G and B-level histogram similarity of the original image and the watermark carrier image after embedding encryption is compared [21]. As shown in Figure 14, the correlation between the original image and the watermark carrier image after embedding encryption is close to 1, while the correlation between the watermark carrier image after double encryption is significantly reduced, indicating the improved algorithm [22]. It can better destroy the correlation of the image to be encrypted and make the encrypted image have good random distribution characteristics.

E. KEY SPACE AND RATE ANALYSIS

The value of the control variable in the chaos equation is not unique. Because the improved algorithm is double chaos encryption, the key space is larger. The four key values needed in this algorithm are ($\mu_1 = 3.9889662245452165$, $\mu_2 = 3.9987653246512161$, $\mu_3 = 3.918168966224552$, $\mu_4 = 3.9975843215678916$), the accuracy is accurate to 16 decimal places, then the key space of the improved algorithm is $10^{16}10^{16}10^{16}10^{16} = 10^{64} \approx 2^{213}$ is equivalent to 213bit of key space. According to literature [23], Alvarez pointed out that the key space must have 2^{100} to meet the required security level and be able to resist exhaustive attacks. Compared with the single chaotic system, the key space is less than 100bit. The improved algorithm provides enough key space. Using the error keys $\mu_{31} = 3.9181689662245456$, $\mu_{11} = 3.9889662245452166$ to decrypt the carrier image and extract the watermark, the results are shown in Figure 15. It is proved that although the experimental key is only one digit different from the correct key, the original image cannot be obtained, and the confidentiality and key sensitivity are very good.

The execution time of image encryption algorithm is usually used to test the processing speed and judge

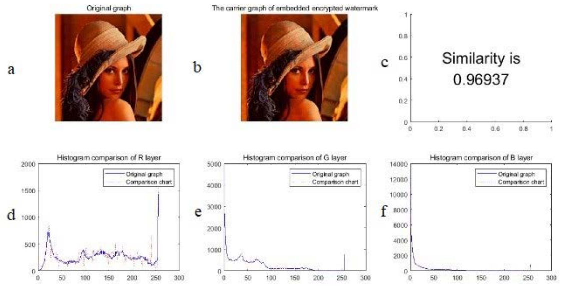

FIGURE 13. comparison of histogram similarity between the original image and the watermark carrier image after embedding encryption.

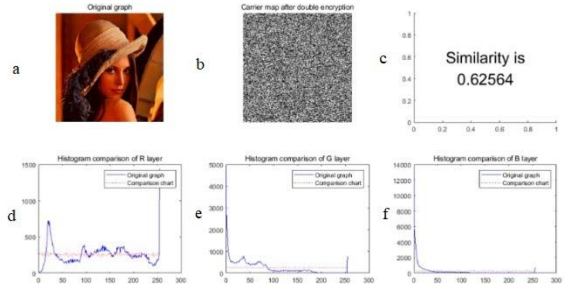

FIGURE 14. Comparison of hierarchical histogram similarity between original image and double encrypted carrier image.

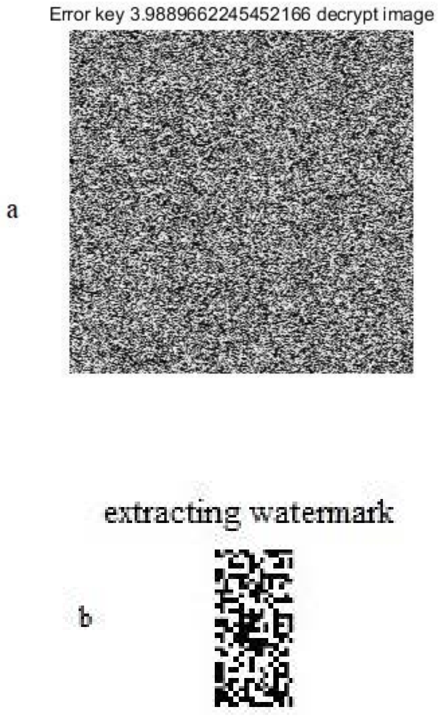

FIGURE 15. Error key decrypting carrier image and extracting watermark.

TABLE 1. Comparison Of encryption rates.

algorithm Time / s	Double encryption	Monochaos	Literature [25]	Literature [24]	Literature [23]
256*256	7.378	1.887	1.5367	2.7097	23.9254
512*512	8.608	2.063	2.6639	7.7548	105.3052
1024*1024	18.953	4.629	10.4278	27.9592	456.1276

TABLE 2. Comparison of double encryption algorithm and carrier image of each ALGORITHM R, G, B component.

Comparison of algorithms		R component	G component	B component
Monochaos	NPCR	99.64%	99.29%	98.70%
	UACI	33.47%	33.31%	33.49%
Double encryption	NPCR	99.60%	99.60%	99.60%
	UACI	33.36%	33.40%	33.37%
Literature [27]	NPCR	99.61%	99.61%	99.61%
	UACI	33.46%	33.46%	33.46%
Literature [26]	NPCR	99.69%	99.68%	99.67%
	UACI	33.54%	33.53%	33.51%

the performance. Take the average value of the proposed algorithm, single hybrid algorithm and other classical algorithms for 10 times respectively, and compare the rate to get the double encryption 4.546s, decryption 2.832s and total time 7.378s of the image with the size of table 1256 * 256. Then through the encryption of the image with different sizes, we find the double encryption proposed with the increase of image size, the operation speed of the secret algorithm is improved. Compared with the algorithm speed of the reference, it is found that the execution speed of each size image is better than that of the reference [24], but the execution speed of 256 * 256 and 512 * 512 size image needs to be improved compared with the reference [25].

F. ANTI DIFFERENTIAL ATTACK ANALYSIS

There are two standards to evaluate the anti-differential attack ability of image encryption algorithm, NPCR and uaci, which calculate the percentage of different pixels in two images and the average strength of the difference. An ideal encryption algorithm is known, NPCR and uaci should fluctuate up and down at 0.996 and 0.334 respectively. We calculated the R, G and B components of the carrier image of the dual encryption algorithm and the single chaos algorithm respectively, and compared them with the relevant values in the references. The data is shown in Table 2 below:

From the results of the above table, it can be seen that although the algorithm in reference [26], [27], the data of single chaos and double encryption carrier image are close to the theoretical value under ideal conditions, the fluctuation of the proposed double encryption algorithm is significantly smaller, the fluctuation value is less than or equal to 0.0004, and it is more sensitive to the subtle changes of image, which proves that the improved algorithm has strong resistance to differential attack.

V. SUMMARY

Through the MATLAB simulation results and analysis, we can see that the improved algorithm can expand the key space, well balance the invisibility, capacity and robustness, good encryption; in the actual picture transmission application, if the encryption of the carrier image is cracked or illegally stolen, the watermark can still be extracted for copyright protection, which is the same as double insurance of the carrier image. However, in the continuous research and experiments, many shortcomings have been found. For example, the logistic system is only limited to one dimension, and the high dimension chaotic mapping algorithm is not involved; in the simulation running experiment, compared with the encryption algorithm based on LDPC code and single chaos, the speed needs to be improved, which is also the direction to be improved in the future.

REFERENCES

[1] J. Zhu and B. Du, "Image encryption algorithm based on chaos and its implementation on FPGA," *J. Inf. Hiding Multimedia Signal Process.*, vol. 10, no. 2, pp. 278–288, Mar. 2019.

[2] Y. Tu, Y. Lin, H. Zha, J. Zhang, Y. Wang, G. Gui, and S. Mao, "Large-scale real-world radio signal recognition with deep learning," *Chin. J. Aeronaut.*, Oct. 2021.

[3] Y. Lin, H. Zhao, X. Ma, Y. Tu, and M. Wang, "Adversarial attacks in modulation recognition with convolutional neural networks," *IEEE Trans. Rel.*, vol. 70, no. 1, pp. 389–401, Mar. 2021.

[4] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inf. Theory*, vol. 8, no. 1, pp. 21–28, Jan. 1962.

[5] S. Myung, K. Yang, and J. Kim, "Quasi-cyclic LDPC codes for fast encoding," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2894–2901, Aug. 2005.

[6] B. Karimi and A. H. Banihashemi, "Construction of irregular protograph-based QC-LDPC codes with low error floor," *IEEE Trans. Commun.*, vol. 69, no. 1, pp. 3–18, Jan. 2021.

[7] B. Kabakulak, Z. C. Taşkın, and A. E. Pusane, "Optimization–based decoding algorithms for LDPC convolutional codes in communication systems," *IISE Trans.*, vol. 51, no. 10, pp. 1061–1074, Oct. 2019.

[8] D. J. C. MacKay, S. T. Wilson, and M. C. Davey, "Comparison of constructions of irregular Gallager codes," *IEEE Trans. Commun.*, vol. 47, no. 10, pp. 1449–1454, Oct. 1999.

[9] C. Marrocco and F. Tortorella, "Exploiting coding theory for classification: An LDPC-based strategy for multiclass-to-binary decomposition," *Inf. Sci.*, vol. 357, pp. 88–107, Aug. 2016.

[10] H. Wymeersch, H. Steendam, and M. Moeneclaey, "Log-domain decoding of LDPC codes over GF(q)," in *Proc. IEEE Int. Conf. Commun.*, vol. 2, Jun. 2004, pp. 772–776.

[11] I. E. Bocharova, B. D. Kudryashov, V. Skachek, and Y. Yakimenka, "BP-LED decoding algorithm for LDPC codes over AWGN channels," *IEEE Trans. Inf. Theory*, vol. 65, no. 3, pp. 1677–1693, Mar. 2019.

[12] C. Han, "An image encryption algorithm based on modified logistic chaotic map," *Optik*, vol. 181, pp. 779–785, Mar. 2019.

[13] X. Huang, M. P. Nia, and Q. Ding, "Research on image encryption based on hyperchaotic system," *J. Netw. Intell.*, vol. 5, no. 1, pp. 10–22, Feb. 2020.

[14] M. Veni and T. Meyyappan, "Digital image watermark embedding and extraction using oppositional fruit fly algorithm," *Multimedia Tools Appl.*, vol. 78, no. 19, pp. 27491–27510, Oct. 2019.

[15] P. Ayubi, M. J. Barani, M. Y. Valandar, B. Y. Irani, and R. S. M. Sadigh, "A new chaotic complex map for robust video watermarking," *Artif. Intell. Rev.*, vol. 54, no. 2, pp. 1237–1280, Feb. 2021.

[16] E. L. Lydia, J. S. Raj, R. P. Selvam, M. Elhoseny, and K. Shankar, "Application of discrete transforms with selective coefficients for blind image watermarking," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 2, Feb. 2021, Art. no. e3771.

[17] S. Li, H. Li, and K. Li, "Research of image watermark algorithm based on LDPC code and wavelet packet transform," in *Proc. IEEE Int. Conf. Inf. Theory Inf. Secur.*, 2011, pp. 840–844.

[18] W. Qidi, L. Yibing, L. Yun, and Y. Xiaodong, "The nonlocal sparse reconstruction algorithm by similarity measurement with shearlet feature vector," *Math. Problems Eng.*, vol. 2014, pp. 1–8, Mar. 2014.

[19] B. Wang, F. C. Zou, and Y. Zhang, "New memritive chaotic system and the application in digital watermark," *Optik*, vol. 172, pp. 873–878, Nov. 2018.

[20] D. G. Savakar and A. Ghuli, "Robust invisible digital image watermarking using hybrid scheme," *Arabian J. Sci. Eng.*, vol. 44, no. 4, pp. 3995–4008, Apr. 2019.

[21] Q. Wu, Y. Li, Y. Lin, and R. Zhou, "Weighted sparse image classification based on low rank representation," *Comput., Mater. Continua*, vol. 56, no. 1, pp. 91–105, 2018.

[22] Q. Wu, Y. Li, and Y. Lin, "The application of nonlocal total variation in image denoising for mobile transmission," *Multimedia Tools Appl.*, vol. 76, no. 16, pp. 17179–17191, 2017.

[23] G. Alvarez and S. Li, "Cryptographic requirements for chaotic secure communications," 2003, *arXiv: nlin/0311039*.

[24] Y. Wu, J. P. Noonan, G. Yang, and H. Jin, "Image encryption using the two-dimensional logistic chaotic map," *Proc. SPIE*, vol. 21, no. 1, 2012, Art. no. 013014.

[25] M. Y. Valandar, M. J. Barani, and P. Ayubi, "A fast color image encryption technique based on three dimensional chaotic map," *Optik*, vol. 193, Sep. 2019, Art. no. 162921.

[26] M. Mollaeefar, A. Sharif, and M. Nazari, "A novel encryption scheme for colored image based on high level chaotic maps," *Multimed. Tools Appl.*, vol. 76, no. 1, pp. 607–629, Jan. 2017.

[27] X. Wu, D. Wang, J. Kurths, and H. Kan, "A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system," *Inf. Sci.*, vols. 349–350, pp. 137–153, Jul. 2016.

ZHONG-XUN WANG was born in Yantai, Shandong, in 1964. He received the Ph.D. degree from the Naval Aeronautical Engineering Institute, in 2009. His research interest includes source channel coding in wireless communications.

KAI-YUE SHA was born in 1995. She is currently pursuing the master's degree with Yantai University. Her research interest includes LDPC codes.

XING-LONG GAO is currently the Laboratory Manager with Yantai University, who has an in-depth study of LDPC codes and the Internet of Things in WSN fields.