

# Digital Image Watermarking Based on Mixed Error Correcting Code

Yonghong Chen, Jiancong Chen

College of Computer Science & Technology, Huaqiao University, Xiamen, China.  
Email: djandcyh@163.com

Received September 1, 2011; revised February 10, 2012; accepted March 5, 2012

## ABSTRACT

In this paper, we present a novel technique based on a mixed Error Correcting Code (ECC)—the convolutional code and the repetition code to enhance the robustness of the embedded watermark. Before embedding, the binary watermark is scanned to one-dimension sequence and later inputted into the (3, 1, 2) convolutional encoder and (3, 1) repetition encoder frame by frame, which will improve the error correcting capability of decoder. The output code sequence is scanned to some matrixes as the new watermark messages. The watermarking is selected in low frequency band of the Discrete Wavelet Transform (DWT) and therefore it can resist the destruction of image processing. Experimental results are presented to demonstrate that the robustness of a watermark with mixed ECC is much higher than the traditional one just with repetition coding while suffering JPEG lossy compression, salt and pepper noise and center cutting processing.

**Keywords:** Error Correcting Code; Discrete Wavelet Transform; Mixed ECC; Watermarking

## 1. Introduction

The rapid expansion of the Internet and overall development of digital technologies in the past years introduces a new set of challenging problems regarding security. One of the significant problems is to prevent unauthorized copying of digital production from distribution. Digital watermarking has provided a powerful way to claim intellectual protection. Watermark must have two most important properties: transparency and robustness. Transparency refers to the perceptual quality of the watermarked data. The watermark should be invisible over all types. Robustness is a most important property of watermark. It means that the watermark is still presented in the image and can be detected after distortion. Ideally, the amount of image distortion necessary to degrade the desired image quality should destruct and remove the watermark in the traditional watermarking without ECC. So it is need to enhance the robustness of the embedded watermark by introducing the ECC, which can control the mistake and improve the reliability of data transmission in digital communication. With ECC appending some redundancy bits in the original embedded watermark, the error part of the extracted watermark can be corrected [1-12].

In this paper a digital image watermarking method based on mixed Error Correcting Code is presented. The main work is to encode the watermark with mixed ECC before embedding. (3, 1, 2) convolutional encoder is selected to encode the binary watermark sequence inputted by frames into some code sequences, among which the

hamming distances weight are heavy. Before being embedded in DWT domain as new watermark messages, the code sequences are encoded once more with repetition coding. This processing can add more redundancy among codes and increase the error correcting capability of decoder. In fact, the convolutional encoder is used to enlarge the hamming distance among message blocks. The error correcting capability is depended on the code distance. At the point of being free from the errors resulting from some destructions, the heavy code distance is always expected, because that the minimum distance means the worst situation in code blocks. The detection method of decoder is maximum likelihood method based on minimum distance principle. In our experiments, the results show that the proposed technique gives a larger error correcting extent and can recover the lost messages as more as possible against the JPEG lossy compression, salt and pepper noise and center cutting processing. When same degree of invisibility is maintained, the watermarking with mixed ECC offers a higher degree of robustness than the one just with repetition coding.

In the signal channel, watermark can be treated as a transmitted signal, while the destruction from attackers is regarded as a noisy distortion in channel. According to the viewpoint mentioned above, we provide an idea using ECC to detect and correct the error part of the extracted watermark. The organization of this paper is as follows. Section 2 presents the coding principle of Convolutional Code. Section 3 presents the characteristic of Convolu-

tional Codes and the decoding principle. Section 4 describes the watermark insertion and extraction. Experimental results and discussions are given in Section 5 and conclusions are drawn in Section 6.

## 2. The Coding Principle of Convolutional Code

Convolutional encoder is a finite memory system. When it works, the input message sequence is divided into some k-length message blocks. The encoder, for every message block, will product (n-k) detecting elements and form an n-length code block, named subcode. At some-time, these (n-k) detecting elements have a relation not only with k message letters in its subcode, but also with

$$\text{where } A = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & \dots \\ & & & & & & & & & 1 & 1 & 1 & 0 & 1 & 0 & \dots \\ & & & & & & & & & & & & 0 & 0 & 0 & \dots \\ & & & & & & & & & & & & & 0 & 0 & 0 & \dots \\ & & & & & & & & & & & & & & \dots & \dots & \dots & \dots \end{bmatrix}$$

The generator matrix  $G_{\infty}$  of (3, 1, 2) convolutional encoder is a semi-unlimited matrix, in which rows and lines are countless. In  $G_{\infty}$ , the later row is just a result from the former one's right moving for 3 steps. So  $G_{\infty}$  can be absolutely defined by the first row  $g_{\infty}$ . And in  $g_{\infty}$ , only 3 blocks are nonzero. The number 3(=m + 1) means the constraint degree in encoder. As  $k \times n$  generator submatrixes,  $g_0, g_1, g_2$  represent the nonzero blocks,  $g_0 = [111], g_1 = [010], g_2 = [001]$ . You will see that  $G_{\infty}$  can be obtained only all these generator submatrixes are known.

When the encoding is in process, the whole message sequence is not inputted into the encoder once a time. To increase the speed in decoding, it need introduce the time-delay. The message sequence M will be sent into encoder by frames and each frame contains L message blocks.

## 3. Characteristic and Decoding Principle of Convolutional Code

The performance of convolutional code lies on code distance and decoding method. The code distance is itself an attribute of convolutional code and determines the potential error correcting capability. And decoding method is a way that how to transform this potential error correcting capability into the practical one. Now, let  $C_1$  and  $C_2$  denote two different binary block sections which are randomly outputted from same  $G_{\infty}$ . Code distance is actually the hamming distance weight after binary addition of corresponding code letters in  $C_1$  and  $C_2$ . Owing to the closeness of linear convolutional code, if  $C_1 + C_2 = C$ ,

m message letters prior to them. Convolutional code is written to be (n, k, m)-form as to emphasize three most important parameters, k represents the message bit, n the code length, k/n the code rate, m the coding storage or storage cycle of message blocks in encoder.

Here, convolutional coding is described with matrix, continuing the way of Linear Block Code. The (3, 1, 2) convolutional encoder is used as an example to perform the proposed technique. Let  $M(=[m_0, m_1, m_2, \dots, m_i, \dots])$  and  $c(=[p_{01}, p_{02}, m_1, p_{11}, p_{12}, m_2, p_{21}, p_{22}, m_3, p_{31}, p_{32}, \dots])$  denote the endless input message sequence and the output code sequence, respectively. (3, 1, 2) convolutional encoder is designed as follows:

$$c = [m_0 \ m_1 \ m_2, \dots, m_i, \dots] \times A = M \times G_{\infty} \quad (1)$$

then C is also one of the output block sections. The rule can be generally described as:

$$d(C_1, C_2) = W(C_1 + C_2) = W(C) = W(C + 0) = d(C, 0) \quad (2)$$

It had been shown that code distance of two random sequences is equivalent to hamming distance weight between some sequence and all-zero one. The error correcting capability of decoder lies on the minimum distance among the output sequences. As usual, maximum likelihood decoding is exactly the minimum distance decoding which becomes equivalent to finding the least-metric (shortest) path.

For any output coded frame, there is always an original unique one corresponding to it. But in decoder, once the error occurs in transmission or storage, the input received frame is a specious and intermittent sequence, just a reference for decoding, not the original one. The performance of maximum likelihood decoding is described as follows: Compute all the hamming distances between the received frame sequence and every original one. Choose an original sequence corresponding the minimum hamming distance as the output estimated value. In (3, 1, 2) convolutional encoder,  $k = 1$ , we let  $L = 8$ , and there are  $2^{kL} = 256$  original sequences, named block sections, for detection. Generally speaking, maximum likelihood decoding does not mean to compare with the whole input code sequence. Instead, when receiving a frame, the decoder compares with all the block sections and chooses a most likelihood one, making the whole input code sequence corresponding to minimum distance in the end. It

need point out that maximum likelihood decoding has a regular recursive structure in decoder. Its complexity is proportional to the  $2^{km}$  shifting states in encoder, not  $L$  which only has a linear relation with the time used for decoding.

#### 4. Watermark Insertion and Extraction

Except for the convolutional coding stated above, we also introduce repetition code as other error correcting encoding technique. The rule of repetition coding is repeating each original signal of a watermark  $N$  times in block section, named block section  $(N, 1)$ . In the decoding process, we use the majority elements of the block section to reconstruct the original signal. For example, we set  $N = 5$  in the binary signal and the  $(000)$  represents 0, the  $(111)$  represents 1. In the decoding process, the reconstructed signal is "0" if the number of "0" is more than 2 in a block section; otherwise it is "1". The mixed combination of convolutional code and repetition code once more enhances the error correcting capability of decoder and gives a larger error correcting extent.

We use a gray image  $F$  in our experiment of which size is  $R_1 \times R_1$  in pixels as host image and the watermark  $W$  is a  $R_2 \times R_2$  binary image. And  $R_1 \times R_1 / (2R_2 \times 2R_2 \times n \times N)$  is acquired to be a integer. The main steps of the watermark embedding procedure based on mixed ECC are presented here.

1) Divide  $F$  into  $2R_1 \times 2R_1$  blocks and a subblock sequence  $B(= B_1, B_2, \dots, B_k)$  is obtained. According to the degree of texture complexity,  $B$  is arranged to  $B'(= B_{a1}, B_{a2}, \dots, B_{ak})$ ,  $B_{a1} \leq B_{a2} \leq \dots \leq B_{ak}$ . In  $B'$ , the anterior  $(n \times N)$  subblocks are chose for embedding with code message.

2) Scan  $W$  into a  $R_2 \times R_2$ -length message sequence  $M$ . Divided  $M$  into some  $k$ -length message blocks. Every  $L$  message blocks as a frame are sent into  $(n, k, m)$  convolutional encoder.  $c$  denotes the whole output code sequence, of which length is  $n \times R_2 \times R_2$ .

3) Scan  $c$  into  $n$   $R_2 \times R_2$  matrixes as the code message matrixes  $(W_1, W_2, \dots, W_n)$ . Then repeat each matrix of code messages  $N$  times and orderly embed these coded matrixes into the chosen subblocks for an invisible watermarking. The way of pixel-to-pixel embedding is commonly used. The addition rule can be generally described as:

$$B_i' = \text{IWDWT} \left[ (W_j + \beta \times B_{iLxy}) \oplus B_{iHxy} \right] \quad (3)$$

where  $\beta$  represents the set of parameter of the embedder,  $B_{iLxy}$  the low frequency subband,  $B_{iHxy}$  the high frequency subbands at scale 1.  $W_j$  and  $B_i'$  refer to one of coded matrixes and one watermarked subblock, respectively.

With an access to the original unwatermarked image  $F$  and generator matrix  $G_{\infty}$ , the steps of watermark extrac-

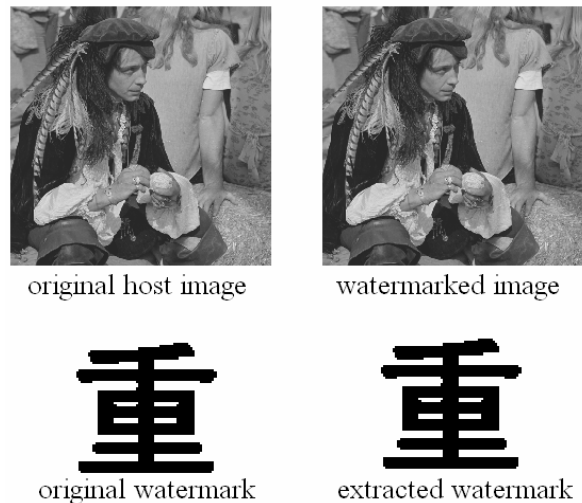
tion are reverse processing of insertion. When extracting, the key step will be how to effectively decode. As to repetition decoding, the  $N$  multiple extracted messages are constructed to one multiple code message matrixes  $(W_1, W_2, \dots, W_n)$  according to principle of the fraction obeying the majority. The work of convolutional decoding is to search out the most likelihood block sections for each received frame in decoder. The  $n$  message matrixes are scanned to a one-dimension sequence which is constituted by some frames. According to maximum-likelihood-decoding principle, compare with block sections and choose the most likelihood one for each frame. At last, link all the most likelihood block sections back to the code sequence  $c$  which will be returned to the original message sequence  $M$ .

#### 5. Experimental Results and Discussions

The  $512 \times 512$  gray host image and the  $64 \times 64$  binary watermark are shown in **Figure 1**.  $(3, 1, 2)$  convolutional code and  $(3, 1)$  repetition code are combined to be mixed ECC,  $L$  and  $\beta$  are set to 8 and 7, respectively. We have obtained PSNR of 44.0259 dB. Experimental result shows clearly that the watermarked image is not perceptually different from the original one.

##### 5.1. Robustness in Image Distortion

In order to verify the capacity of the mixed ECC technique, we have watermarked image suffer some attacks and make sure our technique is able to detect and correct the error part of the extracted watermark. We find that the mixed ECC is robust to lower quality JPEG compression, salt-and pepper noise and center cutting processing (see **Figure 2**). So the result demonstrates an important aspect of mixed ECC is its adequate error correcting capability only if the attacked image becomes valueless. (a)



**Figure 1. Experimental result.**

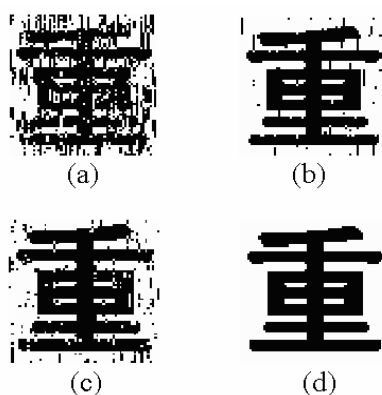


Figure 2. The extracted watermark.

multiplicative noise with density-0.01, NC = 0.7878; (b) salt-and-pepper noise with density-0.05, NC = 0.9722; (c) JPEG lossy compression with quality-50%, NC = 0.9419; (d) center cutting with size-200 × 200, some watermark messages are abandoned, NC = 1.

It can be also found from the experiment that the mixed ECC specially grants a higher degree of robustness to watermark therefore able to resist the JPEG lossy compression, salt-and pepper noise and center cutting processing while the watermarking with and without ECC have little difference in PSNR. Even if the watermarked image is tampered seriously, the mixed ECC technique can correct the error parts as more as possible and maintain the extracted watermark easy to be identified. Figures 3, 4 and 5 show the results graphically for easily distinguishing the differences between two techniques. So we are sure that the watermarking with mixed ECC is much better than the one only with repetition coding.

Figure 3 shows for us that even though when the JPEG qualities are smaller than 20, the quality of the extracted watermark can still provide a certification of the owner. However, when the JPEG quality downs to 40 or more below, the watermarked image is strictly destroyed and commercially valueless. And Figure 4 also reveals the prominent advantage of using mixed ECC technique. Considering that the different embedding positions for different host images, Figure 5 just demonstrates that the mixed ECC can recover all the lost watermark messages at a certain correcting extent. In summary, the pretreatment done to watermark using mixed ECC actually exchanges robustness of watermark with increasing the message redundancy. In this paper, we obtain the expected effect when applying the Error Correcting Code to watermarking.

### 5.2. Transparency of the Embedded Watermark

To verify the stability of transparency, the test is performed on another 99 different images as original signals. The

results shown in Figure 6 verify that the proposed scheme has good and stable transparency.

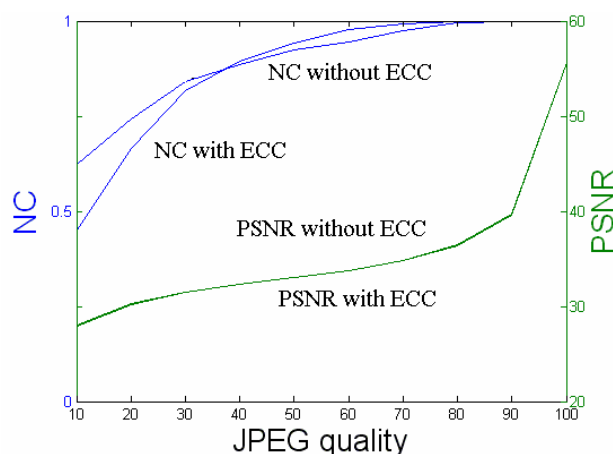


Figure 3. PSNR and NC of watermarking with two techniques under different JPEG qualities.

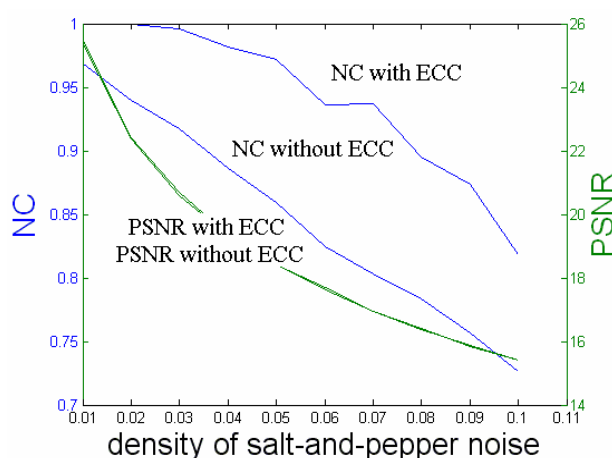


Figure 4. PSNR and NC of watermarking with two techniques under salt-and-pepper noise.

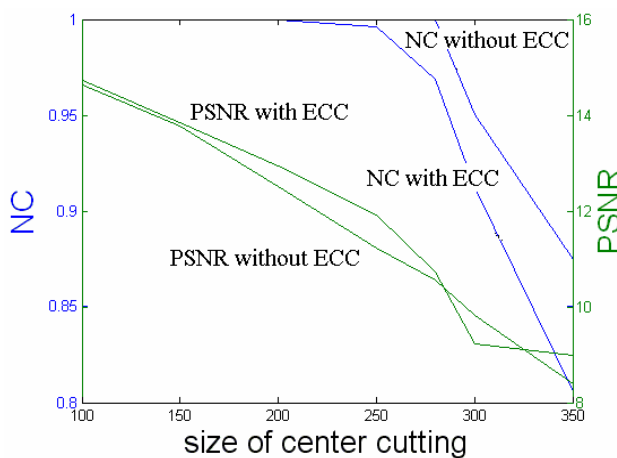


Figure 5. PSNR and NC of watermarking with two techniques under different center cutting sizes.

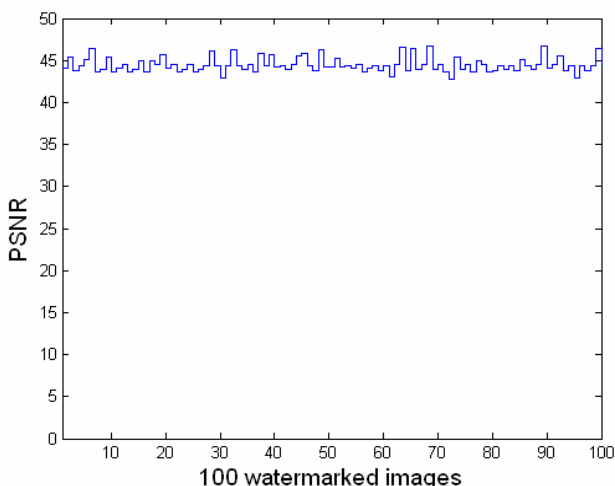


Figure 6. Transparency test results of 100 original images.

### 5.3. Security of the Embedded Watermark

The bit-error-rate (BER) is employed to measure the robustness of the proposed algorithm.

$$BER = \left( \sum_{i=1}^P \sum_{j=1}^Q |W(i,j) - W^*(i,j)| \right) / (P \times Q) \quad (4)$$

where  $P \times Q$  is the size of image.

Figure 7 shows the detection of the watermark to 100 random watermarks, among which there is only one matching the watermark we actually insert and detection BER is 0.

### 5.4. Comparing with Other ECC

We use two ECC algorithms and our mixed ECC algorithm in experiments:

1) Interlaced coding together with repetition 9 times coding: The encoded watermark is 9 multiple of the original watermark respectively (Mixed-Interlaced coding).

2) (7, 3) Cyclic redundancy check coding with repetition 4 times coding: The encoded watermark is probably 9 multiple of the original watermark respectively (Mixed-CRC coding).

We demonstrate the JPEG compression of the watermarked images with different JPEG qualities. Figure 8 shows the results graphically for easily distinguishing the differences between various ECC algorithms. Even though when the JPEG qualities are smaller than 30, the NC of our algorithm are highest to other two ECC algorithms. So is the cutting attack. See Figure 9.

## 6. Conclusion

In this paper, we propose an idea to enhance the robustness of the watermark using the mixed ECC technique. The main work is to encode the watermark with (3, 1, 2) convolutional encoder and (3, 1) repetition encoder before

embedding. The convolutional coding is introduced to automatically take maximum advantage of the interrelation

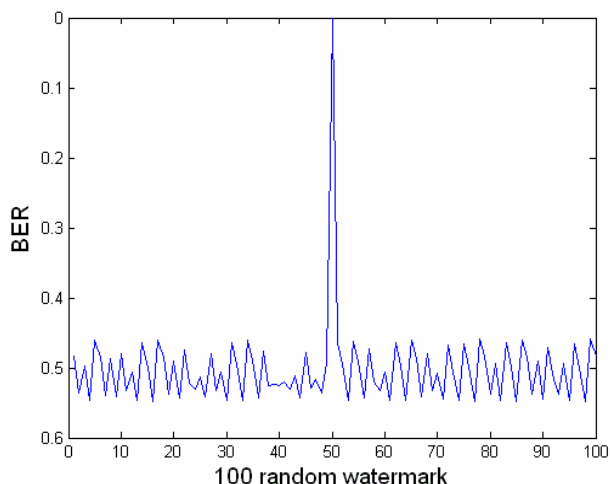


Figure 7. BER of watermark detection to 100 random watermarks.

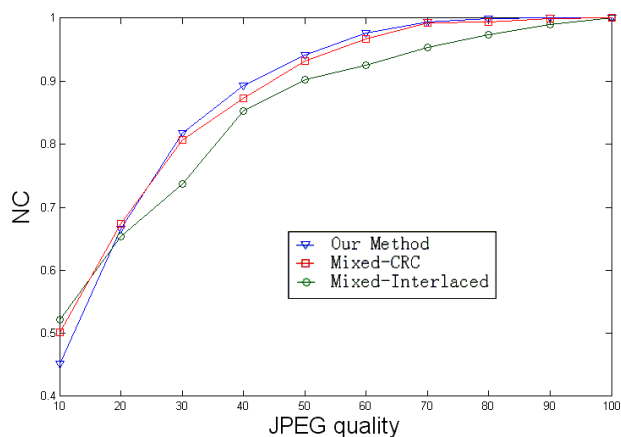


Figure 8. NC of watermarking with various ECC algorithms under different JPEG qualities.

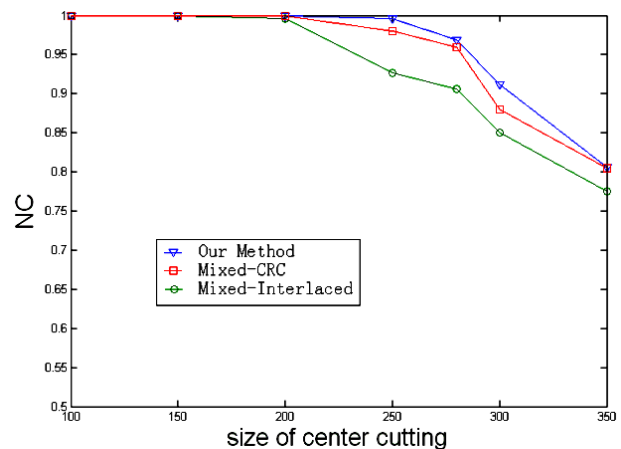


Figure 9. NC of watermarking with various ECC algorithms under different size of cutting attack.

of message blocks, among which the hamming distances will be enlarged therefore resulting convenient for decoding. Furthermore, the joining of the repetition coding can increase more message redundancy, once more enhancing the error correcting capability. After encoding, the output code sequence representing the watermark is invisibly embedded into low frequency bands of some subblocks in host image. Experimental results have confirmed that the mixed ECC based watermarking will have the property that corrects errors of the extracted watermark automatically. With the characteristic of mixed ECC, the robustness of a watermark with ECC is relatively higher than the traditional one just with repetition coding. The coded watermark can survive the lower quality JPEG compression, various salt-and-pepper noise and center cutting processing and maintain a better visual quality of the extracted watermark. Further research will focus on the development of robust watermarking methods with more powerful error correcting capability technique.

## 7. Acknowledgements

This work is supported by Huaqiao University Science and Technology Foundation (No. 10Y0199) and the Fundamental Research Funds for the Central Universities (No. JB-ZR1131), the Project-sponsored by SRF for ROCS, SEM, and the Natural Science Foundation of Fujian Province of China (No. 2011J05151), Natural Science Foundation Project of Chongqing (No. CSTC, 2008BB2070).

## REFERENCES

- [1] C.-H. Huang and J.-L. Wu, "Attacking Visible WaterMarking Schemes," *IEEE Transactions on Multimedia*, Vol. 6, No. 1, 2004, pp. 16-30. [doi:10.1109/TMM.2003.819579](https://doi.org/10.1109/TMM.2003.819579)
- [2] J. Tian, "Wavelet-Based Reversible Watermarking for Authentication," *Proceedings of SPIE Security and Watermarking of Multimedia Contents III*, San Jose, 21 January 2002, pp. 679-690. [doi:10.1117/12.465329](https://doi.org/10.1117/12.465329)
- [3] D. M. Thodi and J. J. Rodriguez, "Prediction-Error-Based Reversible Watermarking," *Proceedings of the International Conference on Image Processing of the IEEE ICIP*, 24-27 October 2004, pp. 1549-1552. [doi:10.1109/ICIP.2004.1421361](https://doi.org/10.1109/ICIP.2004.1421361)
- [4] I. J. Cox and M. L. Miller, "The First 50 Years of Electronic Watermarking," *Journal of Applied Signal Processing*, Vol. 56, No. 2, 2002, pp. 126-132.
- [5] D. M. Thodi and J. J. Rodriguez, "Expansion Embedding Techniques for Reversible Watermarking," *IEEE Transactions on Image Processing*, Vol. 16, No. 3, 2007, pp. 721-730. [doi:10.1109/TIP.2006.891046](https://doi.org/10.1109/TIP.2006.891046)
- [6] Y. J. Hu, S. Kwong and J. W. Huang, "An Algorithm for Removable Visible Watermarking," *IEEE Transactions on Circuits Systems for Video Technology*, Vol. 16, No. 1, 2006, pp. 129-133. [doi:10.1109/TCSVT.2005.858742](https://doi.org/10.1109/TCSVT.2005.858742)
- [7] C. I. Podilchuk and E. J. Delp, "Digital Watermarking: Algorithms and Applications," *IEEE Signal Processing Magazine*, Vol. 18, No. 4, 2001, pp. 33-46. [doi:10.1109/79.939835](https://doi.org/10.1109/79.939835)
- [8] M. U. Celik, G. Sharma and A. M. Tekalp, "Lossless Watermarking for Image Authentication: A New Framework and an Implementation," *IEEE Transactions on Image Processing*, Vol. 15, No. 4, 2006, pp. 1042-1049. [doi:10.1109/TCP.2005.863053](https://doi.org/10.1109/TCP.2005.863053)
- [9] A. van Leest, M. van der Veen and F. Bruekers, "Reversible Image Watermarking," *Proceedings of the International Conference on Image Processing*, Barcelona, 14-17 September 2003, pp. 731-734. [doi:10.1109/ICIP.2003.1246784](https://doi.org/10.1109/ICIP.2003.1246784)
- [10] M. Barni, F. Bartolini and A. Piva, "Improved Wavelet-Based Watermarking through Pixel-Wise Masking," *IEEE Transactions on Image Processing*, Vol. 10, No. 5, 2001, pp.783-791. [doi:10.1109/83.918570](https://doi.org/10.1109/83.918570)
- [11] J. Yang, M. H. Lee, X. H. Chen, *et al.*, "Mixing Chaotic Watermarks for Embedding in Wavelet Transform domain," *Proceedings of IEEE International Symposium on Circuits and Systems*, New York, 26-29 May 2002, pp. 668-671. [doi:10.1109/ISCAS.2002.1011441](https://doi.org/10.1109/ISCAS.2002.1011441)
- [12] K.-X. Yi, J.-Y. Shi and X. Sun, "Digital Watermarking Techniques: An Introductory Revive," *Journal of Image Graphics*, Vol. 6, No. 2, 2001, pp. 111-117.