International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com || Volume 07 - Issue 10 || October 2021 || PP. 18-30

Reliable Encoding and Decoding Algorithm of Sparse Lattice Information Based on the Printing-quantum-dots Image

Wang Yujun[1], Cao Peng[2]
[1,2](*Beijing Key Laboratory of Signal and Information Processing for High-end Printing Equipment, Beijing Institute of Graphic Communication, Beijing, China)*

Abstract: When sparse dot-matrix image of halftone dots (printing-quantum-dots image) is used to realize information recording, information hiding, and information anti-counterfeiting, there is a problem of high bit error rate caused by the stain of printed information and the misjudgment of read information. In this paper, a reliable encoding and decoding algorithm of sparse lattice information based on printing-quantum-dots image is proposed. The encoding algorithm use a combination of information encryption, Low-Density-Parity-Check (LDPC) encoding, interleaved encoding and frame synchronization encoding, generating the printing-quantum-dots image. The decoding algorithm is the inverse process of the encoding algorithm, and can partially intercept the printing-quantum-dots image for reading. From the experimental results, it can be concluded that the combined coding scheme has better error-correcting ability and imperceptibility, the SSIM of before and after embedding reaches above 0.99, and the PSNR reaches above 54dB. Moreover, it can extract the printing-quantum-dots from the cover image, and read the hidden information. Besides, compared to BCH code, and convolutional code, it has high coding efficiency, prominent coding efficiency, as well as faster decoding speed.
Keywords: Dot-matrix image, Halftone dots, Information anti-counterfeiting, Information hiding, Reliable encoding and decoding

1. INTRODUCTION

Printing-quantum-dots refers to a non-separable printing imaging unit, usually a single halftone dot [1,2], used to record information in the field of printing information security. In recent years, the technology of information recording and hiding by using the sparse dot matrix characteristics of halftone dots is a new information anti-counterfeiting and encryption technology, which has become a research hotspot and application issue. However, the size of dot-matrix image unit is usually less than 40-60μm, there is usually bit error in recording and transmitting information through it, so it encounters a bottleneck in application and promotion. Channel coding can be used to detect and correct the noise in the transmission channel, help the information resist interference and improve the robustness of the system. Therefore, it is a good direction to apply channel coding technology to information anti-counterfeiting.

In recent years, the application of reliable coding technology to information hiding has been highly valued in the field of information anti-counterfeiting at home and abroad, and is generally regarded as a significant development direction. The research results mainly include the following aspects:

(1) Channel coding is used for reversible data hiding (RDH) to improve data embedding capacity and efficiency. Kim et al. [3] proposed a large capacity separable reversible data hiding in the encrypted image (SRDHEI) based on Hamming code, which can achieve high embedding efficiency under the condition of low distortion. A high-capacity partially reversible data hiding method based on Hamming code (PRDH) is proposed in reference [4], the embedding rate is 10.5 times that of PRDH in reference [5] and [6], and 3.5 times that of PRDH in reference [6]. Sun et al. [7] used Hamming code to design a reversible data hiding (RDH) method based on matrix embedding, which can achieve a high embedding capacity with low distortion. According to the minimum mean square error criterion between Hamming code and the bits of the original image, Wu et al. [8] proposed a general method of partially reversible data hiding (PRDH), which has good embedding capacity and visual performance. Kapse et al. [9] reviewed the methods of reversible data hiding in the encrypted image (RDHEI), one of which is to apply BCH code to improve the efficiency of data embedding.

(2) Channel coding is used to improve the robustness of data hiding. Liu et al. [10] used BCH code to encode embedded data to improve the robustness and visual quality of data hiding. Usman et al. [11] applied spread spectrum and BCH code to enhance the robustness of the watermark. Mstafa et al. [12] proposed a novel video steganography method in DCT domain based on Hamming and BCH code, which uses channel coding to encode secret message and improve robustness.

(3) The combination of channel coding and encryption algorithm improves the security of information hiding and the robustness of the algorithm. Reference [13] combined chaotic encryption technology and BCH code to improve the security and robustness of the algorithm. Reference [14] used chaotic sequence and LDPC code to encrypt the watermark, which improves the stability and security of the watermark system. In reference

[15], the cryptographic SHA-256 hash and BCH code are applied to the reversible watermark in encrypted images, and the secret data and cover image can still be recovered in the presence of noise attack. Reference [16] used (15,11) Hamming code and error diffusion to embed information in 4×4pixel blocks, which has a high data embedding ability.

LDPC code is a powerful block error-correcting code, which can reach the theoretical capacity limit and has error-correcting ability [17,18,19]. Because of its excellent performance, this paper proposes an information hiding algorithm based on LDPC code. The algorithm uses information encryption, LDPC coding, interlacing coding and frame synchronization coding to encode the hidden information reliably, and then obtains the printing-quantum-dots image by information modulation. The existence of frame synchronization information makes it possible to partially intercept the printing-quantum-dots image and completely read the plaintext. The experimental results show that the algorithm has achieved good results in information hiding and information anti-counterfeiting.

The rest of the paper is organized as follows. Second 2 introduces necessary background of the proposed algorithm, including the encoding and decoding of LDPC code, and channel noise model. Section 3 describes the proposed scheme in detail, including information hiding and information reading of printing-quantum-dots. The experimental results are presented in Section4, while includes the generation and reading results of the printing-quantum-dot image, the error detection and correction ability, imperceptibility, and the test of hiding printing-quantum-dots in the blue channel of the cover, and compares the algorithm with other algorithms. Finally, Section 5 concludes this paper.

2. RELATED WORKS

2.1LDPC code

LDPC code was first proposed by Gallager [17]. It is a linear block code with a low-density check matrix. The sparsity of check matrix is used to solve the decoding problem of long code and realize the decoding of linear complexity. The characteristic of LDPC code is sparse, the specific performance is that the number of "0" in the check matrix $\boldsymbol{H}$ is far more than the number of "1" [20,21]. LDPC code can generally be expressed as (N, K, j, k), then the size of the $\boldsymbol{H}$ matrix is (N-K)×N, and the code rate is R=K/N. The specific definition is that N is the code length, K is the information bit, j is the column weight, and k is the row weight. In the $\boldsymbol{H}$ matrix, row weight refers to the number of "1" in each row, and column weight refers to the number of "1" in each column. According to the size relationship between j and k, LDPC code can be classified two types. If they are equal, it is called regular LDPC code; if they are not equal, it is called irregular LDPC code [22]. To achieve sparseness, the $\boldsymbol{H}$ matrix needs to meet the following conditions:

$$\begin{aligned} &j \geq 3, k > j, (N-K)\cdot k = N \cdot j \\ &j < N-K, k < N \end{aligned} \tag{1}$$

2.1.1 Encoding

The parity check matrix $\boldsymbol{H}$ of LDPC code can be represented by the Tanner bipartite graph, which contains two types of node: information node and check node. In the matrix $\boldsymbol{H}$, information node corresponds to each column element, check code corresponds to each row element. In Tanner graph, the rows (check nodes) are represented by squares, the columns (information nodes) by circles, and the "1" by arcs [14, 23]. For example, the check matrix $\boldsymbol{H}$ and Tanner bipartite graph of (10, 5, 2, 4) LDPC codes are shown in Figure 1.

Parity Check Matrix

$$\boldsymbol{H} = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 & x_9 & x_{10} \end{matrix} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \end{array} \begin{matrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \end{matrix}$$

Bipartite Graph

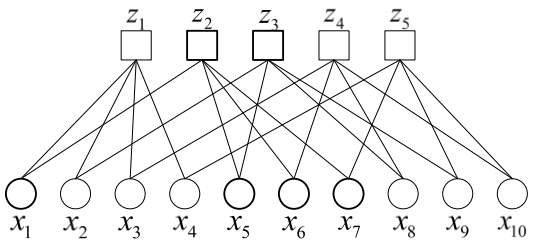


Figure 1. The parity check matrix $\boldsymbol{H}$ and Tanner bipartite graph of (10, 5, 2, 4) LDPC codes

The Gaussian Monitor [24] can be used to operate the $\boldsymbol{H}$ during the coding process, which is shown as follows:

$$\boldsymbol{H} = \left[\boldsymbol{I} \mid \boldsymbol{P}\right] \tag{2}$$

According to the orthogonal relation between the check matrix $\boldsymbol{H}$ and the generation matrix $\boldsymbol{G}$, the generation matrix G can be obtained as follows:

$$\boldsymbol{G}=\left[-\boldsymbol{P}^{T} \mid \boldsymbol{I}\right] \quad (3)$$

Assume that the code group is $\boldsymbol{C}$, and the encoding process uses modulo-2 addition or XOR operation. When the $\boldsymbol{C}$ satisfies the linear equations $\boldsymbol{HC}^{\mathrm{T}}=\boldsymbol{0}^{\mathrm{T}}$, the encoding result of LDPC is shown as follows:

$$\boldsymbol{l}=\boldsymbol{C}\cdot\boldsymbol{G} \quad (4)$$

2.1.2 Decoding

The decoding process of LDPC codes adopts an iterative probability decoding algorithm, among which the more commonly used one is the Belief Propagation (BP) decoding algorithm [25]. In this paper, the decoding algorithm used is the BP decoding algorithm based on soft decision. The soft decision decoding takes the check matrix $\boldsymbol{H}$ as the original model. Measurement is performed based on the Tanner bipartite graph and the obtained information, and iterates between them repeatedly. After judgment, if the equation $\boldsymbol{HC}^{\mathrm{T}}=\boldsymbol{0}^{\mathrm{T}}$ is satisfied, it will be output, otherwise it will continue to iterate and judge until the maximum number of iterations is reached [26]. The specific algorithm step block diagram is shown in Figure 2.

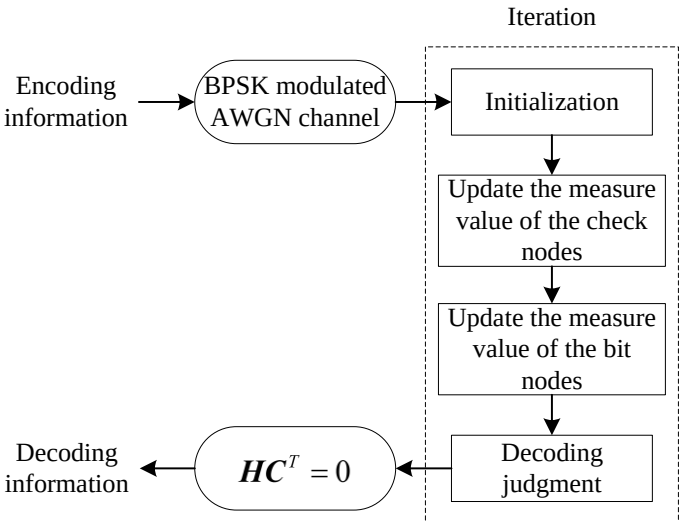


Figure 2. The process of the BP decoding algorithm

2.2 Printing-scanning Channel Model

The information features of printing-quantum-dots mainly refer to the spatial lattice distribution of dots. These features are controlled by pseudo-random to record non-visual information on the basis of satisfying the image display effect, and realize information hiding, anti-counterfeiting, and value-added services. In the process of transmission and printing, the printing-quantum-dots image will be affected by noise, such as the position deviation and shape distortion or even missing of the ink dot, and the stain of flying ink in the printing. Figure 3 shows the established printing-scanning channel model.

The binary graphic data $g_i(x,y)$ of halftone screening passes through the equivalent printing channel $h_p^{'}(x,y)$, then superimposes the noise information $n_p(x,y)$ such as flying ink and ink leakage in the printing process, and obtain the printing image $g_m(x,y)$. Where $h_p^{'}(x,y)$ is formed by introducing non-linear distortion and multiplicative noise $k_{np}(x,y)$ into the ideal printing channel $h_p(x,y)$, that is, $h_p^{'}(x,y)=h_p(x,y)\times k_{np}(x,y)$; During scanning, $g_m(x,y)$ passes through the equivalent scanning channel $h_s^{'}(x,y)$, then superimposes the noise information $n_s(x,y)$ such as geometric distortion and illumination distortion, and obtain the scanning image $g_0(x,y)$. Where $h_s^{'}(x,y)$ is formed by introducing additive noise $k_{ns}(x,y)$ into the ideal scanning channel $h_s(x,y)$, that is, $h_s^{'}(x,y)=h_s(x,y)\times k_{ns}(x,y)$.

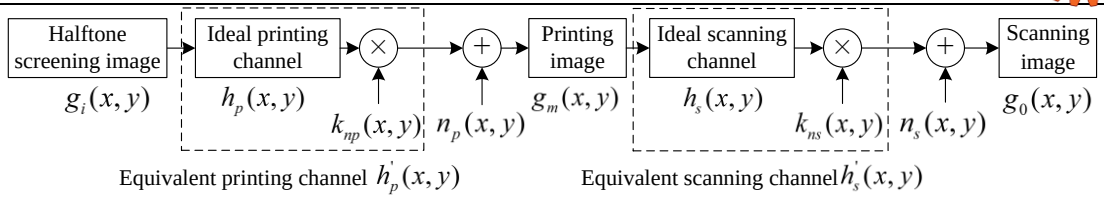


Figure 3. The printing-scanning channel noise model

The printing-scanning systems are cascaded together to realize the whole process of image sending and receiving, and its equivalent mathematical model is Equation (5).

$$\begin{aligned} g_0'(x,y) &= [g_i(x,y) * h_p'(x,y) + n_p(x,y)] * h_s'(x,y) + n_s(x,y) \\ &= g_i(x,y) * h_p'(x,y) * h_s'(x,y) + n_p(x,y) * h_s'(x,y) + n_s(x,y) \\ &= k_n(x,y) * [g_i(x,y) * h_{ps}(x,y)] + n_p(x,y) * [k_{ns}(x,y) * \\ &\quad h_s(x,y)] + n_s(x,y) \end{aligned} \tag{5}$$

Where $h_{ps}(x,y) = h_p(x,y) \times h_s(x,y)$ represents the cascade system of printing-scanning, and $k_n(x,y) = k_{np}(x,y) \times k_{ns}(x,y)$ is the geometric and multiplicative distortion caused by the two processes of printing and scanning.

The distortion and noise pollution in the printing-scanning system are sometimes serious, which usually leads to the pollution of printing-quantum-dots information. Therefore, in order to realize halftone information hiding and its reliable extraction and recognition, it is necessary to study reliability codec technology.

3. PROPOSED SCHEME

In this section, we elaborate on our encoding and decoding scheme for printing-quantum-dots based on LDPC codes. The block diagram of our method is illustrated in Figure 4.

3.1 Information hiding

In this subsection, we describe the information hiding process. To ensure the security of plaintext information and improve the ability of error detection and correction, the following operations need to be carried out:

(1) Information preprocessing

The plaintext of different formats is normalized and converted into a hexadecimal sequence ***M*** for the convenience of subsequent operations.

(2) Information encryption

Information encryption is the process of converting plaintext into ciphertext under the control of key and algorithm. The password system is shown in Figure 5. The plaintext ***M*** is encrypted by the encryption algorithm ***E***, in which the encryption key is k_e, and the ciphertext information ***C*** can be obtained

$$\boldsymbol{C}=\boldsymbol{E}_{k_e}(\boldsymbol{M}) \tag{6}$$

For example, one may use any encryption algorithm such as DES [27], where the encryption key k_e is the same as the decryption key k_d.

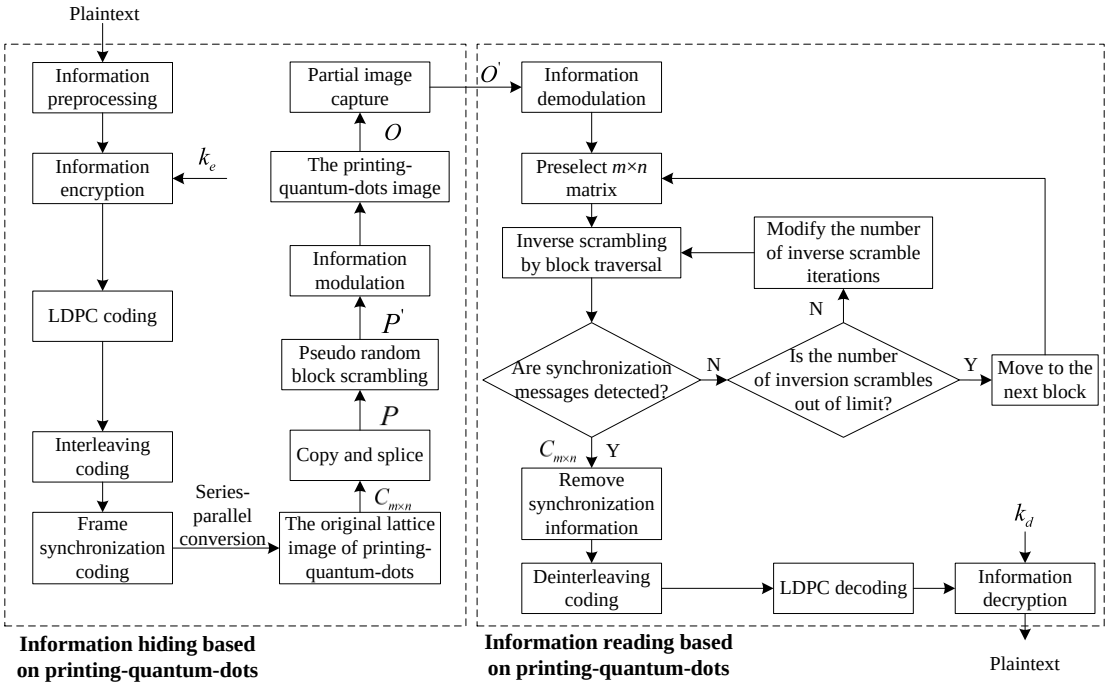


Figure 4. Framework of the proposed scheme

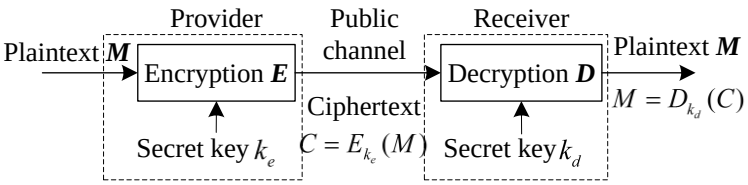


Figure 5. The password system

(3) LDPC combined coding

The ciphertext sequence $\boldsymbol{C}$ is converted into a two-dimensional matrix, and then append the monitor code to each line and each column, so that the number of "1" in each line and each column together with the monitor symbol to be odd (odd check) or even (even check) [28]. Assuming that the length of each row or column symbol together with the monitor symbol is n, where the monitor symbol is a_0, and the symbol information is expressed as $\{a_{n-1}, a_{n-2}, ..., a_1, a_0\}$, it can be expressed as

$$Even\ parity \begin{cases} a_{n-1} \oplus a_{n-2} \oplus \cdots \oplus a_1 \oplus a_0 = 0 \\ a_0 = a_{n-1} \oplus a_{n-2} \oplus \cdots \oplus a_1 \end{cases} \tag{7}$$

$$Odd\ parity \begin{cases} a_{n-1} \oplus a_{n-2} \oplus \cdots \oplus a_1 \oplus a_0 = 1 \\ a_0 = a_{n-1} \oplus a_{n-2} \oplus \cdots \oplus a_1 \oplus 1 \end{cases} \tag{8}$$

The binary code-stream including check information is LDPC coded to obtain symbol information $l_{2n}=\{b_{2n-1}, b_{2n-2}, \ldots, b_1, b_0\}$, and the coding efficiency is 1/2. To interleave l_{2n}[29], we calculate the exclusive-or operations between l_{2n} and pseudo-random bits r_{2n}:

$$e_{2n} = l_{2n} \oplus r_{2n} \tag{9}$$

Where e_{2n} is the sequence after interleaving coding. Then Barker code [30] is added at the end of e_{2n} as frame synchronization information, which is used to record the position of complete information. The coded one-dimensional data is transformed by serial-parallel conversion to obtain a two-dimensional data matrix, that is, the original image of printing-quantum-dots $\boldsymbol{C}_{m\times n}$.

(4) Copying and splicing

To be able to match the size of the cover image, and also to ensure that the printing-quantum-dots image can be partially intercepted for decoding and reading, it is necessary to periodically copy and splice the original image of the printing-quantum-dots to obtain a full spread image $\boldsymbol{P}$.

(5) Pseudo-random block scrambling

Pseudo-random Arnold transform [31] is applied to block $\boldsymbol{C}_{m\times n}$ at different positions in image $\boldsymbol{P}$ to obtain scrambled image $\boldsymbol{P}'$ .The pseudo-random scrambling process can be expressed as

$$\begin{cases} x_d' = (x_d + a \times y_d) \bmod(N) \\ y_d' = [b \times x_d + (a \times b + 1) y_d] \bmod(N) \end{cases} \tag{10}$$

Where x_d and y_d are pixel positions before scrambling, x_d' and y_d' are pixel positions after scrambling, a and b are constants, d is iteration times, and N is the diameter of the image $\boldsymbol{C}_{m\times n}$.

(6) Information modulation

The middle pixel of the $k\times k$ grid is used to represent each pixel in the image $\boldsymbol{P}'$. If the pixel value of the point in the image $\boldsymbol{P}'$ is 1, the middle pixel of the grid is set to 0, otherwise it is set to 1. The mapping relationship is as in formula (11). In this way, the image $\boldsymbol{P}'$ is modulated into a printing-quantum-dots image $\boldsymbol{O}$ with sparse characteristics and large information recording capacity.

$$(x, y) \xrightarrow{f} (x', y') \tag{11}$$

Where (x, y) is the pixel position of the image $\boldsymbol{P}'$, (x', y') is the pixel position of the image $\boldsymbol{O}$, and f is the mapping relationship.

3.2 Information Reading

In this subsection, we describe the information reading process which uses block reading. The printing-quantum-dots image is partially intercepted for decoding and reading. If the intercepted image contains multiple pieces of complete information, it will directly jump out of the traversal process when reading one piece, which greatly improves the information reading speed. The specific algorithm implementation includes the following operations.

(1) Information demodulation

According to the mapping relationship f^{-1}, information demodulation is performed on each pixel (x', y') of the partially intercepted image $\boldsymbol{O}'$ to obtain the pixel (x, y) of the demodulated image $\boldsymbol{D}$.

$$(x', y') \xrightarrow{f^{-1}} (x, y) \tag{12}$$

(2) Information descrambling

We preselect a matrix block of the same size as the image $\boldsymbol{C}_{m\times n}$, and traverse the image $\boldsymbol{D}$ according to the size of the matrix block, then detect synchronization information. If synchronization information is detected, it is descrambled according to formula (13) to obtain the image $\boldsymbol{C}_{m\times n}$; if synchronization information is no detected, it is determined whether the number of descrambling times exceeds the limit: if it exceeds the limit, move to the next bit and traverse again by block, otherwise directly modify the descrambling times, and then perform synchronization information detection.

If the intercepted image of the printing-quantum-dots contains multiple complete information blocks, when traversing the matrix blocks, once the size and synchronization information of the matrix blocks are satisfied, we can directly descramble to obtain the original image of the printing-quantum-dots, and then jump out of the traversal process.

$$\begin{cases} x_d = [(ab + 1) x_d' - a \times y_d'] \bmod(N) \\ y_d = (-b \times x_d' + y_d'] \bmod(N) \end{cases} \tag{13}$$

(3) LDPC decoding

The image $\boldsymbol{C}_{m\times n}$ is transformed into one-dimensional data by parallel-serial conversion, and remove the synchronization information to obtain the data sequence e_{2n}. We calculate the exclusive-or operations between e_{2n} and pseudo-random bits r_{2n}:

$$l_{2n} = e_{2n} \oplus r_{2n} \tag{14}$$

LDPC decoding of symbol sequence l_{2n}: assuming that the initial probability-likelihood ratio message is $L(P_i)$, then the initial channel message is $L^{(0)}(q_{ij}) = L(P_i)$. In the v-th iteration, the message passed from information node j to check node i is

$$L^{(v)}(r_{ji}) = 2\tanh^{-1}\left(\prod_{i' \in R_{j/i}} \tanh\left(\frac{1}{2}L^{(v-1)}\left(q_{i'j}\right)\right)\right) \tag{15}$$

The message passed from the check node *i* to the information node *j* is

$$L^{(v)}(q_{ji}) = L(P_i) + \prod_{j' \in C_{i/j}} L^{(v)}(r_{j'i}) \tag{16}$$

Then the messages of all information nodes are

$$L^{(v)}(q_i) = L(P_i) + \prod_{j \in C_i} L^{(v)}(r_{ji}) \tag{17}$$

The rules of judgment are as follows

$$C_i = \begin{cases} 0 & L^{(v)}(q_i) > 0 \\ 1 & L^{(v)}(q_i) \le 0 \end{cases} \tag{18}$$

If $\boldsymbol{HC}^{\mathrm{T}}=0$ is true, the decoding ends[32], then remove the parity-check information to obtain the ciphertext information.

(4) Information decryption and reading

As shown in Figure 5, information decryption is the process of converting ciphertext $\boldsymbol{C}$ into plaintext $\boldsymbol{M}$, the decryption key is k_d, and the plaintext information is obtained as

$$\boldsymbol{M} = \boldsymbol{D}_{k_d}(\boldsymbol{C}) \tag{19}$$

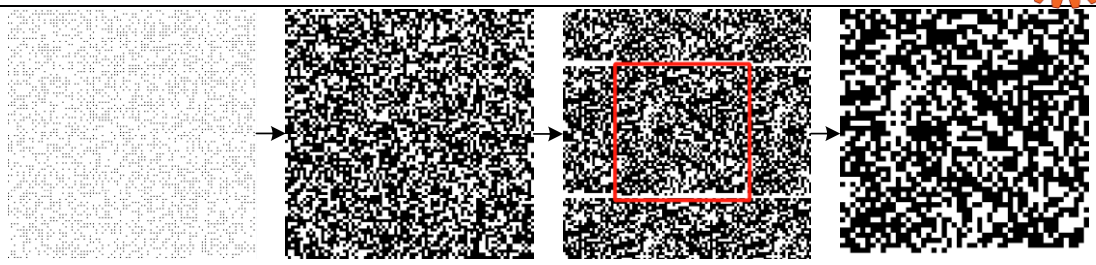
4. EXPERIMENTAL RESULTS

To demonstrate the effectiveness and superiority of our scheme, experiments were conducted on three lengths of strings: 20-character, 40-character and 60-character. The environment of our experiments was based on a personal computer with a 3GHz Intel i5-8500 processor, 8GB memory, 64-bit Windows10 operating system and Matlab R2013a. All of the following experiments use 60-character as an example. In the following subsections, three aspects of experimental results are presented: (1) error detection and correction capability; (2) imperceptibility; and (3) visual quality. Finally, we give the feature comparisons with related schemes. To view the result image of each procedure intuitively, the stream sequence obtained by each processing is converted into black-and-white image.

Figure 6a is the original dot-matrix image containing 60-character, Figure 6bis a pseudo-random scrambling image,and Figure 6c shows the printing-quantum-dot image modulated from Figure 6b. Figure 7b is an image demodulated from Figure 7a. Figure 7c is a descrambling image, which contains a complete information block as shown in Figure 7d, it is the same as the original image obtained by encoding, so the plaintext information can be read out after information decryption.

(a) Original dot-matrix image (b) Pseudo-random scrambling image (c) Printing-quantum-dots image

Figure 6. Information hiding of printing-quantum-dots

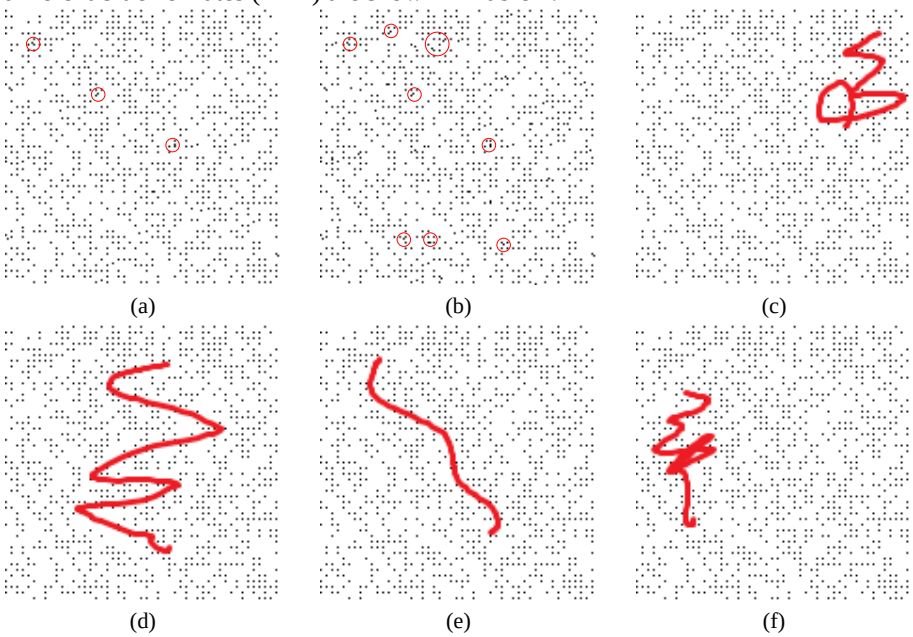


(a) Partially intercepted printing-quantum-dots image (b) Demodulated image (c) Descrambled image (d) Decoded image

Figure 7. Information reading of printing-quantum-dots

4.1 Error detection and correction capability

The error detection and correction ability of the scheme is that the plaintext information can be read from the printing-quantum-dots image with noise. Figure 8ab is a printing-quantum-dots image containing random noise, and Figure 8cdef is a printing-quantum-dots image containing burst noise. The results of decoding and reading under different bit error rates (BER) are shown in Table 1.



(a) (b) (c)

(d) (e) (f)

Figure 8. The printing-quantum-dots image with noise: (a)(b) containing random noise; (c)(d)(e)(f) containing burst noise.

Table 1. Decoding accuracy under different bit error rates

Noise Type	BER	Information Reading
Random noise	Pe<0.3%	Reading
Burst noise	Pe<3.4%	Reading

4.2 Imperceptibility

The original image and watermark are encrypted using the discrete wavelet transform (DWT) and the singular value decomposition (SVD) algorithm [33]. Experiments were conducted on three test images sized 512×512: Lena, Barbara, and Peppers. The watermark image is a printing-quantum-dots image, and the embedding factor is 0.1. The cover image $\boldsymbol{X}$, the watermarked cover image $\boldsymbol{Y}$ and the extracted watermark image are shown in Figure 9. To quantitatively evaluate the imperceptibility of the image, the peak signal-to-noise ratio (PSNR) and the structural similarity index (SSIM) are used. These two methods are widely used to evaluate the quality of the image [34].

(a) Lena (b) Barbara (c) Peppers

(d) Lena embedded in watermark (e) Barbara embedded in watermark (f) Peppers embedded in watermark

(g) Extracted watermark of Lena (h) Extracted watermark of Barbara (i) Extracted watermark of Peppers

Figure 9. Test results: (a) Lena; (b) Barbara; (c) Peppers; (d) Lena embedded watermark; (e) Barbara embedded watermark; (f) Peppers embedded watermark; (g) Extract watermark of Lena; (h) Extract watermark of Barbara; (i) Extract watermark of Peppers.

The PSNR between the image X and the image Y is defined as

$$PSNR = 10 \times \log_{10}\left(\frac{MAX_X^2}{MSE}\right)(dB) \tag{20}$$

Where, *MAX* is the maximum pixel value of image ***X***, and *MSE* is the mean square error between image ***X*** and ***Y***, which is defined as

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[\boldsymbol{X}(i,j) - \boldsymbol{Y}(i,j)\right]^2 \tag{21}$$

Where, $\boldsymbol{X}(i, j)$ and $\boldsymbol{Y}(i, j)$ represent the pixel value of image ***X*** and ***Y*** at position (i, j) respectively; M and N are the width and height of the original cover image.

The SSIM between the image ***X*** and ***Y*** is defined as

$$SSIM(\boldsymbol{X},\boldsymbol{Y}) = \frac{(2\mu_X\mu_Y + C_1)(2\sigma_{XY} + C_2)}{(\mu_X^2 + \mu_Y^2 + C_1)(\sigma_X^2 + \sigma_Y^2 + C_2)} \tag{22}$$

Where, μ_X , μ_Y , σ_X^2 , σ_Y^2 and σ_{XY} are the local mean, variance and covariance of image ***X*** and ***Y*** respectively, and C_1 and C_2 are constants used to maintain stability.

From the perspective of human vision, there is no significant difference between image ***X*** and ***Y***. Besides, from the data in Table 2, it can be seen that the SSIM between image ***X*** and ***Y*** is close to 1, and the PSNR is all greater than 40 dB, which indicates that the printing-quantum-dots image has well imperceptibility.

Table 2. The assessment results of imperceptibility

Cover Image	PSNR (dB)	Average Value of PSNR (dB)	SSIM	Average Value of SSIM
Lena	43.6795		0.9985	
Peppers	45.5311	44.4547	0.9946	0.9973
Barbara	44.1535		0.9988	

4.3 Quality of the implanted image

Color cover image is a GRB image, which contains three channels: green (G) channel, red (R) channel and blue (B) channel. To make the printing-quantum-dots image better hidden in the cover image, it is fully embedded into the B-channel of cover image in the way of gray-gradient. The model is shown as

$$B_{r,c}(i,j)=\begin{cases} B_{r,c}(i,j)-\overline{P_{r,c}(i,j)}\times\xi, & B_{r,c}(i,j)\geq\xi \\ \overline{P_{r,c}(i,j)}\times\xi-B_{r,c}(i,j), & B_{r,c}(i,j)<\xi \end{cases} \quad (23)$$

Where $i=1,2,\ldots,r$, $j=1,2,\ldots,c$, r and c are the width and height of cover image; $P_{r,c}(i,j)\in\{0,1\}$; the value of $B_{r,c}(i,j)$ is 0 to 255; $P_{r,c}(i,j)+\overline{P_{r,c}(i,j)}=1$; $B_{r,c}(i,j)$ and $P_{r,c}(i,j)$ represent the pixel value of the B-channel of cover image and the printing-quantum-dots image at the position (i,j) respectively; ξ is constant.

Experiments were conducted on four kinds of trademark cover images: cover image 1, cover image 2, cover image 3, and cover image 4. Firstly, the B-channel of cover image is extracted, and then the printing-quantum-dots image P is implanted into it by adjusting the value of ξ . The specific process is shown in Figure 10. Figure 11 is color cover image containing printing-quantum-dots. We use formulas (11), (12) and (13) to calculate the MSE, PSNR and SSIM between the cover image of printing-quantum-dots implanted in B-channel and the original cover image, and give the feature comparisons with the cover image of printing-quantum-dots implanted in R/G/B-channel, as shown in table 3. It can be seen from the table that the MSE, PSNR and SSIM of the printing-quantum-dots implanted into the B-channel are higher, and the PSNR is above 54, the SSIM is above 0.99, which indicates that the color cover image obtained by implanting printing-quantum-dots into the B-channel is very similar to the original cover image and achieves a good hiding effect.

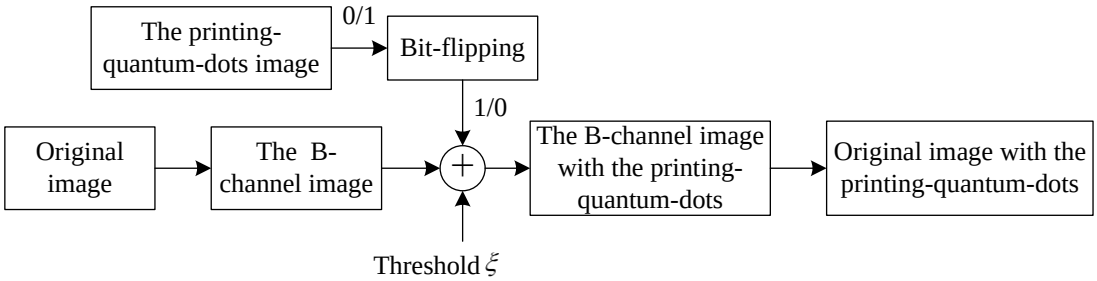
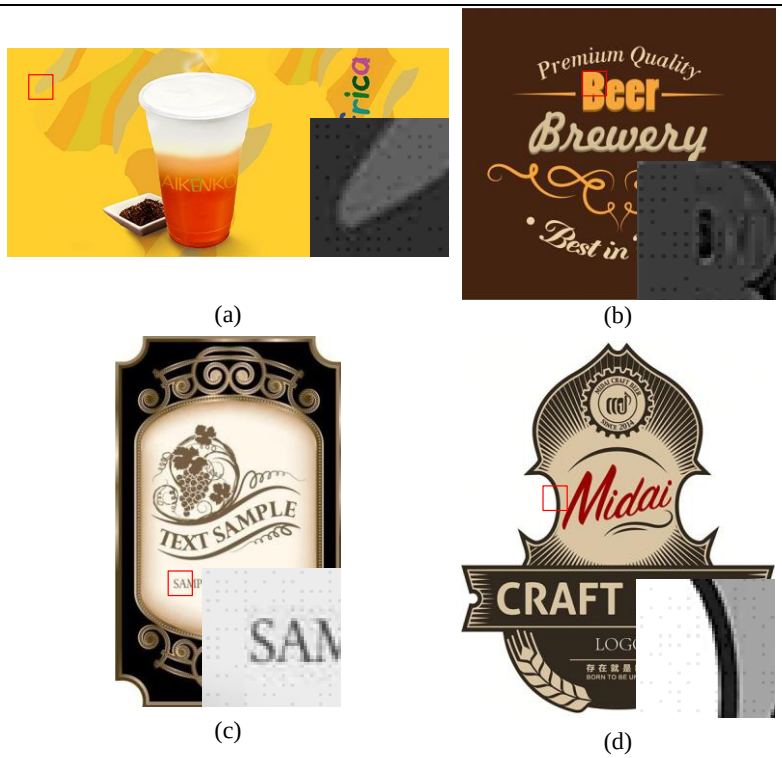


Figure 10. The process of implanting printing-quantum-dots into B-channel

Table 3. The MSE PSNR and SSIM of different implantation methods

CoverImage	Implanting R/G/B-Channel			Implanting B-Channel			Reading
	MSE	PSNR	SSIM	MSE	PSNR	SSIM	
Image 1	32.88	17.79	0.140	0.36	56.78	0.994	Reading
Image 2	16.96	23.54	0.422	0.46	54.84	0.995	Reading
Image 3	31.36	18.20	0.621	0.41	55.72	0.997	Reading
Image 4	44.08	15.24	0.431	0.49	54.19	0.995	Reading



(a) (b) (c) (d)

Figure 11. Cover image with printing-quantum-dots: (a) cover image 1; (b) cover image 2; (c) cover image 3; (d) cover image 4

4.4 Experimental comparison

Table 4 shows the coding efficiency of the proposed scheme and related schemes. Table 5 gives comparisons of decoding time. The combined coding scheme based on LDPC code proposed in this paper is different from reference [35] (BCH code), and convolutional code, the decoding time is much shorter, and the coding efficiency is also higher.

Table 4. Coding efficiency

Channel Encoding	Coding Efficiency
BCH code [35]	4/7
Convolution code	1/2
LDPC code (Ours)	1/2

Table 5. The comparison of decoding time

Block Size /pixel	Decoding Time of Different Decoding Algorithms /s		
	BCH Code [35]	Convolutional Code	LDPCCode (Ours)
138×138	0.52	-	-
147×147	1.19	0.55	**1.04**
165×165	4.93	2.61	**2.58**
174×174	8.30	4.79	**2.27**
180×180	10.77	6.73	**2.28**
195×195	18.24	12.84	**2.30**
210×210	28.16	21.22	**2.30**
240×240	55.21	44.63	**2.32**

5. CONCLUSIONS

In this paper, a reliable encoding and decoding scheme for two-dimensional sparse lattice information based on printing-quantum-dots image is proposed. As the printing-quantum-dots information is easy to be corrupted, we adopt information encryption, interleaving coding, LDPC coding and frame synchronous coding to improve the ability of error correction artificially. This can obtain a printing-quantum-dots image with large information capacity, good hiding effect and difficult to copy, more importantly, the printing-quantum-dots

image can be partially intercepted for decoding and reading. Experimental results show that the scheme has high anti-replication, good information hiding effect, high error detection and correction ability, large data recording capacity and strong imperceptibility.

6. ACKNOWLEDGEMENTS

This work was supported by National Natural ScienceFoundation of China (61972042), Beijing Fund-Municipal Education Commission Joint Project(KZ202010015023), and Research Project of BeijingInstitute of Graphic Communication (Ef202001).

REFERENCES

[1]. H.N. Dharavath. Effect of Color Output Modification Approach (COMA) on the Gray Balance: A Mismatch of Device Calibration, Destination and Source Profiles, and Halftone Screening. *Journal of Graphic Engineering and Design,11(1)*, 2020, 13–25.
[2]. Y.V. Kuznetsov. *High-definition halftone printing*(Principles of Image Printing Technology.Springer, Cham, 2021)331-352.
[3]. C. Kim, D. Shin, L. Leng, et al. Separable reversible data hiding in encrypted halftone image. *Displays,55*, 2018, 71-79.
[4]. X. Wu, C.N. Yang, Y.W. Liu. High capacity partial reversible data hiding by hamming code. *Multimedia Tools and Applications*, *79*, 2020, 23425-23444.
[5]. B. Jana, D. Giri, S.K. Mondal. Partial reversible data hiding scheme using (7, 4) hamming code. *Multimedia Tools and Applications*, *76(20)*, 2017, 21691-21706.
[6]. C.N. Yang, S.Y. Wu, Y.S. Chou, et al. Enhanced stego-image quality and embedding capacity for the partial reversible data hiding scheme. *Multimedia Tools and Applications*, *78(13)*, 2019, 18595-18616.
[7]. Y.X. Sun, Q. Li, B. Yan, et al. Reversible data hiding in dual encrypted halftone images using matrix embedding. *Multimedia Tools and Applications*, *79(37)*, 2020, 27659-27682.
[8]. X. Wu, C.N. Yang, Y.W. Liu. A general framework for partial reversible data hiding using hamming code. *Signal Processing*, *175*, 2020, 107657.
[9]. S. Kapse, K.N. Singh. Survey on Reversible Data Hiding in Encrypted Images Using POB Histogram Method. *International Journal of Advanced Computer Technology*, *8(5)*, 2019, 01-06.
[10]. Y. Liu, H. Zhao, S. Liu, et al. A robust and improved visual quality data hiding method for HEVC. *IEEE Access*, *6*, 2018, 53984-53997.
[11]. I. Usman, A. Khan. BCH coding and intelligent watermark embedding: Employing both frequency and strength selection. *Applied Soft Computing*, *10(1)*, 2010, 332-343.
[12]. R.J. Mstafa, K.M. Elleithy. A novel video steganography algorithm in DCT domain based on hamming and BCH codes. *2016 IEEE 37th Sarnoff Symposium*. *IEEE*, 2016, 208-213.
[13]. S.G. Yang, C.X. Li, S.H. Sun. Text information hiding method based on chaotic map and BCH code in DWT domain of a carrier image. *2007 International Conference on Wavelet Analysis and Pattern Recognition*. *IEEE*, *4*, 2007, 1754-1758.
[14]. Z. Wang, X. Meng. Digital image information hiding algorithm research based on LDPC code. *EURASIP Journal on Image and Video Processing*, *2018(1)*, 2018, 1-12.
[15]. C.V. Kumar, V. Natarajan, K. Nirmala, et al. Encrypted separable reversible watermarking with authentication and error correction. *Multimedia Tools and Applications*, *78(6)*, 2019, 7005-7027.
[16]. C. KIM, D. SHIN, D. SHIN. Data Hiding in a Halftone Image Using Hamming Code (15, 11). *Asian Conference on Intelligent Information and Database Systems*. Springer, Berlin, Heidelberg, 2011, 372—381.
[17]. R.G. Gallager. *Low-Density Parity Check Codes*. Cambridge, MA: MIT Press, 1963.
[18]. D.J.C MacKay, R.M. Neal. Near Shannon limit performance of low density parity check codes. *Electronics letters*, *32(18)*, 1996, 1645-1646.
[19]. C. Berrou, A. Glavieux. Near optimum error correcting coding and decoding: Turbo-codes. *IEEE Transactions on communications*, *44(10)*, 1996, 1261-1271.
[20]. J. Thorpe. Low-density parity-check (LDPC) codes constructed from protographs. *IPN progress report*, *42(154)*, 2003, 42-154.
[21]. Z. Wang, Y. Lou, W. Wang, et al. Research on the application of LDPC code in chaotic sequence image encryption. *Cluster Computing*, *22(3)*, 2019, 6359-6370.
[22]. D. Klinc, J. Ha, S.W. McLaughlin, et al. LDPC codes for the Gaussian wiretap channel. *IEEE Transactions on Information Forensics and Security*, *6(3)*, 2011, 532-540.
[23]. I. Diop, S.M. Farssi, M. Chaumont, et al. Using of LDPC Codes in Steganography. *Journal of Theoretical and Applied Information Technology*, *38(1)*, 2012, 103-109.

[24]. S. Parter. The use of linear graphs in Gauss elimination. *SIAM review*, *3(2)*, 1961, 119-130.
[25]. J. Liu, R.C. de Lamare. Low-latency reweighted belief propagation decoding for LDPC codes. *IEEE Communications Letters*, *16(10)*, 2012, 1660-1663.
[26]. N. Varnica, M.P.C Fossorier, A. Kavcic. Augmented belief propagation decoding of low-density parity check codes. *IEEE Transactions on Communications*, *55(7)*, 2007, 1308-1317.
[27]. G. SINGH. A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal of Computer Applications*, *67(19)*, 2013, 33—38.
[28]. X. WANG, S. TANG. Bit-level Soft-decision Decoding of Double and Triple-parity Reed-solomon Codes Through Binary Hamming Code Constraints. *IEEE Communications Letters*, *19(2)*, 2014, 135—138.
[29]. P.N. Ramavath, A. Kumar, S.S Godkhindi, et al. Experimental studies on the performance of underwater optical communication link with channel coding and interleaving. *CSI Transactions on ICT*, *6(1)*, 2018, 65-70.
[30]. E.E. Hollis. Comparison of combined Barker codes for coded radar use. *IEEE Transactions on Aerospace and Electronic Systems*, *1*, 1967, 141-143.
[31]. M. Hamidi, M. El Haziti, H. Cherifi, et al. Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform. *Multimedia Tools and Applications*, *77(20)*, 2018, 27181-27214.
[32]. I.E. Bocharova, B.D. Kudryashov, V. Skachek, et al. BP-LED decoding algorithm for LDPC codes over AWGN channels. *IEEE Transactions on Information Theory*, *65(3)*, 2018, 1677-1693.
[33]. F.N. Thakkar, V.K. Srivastava. A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. *Multimedia Tools and Applications*, *76(3)*, 2017, 3669-3697.
[34]. Y.X. Sun, B. Yan, J.S. Pan, et al. Reversible data hiding in encrypted color halftone images with high capacity. *Applied Sciences*, *9(24)*, 2019, 5311.
[35]. Y.J. WANG, P. CAO.Reliability Encoding and Decoding Algorithm of Multiple Combination Information Based on Printed Quantum Dots.*Packaging Engineering*, *42(19)*,2021, 192-203.