An Image Watermarking Algorithm Based on Discrete Hopfield Neural Network Encryption

An Image Watermarking Algorithm Based on Discrete Hopfield Neural Network Encryption

Liu Qingliang[1], Sui Shujiao[1*], Yang Shuguo[2], Xiong Pengcheng[3]

[1] School of Mathematics and Physics, Qingdao University of Science and Technology, Qingdao 266061, China

[2] Institute of Intelligence Science & Data Technology, School of Mathematics &Physics, Qingdao University of Science and Technology, Qingdao 266061, China

[3] Central Economics Team, Amazon Inc., 345 Boren Ave N, Seattle, WA 98109, USA

Abstract: With the rapid development of science and information technology, it is more and more important to design a robust image watermarking algorithm to protect the intellectual property and information security of images. First of all, this paper encrypts the watermark information to improve the security of the watermarking algorithm through discrete Hopfield neural network based on chaos. Then, based on the image wavelet decomposition, the watermark information is embedded into the low and middle frequency wavelet coefficients according to the minimum Visual error and pixel position distortion. Experiments show that the algorithm has good security, robustness and invisibility.

1 Introduction

With the rapid development of science and information technology, it is more and more important to design a robust image watermarking algorithm to protect the intellectual property and information security of images. It is found that DWT transform has good spatial location, frequency expansion and multi-resolution characteristics. And it can well reflect the characteristics of human visual system. The watermark generated by wavelet transform has good visual effects and resistance to multiple attacks, DWT transform has been widely used in image watermarking and development [1,2].

In addition, with the development of image watermarking technology, watermarking information encryption has become one of the effective methods to ensure the security of image watermarking. Traditional watermark encryption methods are logistic, arnold, chaotic encryption [3-5]. Although these traditional methods have better encryption effects, they are mostly well known to the public. Once an attacker masters the encryption algorithm, it is easy to obtain the watermark information embedded in the images. In order to better encrypt watermarking, neural network learning algorithms, error correction coding and other technologies are also widely used in watermark encryption algorithm. Such as Tsai and others based on neural network adaptive audio water technology, by recording the relationship between the original audio and watermarked audio information to achieve blind detection[6]; Liang Jiadong and others based on Chebyshev chaotic neural network video watermarking Algorithm. This algorithm is used to encrypt the watermark information to improve the security of the algorithm[7]. In addition, in order to better meet the human visual characteristics, Yang Haitao proposed a color image watermarking algorithm using JND and zero-tree coding [8]; Ren Keqiang[9] proposed a watermarking algorithm based on BCH and JND to better meet the human visual effects.

In order to improve the security of the watermarking algorithm, this paper encrypts the watermark information based on the discrete Hopfield neural network with chaos, and further improves the robustness and invisibility of the watermarking algorithm. Then, based on the image wavelet decomposition, the watermark information is embedded into the low and middle frequency wavelet coefficients according to the minimum Visual error and pixel position distortion.

2 DHNN Encryption System Based on Chaos

2.1 Hyper-chaos System

The low-dimensional chaotic system has certain defects, such as logistic map, which is very sensitive to the initial value. The generated chaotic sequence has the characteristics of non-periodic and non-convergence. However, the high-dimensional chaotic system has more directional instability and larger key space, which can better meet the watermarking security requirements of watermarking information. Therefore, this paper chooses two-dimensional hyper-chaotic system as follows [10]:

$$\begin{cases} x_{n+1} = 0.167x_n^2 - 1.09y_n^2 \\ y_{n+1} = 1.24x_n - 0.3y_n \end{cases} \quad (1)$$

Enter the initial value (x_0, y_0), the formula (1) will get a generate sequence x_n and y_n.

2.2 Discrete Hopfield Neural Network System [11]

DHNN is a single-layer, feedback network with binary input / output. Assuming a DHNN structure consisting of three neurons, the structure is as follows in Figure 1. In the above figure, layer 0 is just an input to the network. It is not an actual neuron, so it has no computational function. The first layer is a neuron. Therefore, the summation is performed on the product of the input information and the weight coefficient, and then the output information is passed through non- Linear function processing f. In this paper, $f(u_j(t)) = \mathrm{mod}(abs(u_j(t)), 2)$.

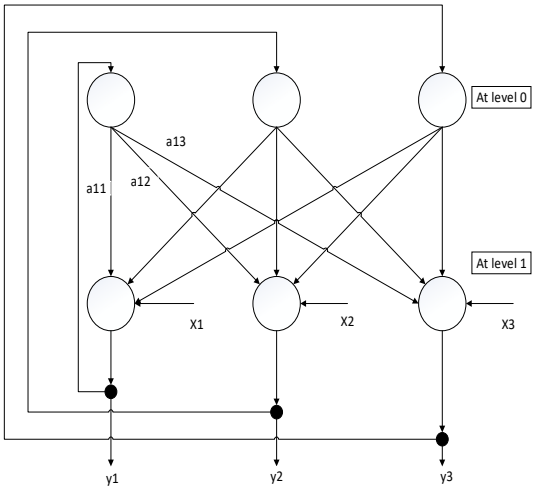

Figure 1.DHNN

In general, A and θ can uniquely identify a DHNN. The DHNN weights A selected in this paper satisfy:

$$a_{ij} = \mathrm{mod}(\left\lfloor 10 * abs(\frac{x(i) - x(j) + 1.5}{2.5}) \right\rfloor, 2) \quad (2)$$

The DHNN threshold θ satisfies:

$$\theta_i = \mathrm{mod}(\lfloor 10 * abs(y(i)) \rfloor, 2) \quad (3)$$

When $i = j$, there is $a_{ij} = 0$, that is to say, the chaotic DHNN is a stable network.

2.3 Watermark Encryption Algorithm Description

A binary image of $N \times N$ size is selected as the watermark image, and the watermark image data matrix $W(x, y)$ is expanded in columns to obtain the original watermark signal sequence $w(x)$. According to the key K (the value of chaotic sequence (x_0, y_0) and the number of DHNN iterations L), a DHNN based on chaos is obtained. In this paper, key K is $(0.2, 0.7)$ and $L = 3$ .Network input sequence is $S = \{s_i\}, i = 1, 2, \cdots, n$, in which:

$$s_i = \mathrm{mod}(\left\lfloor 10 * abs(\frac{x(i) - y(i) + 1.5}{2.5}) \right\rfloor, 2) \tag{4}$$

An output sequence $h(x)$ of the above network with length $N \times N$ is obtained from the DHNN system and XOR with $w(x)$ as shown in the following equation to obtain an encrypted watermark signal sequence $w'(x)$.

$$w'(x) = w(x) \oplus h(x) \tag{5}$$

3 Watermark Embedding Algorithm Description

For an arbitrary size of the image, and cut it to $M \times M$ size, and do the following:

Step1: Extract the image $I(x, y)$ brightness component data matrix, and use Haar wavelet basis of its two-layer wavelet decomposition.

Step2: Extracting wavelet coefficients $LL2(x, y)$ of the low-frequency approximation sub-graph after the second-layer wavelet decomposition, the absolute value of the filter residue is obtained through a high-pass filter H first, and then a low-pass filter L acts on the absolute value of the residual to calculate the pixel value Position distortion $D(x, y)$. The formula is as follows [12]:

$$D = \left| I \otimes H \right| \otimes L \tag{6}$$

Step 3: Expand $D(x, y)$ by column and sort it from big to small to obtain $d(x)$, and select T as the threshold value to obtain a binary matrix $L(x, y)$, and the calculation formula is as follows.

$$T = d(N \times N + 1) \tag{7}$$

$$L(x, y) = \begin{cases} 1 & D(x, y) > T \\ 0 & D(x, y) \le T \end{cases} \tag{8}$$

The position marked as 1 is the watermark embedding position (high texture area of the low-frequency approximation sub-graph).

Step 4: The encrypted watermark signal is embedded into the low frequency approximation sub-graph wavelet coefficients according to the following formula. Explodes by column $L(x, y)$, searches for a position marked as 1, and counts as t (t counts from 1 to $N \times N$ ends).

If $L(x, y) = 1$,

$$LL2(x, y) = \begin{cases} LL2(x, y) + \alpha * D(x, y) & w(t) = 1 \\ LL2(x, y) - \alpha * D(x, y) & w(t) = 0 \end{cases} \tag{9}$$

Where α is the embedding strength, in this article $\alpha = 0.4$.

4 Watermark Extraction and Detection

4.1 Watermark Extraction

For the image to be measured I^*, firstly, it is subjected to a two-layer wavelet transform to obtain a wavelet coefficient $LL2^*(x, y)$ of the low frequency approximation sub-graph, and then the encrypted

watermark sequence is extracted according to the following formula. The search begins with the $L(x,y)$ column, marked as 1, and counted as t (t starts counting from 1 to $N \times N$ ends).

If $L(x,y)=1$,

$$w^*{}'(t)=\begin{cases}1 & LL2^*(x,y) > LL2(x,y)\\ 0 & LL2^*(x,y) \le LL2(x,y)\end{cases} \quad (10)$$

According to the key K, a sequence $h(x)$ of length $N \times N$ is obtained by the above chaotic DHNN system, and is subjected to an exclusive XOR operation as shown in the following formula to obtain the extracted watermark signal sequence $w^*(x)$, and further obtained $W^*(x,y)$.

$$w^*(x)=w^*{}'(x)\oplus h(x) \quad (11)$$

4.2 Watermark Detection Index

After the original image embeds the watermark information, the quality of the watermarked image is measured by the peak signal-to-noise ratio (PSNR) value. The watermark information is detected by calculating the extracted watermark NC value to determine whether the image to be tested contains watermarking [13].

5 Algorithm Innovation

In the watermark encryption algorithm, a new Hopfield neural network encryption system based on chaos is introduced, which increases the direction uncertainty of the chaotic system, enlarges the key space and further improves the security of the watermarking algorithm.

In the watermark embedding algorithm, we further optimize the location of the watermark embedding and ensure that the embedding changes are more concentrated in the texture region of the wavelet approximation sub-graph. In addition, all the pixel locations in the texture area have a relatively small change in embedding, that is, embedding information with a relatively small degree of distortion as embedding intensity in a place where the distortion is large, and a place with a smaller distortion in accordance with a relatively large degree of distortion as Embedded strength embedded information. This not only ensures the robustness of the watermarking algorithm, but also reduces the image distortion caused by watermark embedding.

6 Simulation Experiment

6.1 Experimental Environment Settings

Experimental software MATLAB2016a, select 512 * 512 "Scaven.jpg" carrier image and 64 * 64 binary watermark image "QUST", and use Section 2.3 to encrypt the watermark image, as shown below Figure 2 are the original carrier image, watermark image and encrypted watermark image.

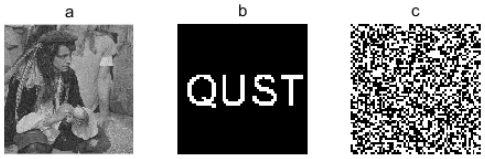

Figure 2.Original image and encrypted watermark image

Figure 3.Watermark embedded position, including watermarked images and watermarked images

The imperceptibility of the image watermarking algorithm requires that the watermark cannot be visually perceived by the carrier image after embedding the watermarking. According to the above embedding algorithm, this paper embeds the watermark in the carrier image. The PSNR value of the watermarked image is 35.2413, and the NC value of the extracted watermark is 1. As shown in Figure 3 are watermark embedding position, contains watermark image and watermark image.

In general, a high PSNR image quality is relatively high. Normally, when the PSNR value is above 28, the image quality difference is not so significant. When the PSNR value is higher than 35 to 40, the image difference cannot be visually recognized. Therefore, this article embedded watermark image cannot tell the difference after the naked eye.

6.2 Attack Experiment

The watermarking images were subjected to the following attacks: 'salt and pepper noise', 'Gaussian filter ', 'rotate', 'cut', 'JPEG compression' and so on. Different intensities of each attack were tested. The robustness of the algorithm was verified by comparing the PSNR and NC values.

(1) Salt and Pepper Noise

There are many types of noise. In this paper, 'salt and pepper noise' is taken as an example. By randomly changing the pixel value of the image, black and white noise points are generated by the image sensor and the transmission channel. In this paper, watermarking images with intensity coefficient of 0.01, 0.02, 0.05 salt and pepper noise attack, the extracted watermark effect map shown in Figure 4.

(2) Gaussian filter

Gaussian filter attack is the process of weighted averaging each pixel value in the image through the pixel itself and the pixel values in its neighborhood. In this paper, Gaussian filter attacks on watermarked images were performed, with intensities of [5, 0.01], [5, 0.05], [5, 0.1], respectively. The watermark extracted after the attack is shown in Figure 5 below.

(3) Rotate

Taking the center of the image as the center, rotate clockwise by different angles, and then cut the rotated image into the original image size, and retain the original image information to the maximum extent, and then rotate the whole image counterclockwise to obtain the corresponding angle as final image. In this paper, the rotation attacks of 5 °, 10 ° and 15 ° are carried out respectively. The extracted watermark image is shown in Figure 6 below.

(4) Cut

Cut attack is to cut off any size of image block in any position of the image, and try to keep the main content of the image. In this paper, the size of 16 × 16, 32 × 32, 64 × 64 pixel image blocks are cut in the center of the image, the upper left corner and the lower right corner, respectively. The extracted watermark is shown in Figure 7 below.

(5) JPEG compression

JPEG compression is a type of loss compression that takes advantage of the human visual system's characteristics by combining the loss-of-view redundancy with the redundant information of the data itself, using a combination of quantization and lossless compression coding. In this paper, JPEG compression quality factor is divided into 80, 70, 60, extracted watermark effect as shown in Figure 8 below.

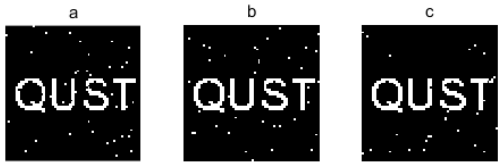

Figure 4.Image watermark extracted after 'Salt and Pepper noise' attack

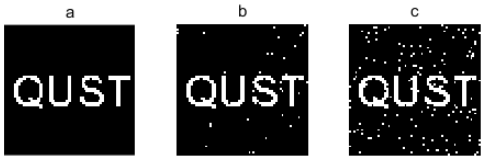

Figure 5.Image watermark extracted after 'Gaussian filter' attack

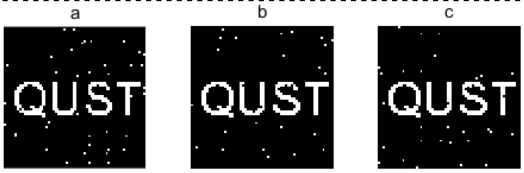

Figure 6.Image watermark extracted after 'Rotate' attack

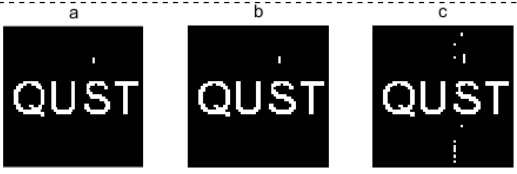

Figure 7.Image watermark extracted after 'Cut' attack

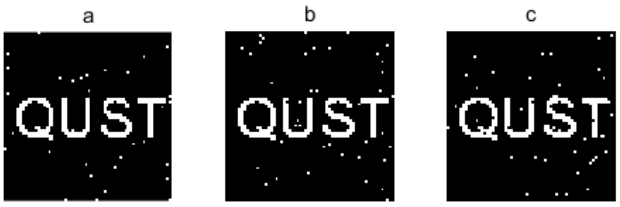

Figure 8.Image watermark extracted after 'JPEG compression' attack

After the watermarked images are attacked with the above-mentioned different intensity types, the PSNR values corresponding to the post-attack images and the NC values for watermarking are calculated through experiments, as shown in Table 1 below.

It can be seen from the experimental renderings and experimental data that the image still has better quality after embedding the watermark, and can still extract the watermark information well when the watermarked image suffers different kinds of intensity attacks. Even if the attack strength is large, it can also identify the watermark information more clearly, indicating that the watermarking algorithm is robust to the above attacks.

7 Conclusion

In this paper, the watermarking algorithm is first encrypted by using the DHNN based on chaos, which improves the security of the watermarking algorithm compared with the literature [10]. Secondly, based on the image wavelet decomposition, the minimum visual error and the size of each pixel distortion value, the watermark information embedded in the low-frequency wavelet coefficients. By compared the algorithm with the literature [7], the watermarked picture quality is better, and anti-attack ability is stronger. By adding the watermark effect chart can be seen, after adding the watermark, the image quality is good and the watermark invisibility is good; PSNR value and NC value under various attacks obtained by the relevant attack experiments can be seen, even if the watermark image in the PSNR value In the low case, the watermark information can still be detected better, indicating that the robustness of the algorithm is better.

Table 1.PSNR and NC in Different Attack Strengths

Attack Type	Strength	PSNR	NC
Salt and Pepper	0.01	27.1458	0.9346
	0.02	27.1304	0.9393
	0.05	27.1333	0.9500
Gaussian filter	[5,0.01]	34.0758	1
	[5,0.05]	27.1389	0.9394
	[5,0.1]	24.2093	0.7987
Rotate	5°	27.1439	0.9371
	10°	27.1481	0.9550
	15°	27.1323	0.9476
Center cut	16×16	39.5923	0.9948
	32×32	34.2376	0.9948
	64×64	28.0846	0.9681
JPEG	80	27.1317	0.9467
	70	27.1647	0.9350
	60	27.1319	0.9268

Acknowledgments

This work are supported by Shandong Province Key Research and Development Planning Project (2015GGX101020)， in part by Shandong Province Graduate Education Innovation Planning Project (SDYY16010)，in part by the Project of Shandong Province Education Science in 12th Five-Year Plan

(YBS15014).， in part by the Project of Shandong Province Instructing Ability Improvement for Graduate Supervisor (SDYY17042).

References

[1] Reza M S, Khan M S A, Alam M G R, et al. An Approach of Digital Image Copyright Protection by Using Watermarking Technology [J]. *International Journal of Computer Science Issues*, 2012, 9(2).
[2] Liu Yanqi, Zhan Fuyu, MATLAB image and video processing practical examples[M], *Electronic Industry Press*,2015: 280-290.
[3] Wu Danhui, Zheng Enrang, Research on Encryption Algorithm o f I m a g e Watermarking Based on Logistic and Arnold[J], *Computer Measurement and Control*, 2017, 4:193-196.
[4] Peng Chuan, Mo Haifang, Logistic Chaos Based Robust Watermarking Scheme, *Computer Simulation*,2012,(9):278-282.
[5] Wu Lingling, Zhang Jianwei, Ge Qi. Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm [J]. *Microcomputer Information*, 2010, 26(14):206-208.
[6] Tsai H H, Cheng J S. Adaptive Signal-Dependent Audio Watermarking Based on Human Auditory System and Neural Networks [J]. *Applied Intelligence*, 2005, 23(3):191-206.
[7] Liang Jiadong, Yang Shuguo. A Video Watermarking Algorithm Based on Chebyshev Chaotic Neutral Network [J]. *Computer and Modernization*, 2017(04):14-17.
[8] Yang Haitao, Zheng Hongyuan, A Digital Watermarking Algorithm For Color Images Based on JND and Zerotree Coding [J],*Computer Applications and Software*, 2012, 29(06):278-281.
[9] Ren Keqiang, Wang Fayin, Digital image watermarking algorithm in wavelet domain based on BCH and JND [J], *Video Engineering*, 2016, 40(9):22-25.
[10] XIAO Zhenjiu, LI Nan, WANG Yongbin, et al. Zero watermarking scheme for medical image temper location based on hyper-chaos encryption. *Computer Engineering and Applications*, 2017,（7）：115-120.
[11] Sabahi F, Ahmad M O, Swamy M N S. An unsupervised learning based method for content-based image retrieval using hopfield neural network[C]// *Signal Processing and Intelligent Systems*. IEEE, 2017.
[12] Li B, Wang M, Huang J, et al. A new cost function for spatial image steganography[C]// *IEEE International Conference on Image Processing*. IEEE, 2015:4206-4210.
[13] Yang Shuguo, Research on Robust Image Digital Watermarking Technology [D], *Harbin Engineering University*, 2003:32-46.