Intra-Block Max-Min Algorithm for Embedding Robust Digital Watermark into Images*

F.Y. Duan[1], I. King[2], L.W. Chan[2], and L. Xu[2]

[1] Institute of Information Science
Wuyi University
Jiangmen, Guangdong, China 529020
fyduan@letterbox.wyu.edu.cn

[2] Department of Computer Science & Engineering
The Chinese University of Hong Kong
Shatin, N.T., Hong Kong, China
{king,lwchan,lxu}@cse.cuhk.edu.hk

Abstract. We present a new DCT-based block max-min algorithm for digital watermark embedding in images. Our algorithm uses intra-block bordering upon pixels relations to generate the watermarked image. The features of our method to embed the watermark are: (1) the watermark is perceptually invisible; (2) low loss of relevant information of the original image; (3) the watermark can be read only by using a secret key; (4) the watermark is robust against translation and area cropping; and (5) retrieval of embedded watermark does not need the original image. We describe the algorithm framework and its performance against translation and area cropping with experiments.

1 Introduction

Digital watermarking is becoming increasingly popular and important as users seek ways to protect their proprietary information being transmitted over the Internet. Digital watermarking is useful in the authentication of multimedia information such as text, sound, image, and video, to ensure the undisputed proof of ownership on copyrighted materials. It is one of the better ways to protect intellectual property from illicit copying [17].

The digital watermarking is not unlike image coding when an *original signal* is embedded with the *watermarking signal* with additional requirements depending on the applications. These requirements must guard against tempering of the watermarked signal. For example, the watermarking may resist geometric transformation, compression, and sampling to ensure that the watermarking signal can still be retrieved with a high degree of accuracy. Moreover, the watermark should be perceptually invisible to the viewer nor should the watermark degrade the quality of the content.

* This work is supported in part by RGC Earmarked Grant # CUHK4176/97E.

There are also other system issues to address when designing a suitable watermarking algorithm. For example, there is always the trade-off issue of the complexity of the algorithm and the computational resource required to achieve the result. In other words, although one may achieve a high degree of security with a watermarking algorithm, the computational cost to code and decode such a watermarking may be prohibitive. Hence, it is the goal in designing the watermarking algorithm to have a suitable technique which satisfies many of the requirements with good real-time performance.

2 Previous Work

There are many ways to perform information embedding in signals. Here we are interested mainly with digital images as the source signal. There are two main classes of watermarking techniques: visible [9] and perceptually invisible [1, 3, 4, 6, 7, 10, 11, 12, 13]. The perceptually invisible watermarking techniques consist of both two-dimensional spatial watermarks [1, 3, 10, 11, 12, 13] and frequency domain watermark [4, 6, 7] while IBM has developed a proprietary visible watermark to protect images that are part of the digital Vatican library project [9].

One early watermarking method obtains a checksum of the image data, then embeds the checksum into the least significant bits(LSB) of randomly chosen pixels for watermarking [14]. Others have added a maximal length linear shift register sequence to the pixel data and identified the watermark by computing the spatial cross-correlation function of the sequence and the watermarked image [10, 15, 16]. Watermarks also can modify the image's spectral or transform coefficients directly. These algorithms often modulate DCT coefficients according to a sequence known only to the owner [4, 8]. A straightforward technique is proposed to gray scale images by adding a watermark image to the original image [1, 10]. Watermarks can be image dependent. For example, [5] uses independent visual channels for watermark embedding and [2] generated watermarked images by modulating JPEG coefficients. These watermarks are designed to be invisible, or to blend in with natural camera or scanner noise.

In [7], Hsu presented a DCT-based algorithm using inter-block relation to implement the middle-band embedding. First, the author used a fast two-dimensional pseudo-random number traversing method to permute the signature image. Second, the input image was divided into blocks of size 8×8, and then each block is DCT transformed. Third, Hsu chose the middle-band coefficients for watermark embedding. Then, a 2-D sub-block mask is used to compute the residual pattern from the chosen middle-band coefficients of inter-block. After the residual pattern is obtained, for each marked pixel of the permuted signature data he then modified the DCT coefficients according to the residual mask.

Our method is different from [7] in one major aspect. Instead of using inter-block relations, our algorithm uses intra-block relations to generate the watermarked image. Specifically, our method does not require the original image to extract the watermark. Hence, this method is less cumbersome than other methods requiring the original image. From our experiments we found this method to be more robust against localized distortions since the size of the blocks is smaller and the blocks are closer together.

In Section 3, we present our new proposed watermarking algorithm. We then present our experimental results in Section 4. Discussion is presented in Section 5 and conclusion is found in Section 6.

3 Proposed Algorithm

3.1 Digital Watermark Embedding

Let OI and OW be the original grayscale image and the original binary digital watermark respectively. They are defined as,

$$OI = \{oi(i,j), 1 \leq i,j \leq N\}, oi(i,j) \in \{0, \cdots, L-1\}, \tag{1}$$

where L is the number of grayscale levels for the image.

$$OW = \{ow(i,j), 1 \leq i,j \leq N'\}, ow(i,j) \in \{0,1\}, \tag{2}$$

with $N' = N/4$ in our case.

Permutation of the Watermark Data A secret key $K(l)$ is a random permutation of the integers from 1 to N'^2. It is used to permute the watermark. The order is defined as,

$$K[(i-1) \times N' + j] - 1 \equiv i' \pmod{N'} + j' \tag{3}$$

then,

$$W'(i,j) = OW(i'+1, j'+1). \tag{4}$$

After this permutation step of the watermark data, we have a scrambled binary watermark data which can be used in the next step.

Block Transformation of the Image The image OI is divided into 8-by-8 blocks, $BOI_{m,n}$, and the two-dimensional Discrete Cosine Transform (DCT) is computed for each block using

$$D_{m,n} = DCT(BOI_{m,n}), \qquad 1 \leq m,n \leq M \tag{5}$$

$$= \{d_{m,n}(k,l), 1 \leq k,l \leq 8\} \tag{6}$$

with $M = N/8$ in our case.

Modification of DCT Coefficients The permuted watermark W' is also divided into $M \times M$ blocks $BW'_{m,n}$ with the block size 2-by-2.

When $BW'_{m,n}(i) = 1,\ 1 \leq i \leq 4$, we perform an exchange of the K_i^0 with maximum grayscale value among $K_i^0, ..., K_i^5$. When $BW'_{m,n}(i) = 0$, we perform an exchange of the K_i^0 with minimum grayscale value among $K_i^0, ..., K_i^5$.

After the modification of DCT on D, we obtain the modified D' which requires the inverse to compute the watermarked image.

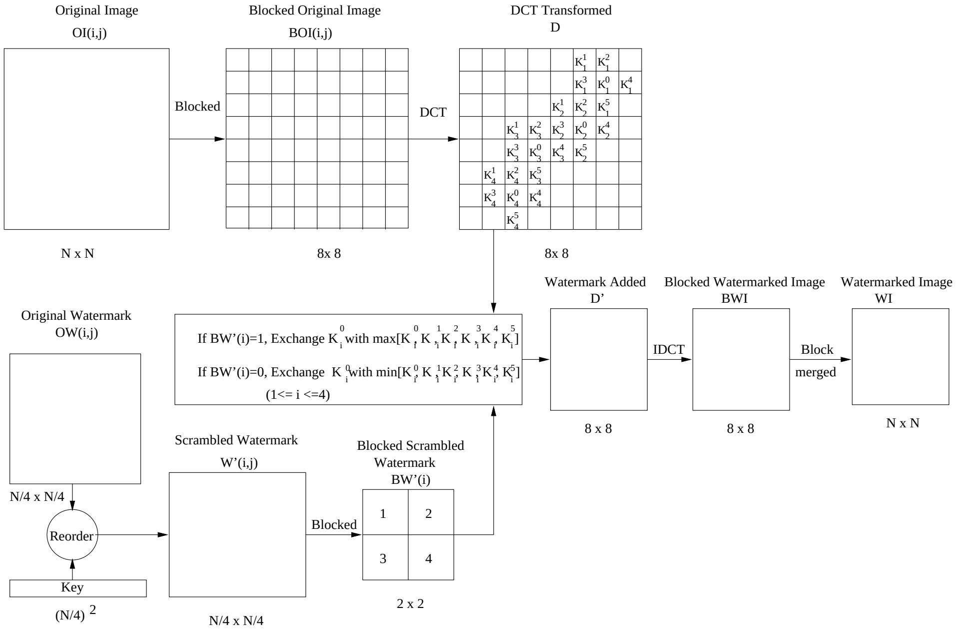


Fig. 1. The schematic of a general key-based watermarking process.

Inverse DCT We then calculate the inverse two-dimensional DCT of each block as,

$$BWI_{m,n} = IDCT(D'_{m,n}) \tag{7}$$

and then arrange the blocks back together in a single watermarked image. A schematic of the embedding watermark to image process is illustrated in Fig. 1.

3.2 Extracting Method

The extraction of watermark EW requires the test image TI and the key sequence K, without needing the original image. The schematic of extracting watermark process is shown in Fig. 2. The extraction steps are as follow:

Block Transformation The test image is divided into $M \times M$ block $BTI_{m,n}$ with the block size 8-by-8. Each block is DCT transformed.

$$D1_{m,n} = DCT(BTI_{m,n}) \tag{8}$$

Extracting the Permuted Watermark

$$BW1(i) = \begin{cases} 1 & K_i^0 > median[K_i^1, K_i^2, K_i^3, K_i^4, K_i^5], \\ 0 & \text{Otherwise.} \end{cases} \tag{9}$$

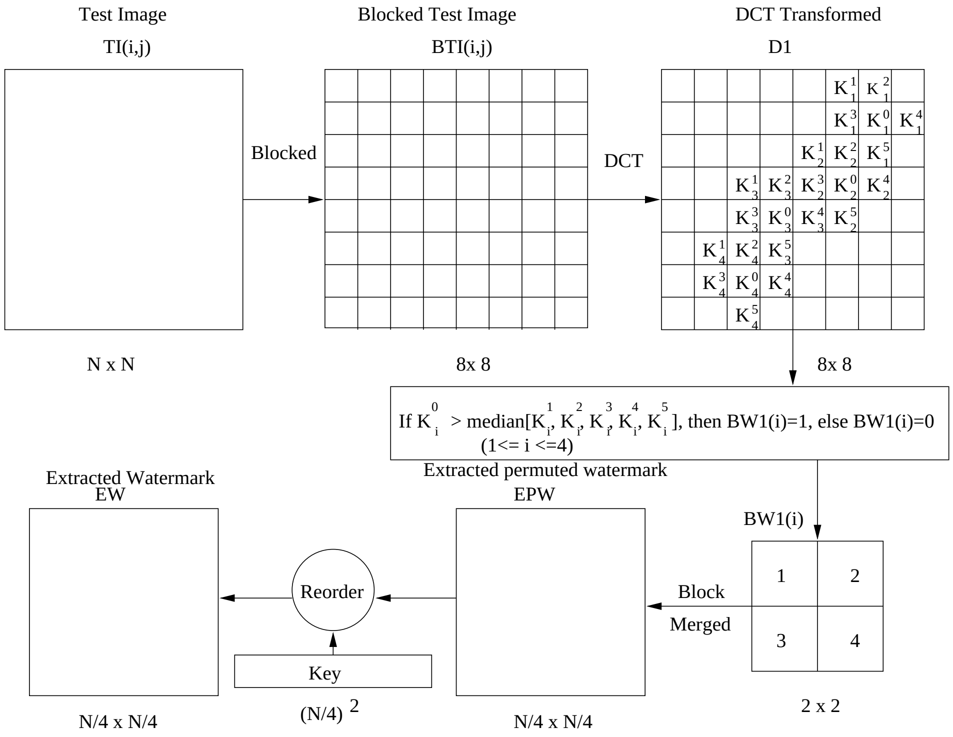


Fig. 2. The schematic of extracting watermark process.

where $1 \leq i \leq 4$, $K_i^0, K_i^1, K_i^2, K_i^3, K_i^4, K_i^5$.

We then arrange the blocks $BW1_{m,n}$ back together in a single extracted permuted watermark EPW. Finally, the extracted watermark EW is obtained by using of the follow equation.

$$EW(i'+1, j'+1) = EPW(i,j) \tag{10}$$

where the relation among i, j, i', j' meets Eq. (3). See also Fig. 2 for a more detailed schematic of the digital watermark extracting process.

4 Experiments

We perform two basic transformations: (1) translation and (2) cropping. The experiments were conducted on UltraSparc workstation with Matlab 5. The original image is a 256 level 256×256 grayscale image.

We defined the Average Intensity Error (AIE) when comparing the watermarked image with the original as,

$$\text{AIE} \equiv \frac{\sum |OI - WI|}{N \times N}. \tag{11}$$

Table 1. Values of the variables used in our experiment

Variable Name	Meaning	Variable Type	Value
OI	Original Image	matrix	256×256
WI	Watermarked Image	matrix	256×256
OW	Original Watermark	matrix	64×64
EW	Extracted Watermark	matrix	64×64
EW'	Extracted Watermark from Black Image	matrix	64×64
K	Key	vector	1×64^2
N		integer	256
N'		integer	64
M		integer	32
L		integer	8

We found that the AIE is approximately 11.9 using the watermarked image shown in Fig. 4(b). This result is quite acceptable since we cannot distinguish the original image and the watermarked image perceptually.

4.1 Translation

Using cropped watermarked image of same cropping sizes over different location of the watermarked image to extract watermark, we test our method's ability to recover watermark image under translation shift with the Relative Error Rate (RER) as the performance criterion:

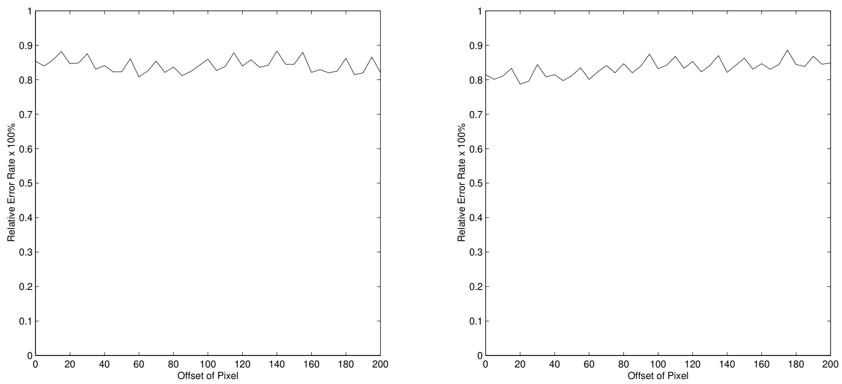
$$\begin{aligned} \mathrm{RER} &\equiv \frac{\sum |OW - EW|}{N' \times N'} \div \frac{\sum |OW - EW'|}{N' \times N'} \\ &= \frac{\sum |OW - EW|}{\sum |OW - EW'|} \times 100\%. \end{aligned} \tag{12}$$

where EW' means the extracted watermark from black image. The experimental results are shown in Fig. 3 for both horizontal and vertical translations.

Our method is translational invariant since there is no significant effect under translation with a constant size as shown in Fig. 3 when we used a cropping image of 50×230 selected horizontally and vertically. The error obtained is fairly similar which demonstrated that this method is robust against translation.

4.2 Cropping

Our experiments also showed that our method is sensitive to the size of the cropped area. The error is linear and inversely proportional to the size of the cropped areas as shown in Fig. 5. It is similar with one found in [6]. Here we varied the size of the cropped image from 100% (256×256) to 0.055% (11×11) with



(a) (b)

Fig. 3. We used a cropped image of 50×230 and translate it horizontally in (a) and vertically in (b).

the RER ranging from 1% to 100% respectively. Furthermore, we observed that when the RER is greater than 86.6% (the cropped image size is less than 14%) the retrieved watermark image cannot be distinguished with the original watermark perceptually. These results demonstrated that our proposed algorithm is more robust to the cropping than the ones proposed in [6, 7].

5 Discussion

The average retrieved watermark error per pixel is linear and inversely proportional to the percentage of cropping image. When the cropping image is around 14% of the original image, the retrieved watermark is illegible perceptually. Even when we used the whole watermarked original image without cropping, there is still an error arising from the DCT computation. This background error is about 0.1-0.2%. The condition of failure of the method is that the variation of the grayscale value of the original image is very small.

6 Conclusion

We present a new DCT-based block algorithm for watermark embedding in digital images. Its main advantages to [6, 7] are: (1) the watermark can be extracted without the original image and (2) its robustness against cropping and translation distortions. Instead using inter-block relations, our algorithm uses intrablock relations to generate the watermarked image. This method is more robust

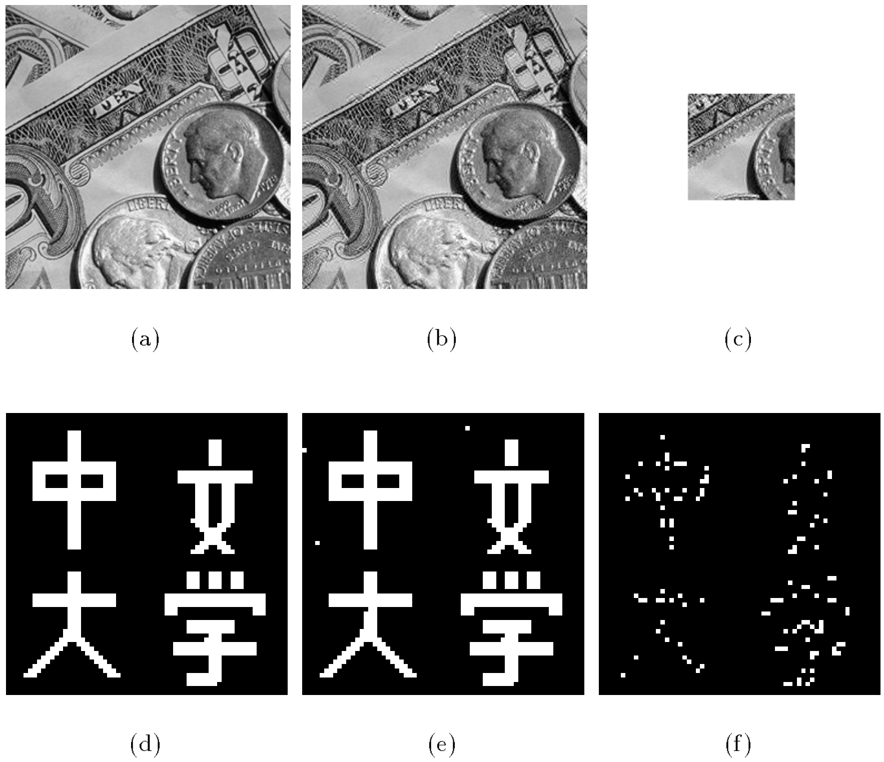


Fig. 4. (a) the original image, (b) the watermarked image, (c) the minimum size cropping watermarked image, (d) the original watermark , (e) the extracted watermark from (b), (f) a poor extracted watermark from (c) with RER of 86.6% using 14% of the image area from the watermarked image.

against localized distortions since the size of the blocks is smaller and the blocks are closer together.

In our experiments we added the watermark to the image by modifying the more perceptually significant components of the image spectrum. The difference between the original and the watermarked image is small. This result is quite acceptable since we can distinguish the original image and the watermarked image perceptually.

Our experiments showed that our method is sensitive to the size of the cropped area. The Relative Error Rate is linear and inversely proportional to the size of the cropped area. We observed that when the RER is greater than 86.6% (the cropped image size is less than 14%) the retrieved watermark cannot be distinguished with the original watermark perceptually. However, when the RER

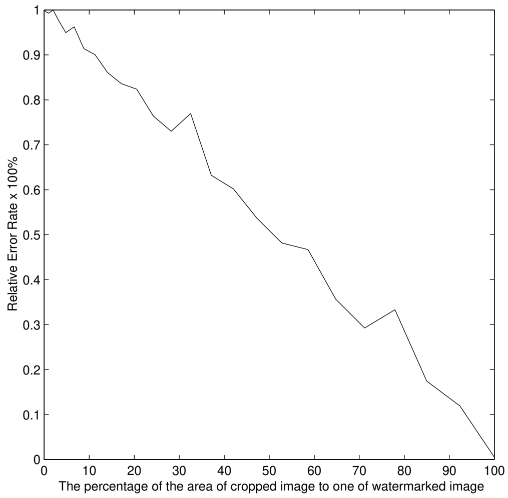


Fig. 5. We vary the size of the cropped image at the center of the image and found that the error is inversely proportional to the area of the cropped image.

is greater than 64.6% (the cropped image size is less than 37%) the retrieved watermark cannot be distinguished with the original watermark perceptually in [6].

The features of our method of embedding digital watermarks in images are as follow:

1. the watermark is perceptually invisible;
2. low loss of relevant information of original image;
3. the watermark can be read only by using a secret key;
4. the watermark is robust against translation and area cropping;
5. retrieval of embedded watermark does not need the original image.

References

1. W. Bender, D. Gruhl, N. Mormoto, and A. Lu. Techniques for data hiding. In *Proceedings of the SPIE*, San Jose CA, USA, February 1995.
2. F.M. Boland, J.J.K.O Ruanaidh, and C. Dautzenberg. Watermarking digital images for copyright protection. In *Proceedings of the International Conference on Image Processing and its Applications*, pages 321–326, Edinburgh, Scotland, July 1995.
3. G. Caronni. Assuring ownership rights for digital image. In *Proc. Reliable IT Systems*. VIS'95. Vieweg Publishing Company, 1995.
4. I.J. Cox, Joe Kilian, Tom Leighton, and Talal Shamoon. Secure spread spectrum watermarking for images audio and video. In *IEEE Int. Conf. on Image Processing*, volume 3, pages 243–246, Lausanne,Switzerland, September 1996.

5. J.F. Delaigle, C.De Vleeschouwer, and B. Macq. Digital watermarking. In *Proceedings of the IS & T/SPIE Conference on Optical Security and Counterfeit Deterrence Techniques*, volume 2659, pages 99–110, San Jose, CA, USA, Feb.1-2 1996.
6. F.Y. Duan, I. King, L.W. Chan, and L. Xu. Intra-block algorithm for digital watermarking. In *14th International Conference on Pattern Recognition (ICPR'98)*, Brisbane, Queensland., Australia, 17-20 August 1998.
7. C.T. Hsu and J.L. Wu. Hidden signatures in image. In *IEEE Int. Conf. on Image Processing*, volume 3, pages 223–226, Lausanne,Switzerland, September 1996.
8. E. Koch and J. Zhao. Towards robust and hidden image copyright labeling. In *Proceedings of the 1995 IEEE Workshop on Nonlinear Signal and Image Processing*, pages 452–455, Neos Marmaras, Greece, June 20-22 1995.
9. F. Mintzer, A. Cazes, F. Giordano, L. Lee, K. Magerlein, and F. Schiattarella. Capturing and preparing images of vatican library manuscripts for access via internet. In *Proceedings of the IS & T's 48th Annual Conference*, pages 74–77, Washington,DC, May 1995.
10. R.G.van Schyndel, A.Z. Tirkel, N.R.A. Mee, and C.F. Osborne. A digital watermark. In *Proceedings of the IEEE International Conference on Image Processing*, volume 2, pages 86–90, Austin, Texas, USA, November 1994.
11. J.R. Smith and B.O. Comiskey. Modulation and information hiding in images. In R. Anderson, editor, *Information Hiding:First Int. Workshop Proc.*, volume 1174 of Lecture Notes in Computer Science, pages 207–226. Springer-Verlag, 1996.
12. M.D. Swanson, B. Zhu, and A.H. Tewfik. Transparent robust image watermarking. In *Proceedings of the 1996 International Conference on Image Processing*, volume 3, pages 211–214, Lausanne, Switzerland, Sept. 16-19 1996.
13. L.T. Turner. Digital data security system. In *Patent IPN WO 89/08915*, 1989.
14. S. Walton. Image authentication for a slippery new age. In *Dr.Dobb's Journal*, pages 18–26, April 1995.
15. R.B. Wolfgang and E.J. Delp. A watermark for digital images. In *IEEE Int. Conf. on Image Processing*, volume 3, pages 219–222, Lausanne,Switzerland, 1996.
16. R.B. Wolfgang and E.J. Delp. A watermarking technique for digital image:further studies. In *Proceedings of the International Conference on Imaging Science,System, and Technology*, pages 279–287, Las,Vegas, June 30-Julu 3 1997.
17. J. Zhao. Look, its not there: Digital watermarking is the best way to protect intellectual property from illicit copying. In *Byte Magazine*, January 1997.

This article was processed using the LaTeX macro package with LLNCS style