Digital Watermarking Based on the Error Correcting Coding

Jinyu Lu [1, a *] and Tao Qu [2, b]

[1]College of Engineering Bohai University Liaoning, Jinzhou, China

[2]School of Electronics & Information Engineering

University of Technology Liaoning Liaoning, Jinzhou, China

[a]156241142@qq.com, [b]54333928@qq.com

Keywords: Watermark; Hamming coding; Error-correcting coding; Discrete wavelet transform (DWT); Robustness

Abstract. A novel digital watermarking scheme is proposed instead of the traditional watermarking. The binary watermark image is processed by error-correcting coding before it is embedded into the discrete wavelet-transformed host image. It is more effective to improve the security and robustness of the watermarked image by proposed scheme. Amount tests and results indicate that the proposed scheme have security and robustness against noise and commonly image processing methods such as Gaussian's noise, filtering, JPEG compression, and crop procession etc.

Introduction

Why is the digital watermark embedded into the protected object such as the images and audio, video and so on? The reason is that it is able to prove their copyright ownership of the digital information. Generally the digital watermark is the author's name, serial numbers, logos etc.

Actually the digital watermark is a set of data, which is carried the ownership of digital products. The digital watermark is permanently embedded in the multi-media data used for copyright protection. Usually the watermarking system includes watermark embedded system and watermark-detection system. Watermark embedded system has two inputs which one is the host image, which another is the watermark and the output is watermarked image. Watermark-detection system is used to extracting watermark.

The universal digital watermarking system includes the embedding and detecting (extraction) two processes. In the digital watermark embedding process, the goal of the embedded algorithm is to find a better half between invisibility and robustness. Detection (extraction) process mainly is to design a corresponding to the embedding procedure detection (extraction) algorithm. Detection algorithm based on the test result of statistical principle to judge watermark existence, its goal is to reduce the false-probability as low as possibly. Comparing watermarked image (such as string or ICONS, etc.) with the original watermark image we judge whether the watermark existence or not. And, to give the increase the difficulty of removing watermark, most of the water for all printed on the embedded and detected (extraction) used the key, only the master key can read the watermarks.

The function of watermark embedding system is to embed watermark into the original image, however, in order to successfully extract the watermark signal, the algorithm must make a watermark on the intentional or unintentional attacks and distortions (equivalent to channel noise) of robustness. "Fig. 1" is a general watermark embedding process, the input for the original image I, the watermark W, the key K (public or private), the output is watermarked image I', then the process of embedding can be defined as: I×K×W→I'.

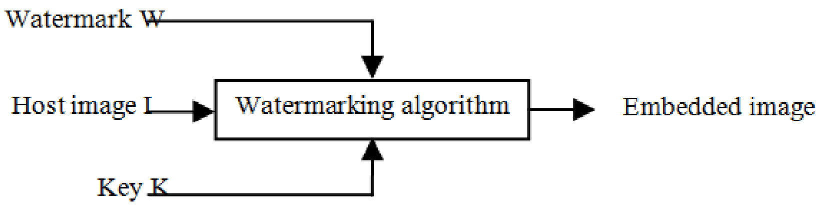


Figure 1. Watermark embedding process

The function of watermark detection system is to complete that the image is detected from the extracted watermark signal. It describes the general watermark detection process in “Fig. 2”, in which the study shows the confidence of the image I’, there is the possibility of watermark.

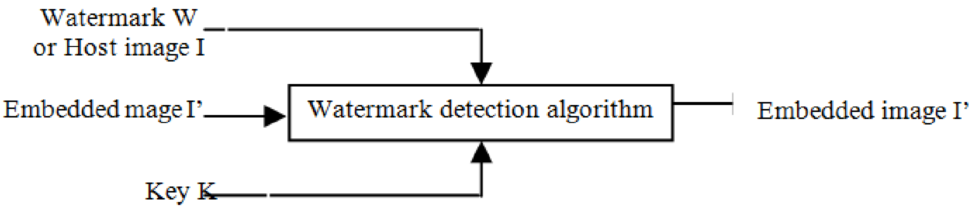


Figure 2. Watermark detection process

Because digital watermarking technology can effectively solve its multimedia copyright protection issue, it has received most attentions on both the international scientific community and the business community.The research of digital water-marking technology going more deeply, the range of application is more widely.

According to the different main media, it can be classified into image watermarking, digital watermarking and other audio etc. Currently digital watermarking is kept their eyes on by scientists and technicians.

To view as the meaning of the embedded watermark, digital watermarking technology includes two parts: insignificant watermarking and significant watermarking. The former applies the watermark which is no practical significance of binary the PN sequence, ID number etc. the latter applies the watermark which is significant signal such as image, writing etc. In comparison, the significant watermarking visually shows the message of work and can protect the work’s copyright, so it is the focal point of watermarking study now.

In recent years, people have projected many methods to improve robustness. The reported typical ways are as follows: the choice of embedded method[1,2], an adaptive watermarking algorithm based on HVS/HAS (human vision system/human auditory system) Model[3,4], the application of error-correcting code[5~9],the way based on CDMA[10]etc. However, today's typical methods on the digital watermark technique are the hot spot of algorithm.

It was in line with this, the paper from information encoding angle, proposed the image watermarking algorithm which based on the error-control coding technology, and the solution is: encode Hamming code before embedding image watermark signal, in the extraction, so it can correct mistakes. During the transmission, extract correctly from the watermark, this paper used the wavelet coefficients quantification methods on embedding and extracting, finally, this paper tested robustness about the method, and experimental results show that by using this method extracting accuracy is high and strong robustness.

Reserearch Hotsports

Considering the similarity of watermarking system and communication system, watermarking problem is similar to a communication problem (communication model as shown in "Fig. 3")

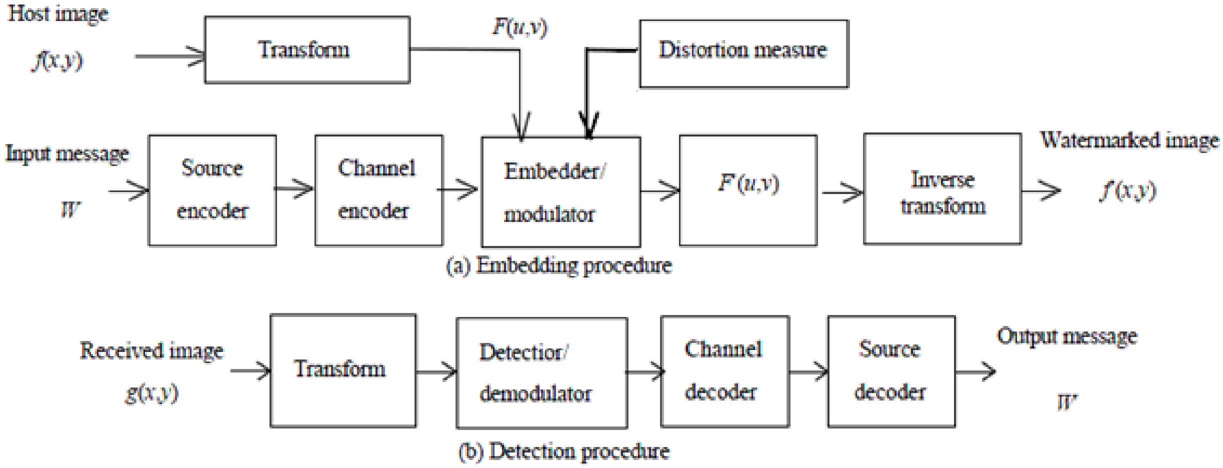


Figure 3. General communications model for digital watermarking

So it improves robustness of watermark system using the digital communication principle and method. Some scholars apply it to the watermark algorithm (error-correcting code has been applied include: BCH codes, convolutional codes, RS codes, Turbo Codes, LDPC codes, etc.)

However, watermark is placed restrictions on imperceptible nature and has a balance between length and intensity of the watermark bit. In addition, the watermark has a higher error rate (0.1 to 0.5). As a result, there are the following questions: what circumstances, error correction code would improve the robustness of the watermark? Which kind of coding is the most suitable? Rate should be how to choose?

To solve these problems, some scholars studied. Huang etc. compared the repetition code, BCH code and related test performance. Zinger etc. investigated performance of linear block codes watermark channel, given optimal coding strategy. Baudry etc. studied the watermark channel BCH code, repetition code and the performance of convolutional codes. Balado etc. project Turbo code scheme for improving the robustness of the watermark which is more effective, as long as the use of adequate low bit rate, its performance of cutting attacks is as good as or better than the spread spectrum scheme. Desset etc. regard the watermark-channel as high-noise channel (bit error rate: 0.1to0.5), by analysis the BCH code and repetition code error rate distribution, and give the optimal repetition code error rate interval. Some of these studies answer the above questions. This paper will study the application of linear block error-correcting codes in binary watermark image.

Algorithm of Embedding Watermark

Error-correcting Coding Theory. In this paper, watermark image is a binary watermark; the value of binary is 0 or1, in order to correcting the mistake in the communication process, using error-correcting code to achieve the goal. If it correct one mistake at the receive end, we can use linear block error-correcting code (3, 1).

Linear block code (3,1) can be defined as coding theory, assuming linear block code (3,1) is a0,a1,a2, with s1, s2and s3 show syndrome in three supervisory relationship, then, the value of s1, s2 and s3 location of fault codes correspondence can be provided as listed in the table I. Can be seen from the table provided, we can also correspond to the provisions of another relationship, this does not affect the general discussion.

Table 1 Relationship of Corrector and Mistake Position

S_0	S_1	S_2	Mistake position
1	1	0	a0
1	0	1	a1
0	1	1	a2
0	0	0	No mistake

When one mistake is at a0, a1, s1is 1, otherwise is 0, it mean that a0 and a1 compose even supervision relationship

$$s_1 = a_0 \oplus a_1 \tag{1}$$

The same argument, a0, a2 compose even supervision relationship

$$s_2 = a_0 \oplus a_2 \tag{2}$$

And a1, a2 compose even supervision relationship

$$s_3 = a_1 \oplus a_2 \tag{3}$$

In sending coding, for watermark image is binary image, the value of binary is 0 or1, it code 0 to 000, and 1to 111, correct coding make s_1, s_2 and s_3 of 0.

$$\begin{cases} a_0 \oplus a_1 = 0 \\ a_0 \oplus a_2 = 0 \\ a_1 \oplus a_2 = 0 \end{cases} \tag{4}$$

In the receive end, by Eq.1~4 calculate s_1, s_2 and s_3 then based on table to judge mistake and finding mistake to correct.

Embeding and Detection. Assumed the binary watermark image matrix is denoted by $W = \{w(x, y), 1 \le x \ge M, 1 \le y \le M\}$; The original image is $F = \{f(x, y), 1 \le x \ge M, 1 \le y \le M\}$. $w(x, y)$ is pixel value of binary watermark image , $f(x, y)$is pixel value of original image. Taking into account the watermark robustness and imperceptibly, we embed the watermark into the image of L-class sub-diagram approximation coefficient. And by modifying the coefficient of the fractional part of the sub-graph to embed watermark to ensure that wavelet coefficient does not cause a big change.

Large number pixel values of the watermark is excellent value, the corresponding pixel values of pixels called Merit pixels, the other is inferior to the value of the watermark, the value of the corresponding is bad pixel[15]. To statistics Watermark pixel before embedding the watermark , find the Merit value of the pixels, and then the corresponding pixel vector of wavelet coefficients was modified to decimals, so that the modified coefficient between the poor value of the pixel corresponding to the wavelet coefficients modify the vector to an integer. The Under the threshold and the upper threshold is called dc1 and dc2 is the threshold distance. Obviously, the vector do not been changed, in which the scope of the original value of fractional part of the wavelet coefficients. Merit pixels of the watermark greater the larger not need to modify proportion of the wavelet coefficients;

another greater of threshold distance, the need to modify the wavelet coefficients of the smaller proportion of the embedded watermark vector smaller degree of decline in visual quality. However, if is larger value will reduce accuracy of watermark extraction which led to decreased stability so adjusted according to actual needs values is necessary.

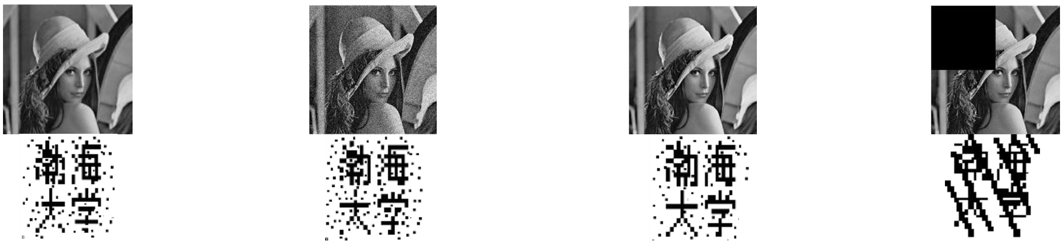
Expermental Results

In this paper, doing experiment with the watermark carrier Lena image 512×512 Bits of Lena of gray image and binary watermark image of 32×32Bits. This paper analyzed the distortion of watermark embedding process by Subjective observation and PSNR value, evaluated quality of the extracted watermark by subjective observation of watermark. Table 2, first calculates the threshold range corresponding to PSNR values of Carrier image watermark.

Table 2 The PSNR Value of the Different Region

Threshold	PSNR
[0.25,0.75]	39.6163
[0.30,0.90]	39.6578
[0.10,0.80]	39.823 4
[0.15,0.85]	40.201 8
[0.20,0.80]	40.302 1
[0.25,0.85]	40.118 8

a) JPEG compression:JPEG compression is the most familiar operation of the image management.Any unauthorized coding compressing images are correlativity exists and the redundant information. The experiment show as Fig. 4 (a).
b) Guass noise attacking:Guass noise attacking is the familiar attacking of the image management.The experiment show as Fig. 4 (b).
c) Filter attacking :The experiment show as Fig. 4 (c).
d) Cutting attacking:The experiment show as Fig. 4 (d).



(a) JPEG Compression (b) Gauss Noise Attacking (c) Median Filter Attacking (d) Cutting Attacking

Figure 4. JPEG compression, Gauss noise attacking, Median filter attacking and Cutting attack experiment

Conclusions

Using error-correcting coding the binary image watermark is processed before embedded into wavelet transform of the original gray image. The experimental results show that the proposed scheme is robust against popular attacks. Because the algorithm is easier, the watermark can be blind detected.

References

[1] S. Yin, X. Li, H. Gao, O. Kaynak, Data-based techniques focused on modern industry: An overview, IEEE Transactions on Industrial Electronics,62(1):657-667, 2015.

[2] S. Yin, Z. Huang, Performance monitoring for vehicle suspension system via fuzzy positivistic C-means clustering based on accelerometer measurements, IEEE/ASME Transactions on Mechatronics, 20(5):2613-2620, 2015.

[3] Yu Min, Chen Jun; Application Research of Computers, vol.33(2016)No.9

[4] S. Yin, X. Zhu,?Intelligent particle filter and its application on fault detection of nonlinear system, IEEE Transactions on Industrial Electronics, 62(6):3852-3861, 2015

[5] Chi Xiao-fang, Feng Gui; Dong Xiao-hui: Journal of Huaqiao University(Natural Science),Vol.36(2015)No.5,p.534

[6] S. Yin, X. Zhu, O. Kaynak, Improved PLS focused on key performance indictor related fault diagnosis, IEEE Transactions on Industrial Electronics, 62(3):1651-1658, 2015.

[7] Chen G, Ma H J, Chen N. A blind watermarking algorithm based on singular value decomposition and quantization[C] Proc. of the 10th World Congress on Intelligent Control and Automation. 2012: 4887-4890

[8] S. Yin, O. Kaynak, Big data for modern industry: challenges and trends, Proceedings of the IEEE, 102(3):143-146, 2015.

[9] Singh C, Ranade S K. Rotation invariant moments and transforms for geometrically invariant image watermarking [J]. Journal of Electronic Imaging, 2013, 22(1): 13-34.

[10] Tsougenis E D, Papakostas G A, Koulouriotis D E, et al. Performance evaluation of moment based watermarking methods: a review [J]. Journal of Systems and Software, 2012, 85(8): 1864-1884.