Intra-Block Algorithm for Digital Watermarking[*]

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

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

Abstract

We present a variant to the Discrete Cosine Transform (DCT)-based block algorithm proposed in [3] for signal embedding in digital images. Instead of inter-block relations, our algorithm use intra-block relations to generate the output. We demonstrate the algorithm and its performance against translation and area cropping.

Keywords: digital watermarking, discrete cosine transform, block coding techniques.

Conference Tracks: Algorithm & Techniques (image coding, image signal)

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.

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

[*] This work is supported in part by RGC Earmark Grant # CUHK4176/97E

[†] Contacting author.

sampling to ensure that the watermarking signal can still be retrieved with high degree of accuracy.

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 great. Hence, it is the goal in designing the watermarking algorithm to have a technique which satisfies many of the requirements with good realtime 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.

In [6], Walton uses a checksum on the image data which is embedded in the least significant bits of certain pixels for watermarking. Others have added a maximal length linear shift register sequence to the pixel data and identify the watermark by computing the spatial cross-correlation function of the sequence and the watermarked image [5].

Watermarks can be image dependent. For example, [2] uses independent visual channels for watermark embedding and [1] generated watermarked images by modulating JPEG coefficients. These watermarks are designed to be invisible, or to blend in with natural camera or scanner noise.

Visible watermarks also exist; IBM has developed a proprietary visible watermark to protect images that are part of the digital Vatican library project [4].

In [3], Hsu presented a DCT-based algorithm using inter-block relation to implement the middle-band embedding. First, he used a fast two-dimensional pseudo-random number traversing method to permute the signature image. Second, the input image is divided into blocks of size 8×8, and then each block is DCT transformed. Third, he chose 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 modified the DCT coefficients according the residual mask.

Our method is different from [3]. Instead using inter-block relations, our algorithm use intra-block relations to generate the output. This method seems to be more robust

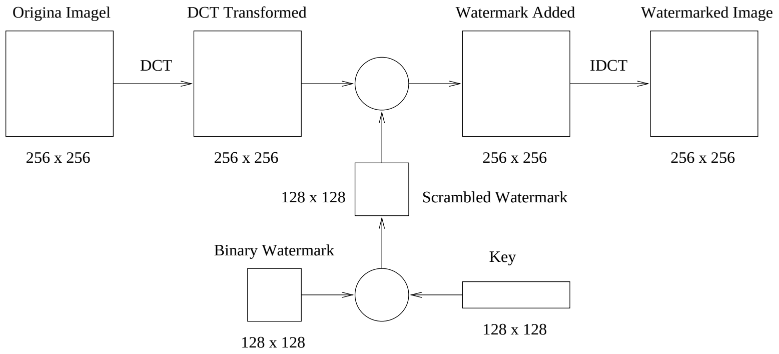


Figure 1: The schematic of a general key-based watermarking process.

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

In Section 2, we present our new proposed watermarking algorithm. We then present our experimental results in Section 3. Discussion is presented in Section 4 and then we conclude in Section 5.

3 Proposed Algorithm

3.1 Embedding Approach

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

$$O = \{o(i,j), 1 \leq i,j \leq N\}, o(i,j) \in \{0, \cdots, 2^L - 1\}, \tag{1}$$

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

$$W = \{w(i,j), 1 \leq i,j \leq N/2\}, w(i,j) \in \{0,1\}, \tag{2}$$

with $N' = N/2$ in our case.

Key Sequence Production

Let a key sequence K be defined as a vector of size N'^2 with a random permutation $\Pi \equiv (\pi_1, \pi_2, \cdots, \pi_{N'^2})$.

Permutation of the Watermark Data

$$W'(i,j) = W(i',j') \tag{3}$$

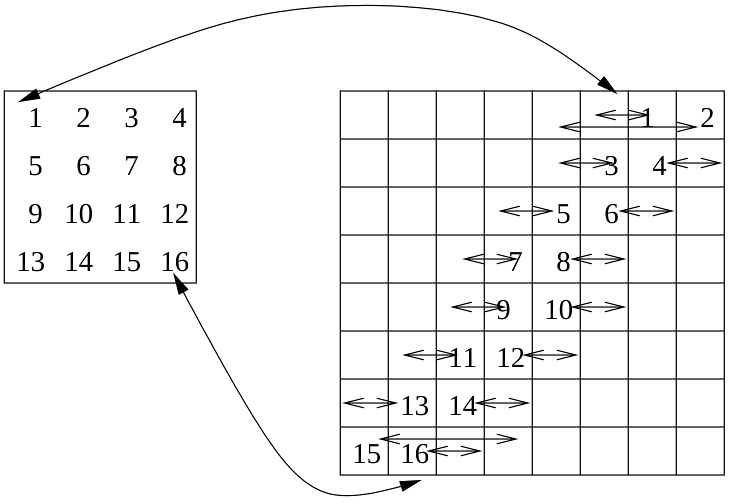


Figure 2: How the scambled binary watermark image is embedded into the DCT transformed original image. If the entry in W' is "1", the corresponding block of D' entry is exchanged.

where (i', j') is permuted to (i, j) using the sequence K. After this permutation step of the watermark data is performed, we have a scrambled binary watermark image which can be used in the next step.

Block Transformation of the Image

The image O is divided into $M \times M$ blocks with each block size of N/M. Each block is then transformed by the Discrete Cosine Transform (DCT) using

$$\begin{aligned} D_{m,n} &= DCT(O_{m,n}), \qquad 1 \leq m, n \leq M & (4) \\ &= \{d_{m,n}(k, l), 1 \leq k, l \leq N/M\} & (5) \end{aligned}$$

Modification of DCT Coefficients

The permuted watermark W' is also divided into $M \times M$ block with the block size, $N/(2M)$.

There are two cases for updating the coefficients. When $w'_{m,n}(i, j) = 1$ and the index is odd, we perform an exchange of $d_{m,n}(i, j)$ with $d_{m,n}(i, j-1)$ with the exception in the last row. When the index is even, we exchange $d_{m,n}(i, j)$ with $d_{m,n}(i, j+1)$ with the exception in the first row. The exchange matrix is illustrated in Fig. 2.

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

Inverse Block Transform

$$O'_{m,n} = IDCT(D'_{m,n}) \tag{6}$$

3.2 Extracting Method

The extraction of watermark W requires the original image O, the embedded images O' and the key sequence K. The extraction steps are as follow:

3.2.1 Block Transformation

Both the original image O and the embedded image are DCT transformed.

$$\begin{aligned} D_{m,n} &= DCT(O_{m,n}) && (7)\\ D'_{m,n} &= DCT(O'_{m,n}) && (8) \end{aligned}$$

3.2.2 Extracting the Permuted Watermark

For odd,

$$W'_{m,n} = \text{sign}(d_{m,n}(i,j) - d_{m,n}(i,j-1)) \oplus \text{sign}(d'_{m,n}(i,j) - d'_{m,n}(i,j-1)) \tag{9}$$

For even,

$$W'_{m,n} = \text{sign}(d_{m,n}(i,j) - d_{m,n}(i,j+1)) \oplus \text{sign}(d'_{m,n}(i,j) - d'_{m,n}(i,j+1)) \tag{10}$$

where $\oplus$ is the exclusive OR function defined as,

$$x \oplus y \equiv \begin{cases} 1 & \text{if } x \neq y \\ 0 & \text{Otherwise} \end{cases} \tag{11}$$

and the sign function defined as,

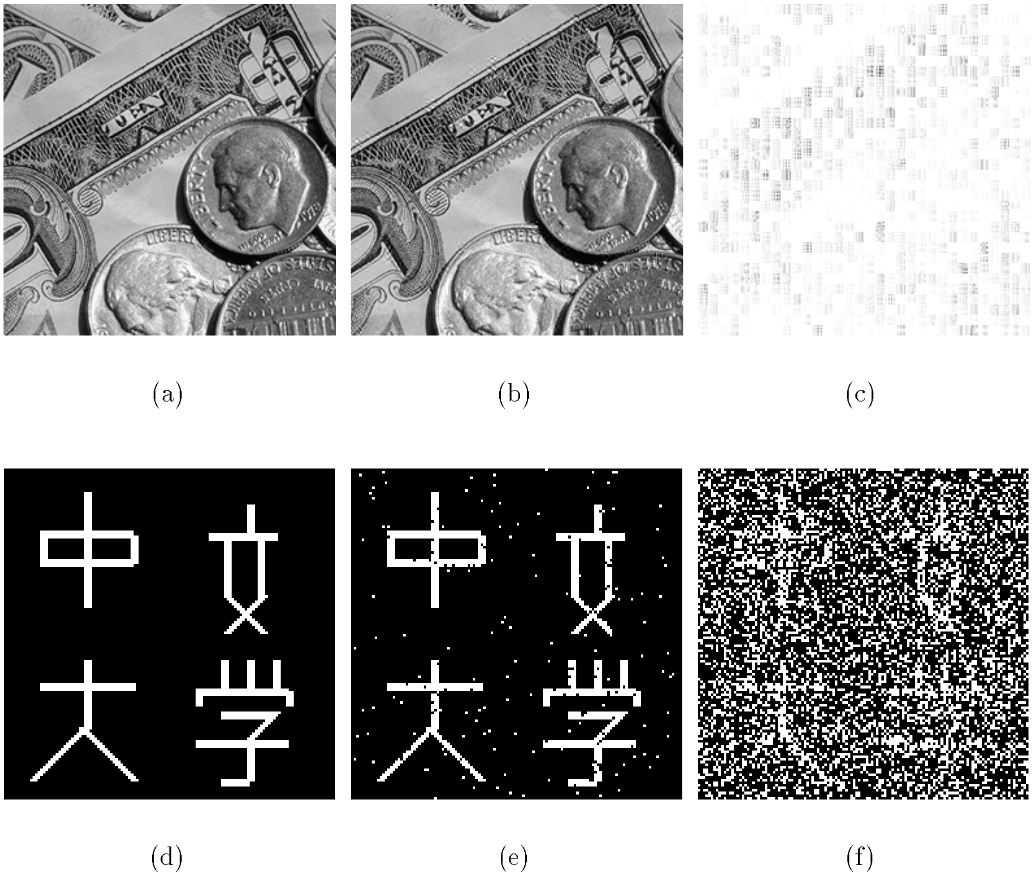
$$\text{sign}(x) \equiv \begin{cases} 1 & x > 0 \\ 0 & \text{Otherwise} \end{cases} \tag{12}$$

4 Experimental Results

We perform two basic transformations: (1) translation and (2) cropping. The experiments were conducted on UltraSparc workstation with Matlab 5.

Table 1: Values of the variables used in our experiment

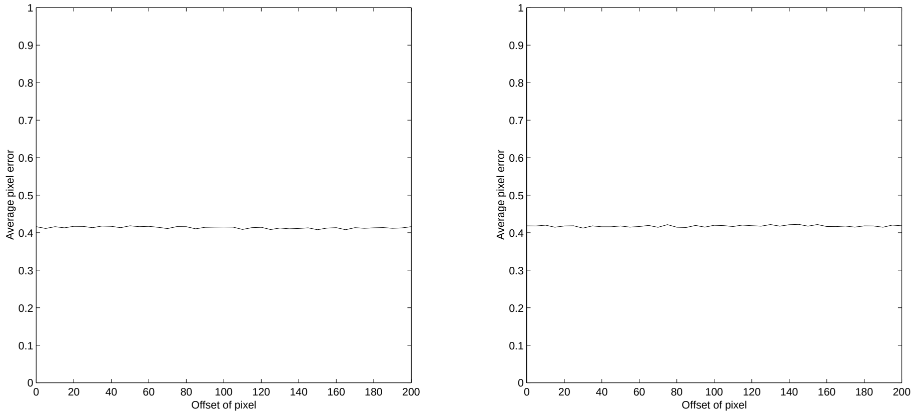
Variable Name	Variable Type	Value
O	matrix	256×256
O'	matrix	256×256
W	matrix	128×128
K	vector	1×128^2
N	integer	256
N'	integer	128
M	integer	32
L	integer	256



(a) (b) (c)

(d) (e) (f)

Figure 3: (a) the original image, (b) the watermarked image, (c) the difference between the original and the watermarked image, (d) the original watermark image, (e) the extracted watermark image, (f) the worst extracted watermark image with average pixel error of 0.295 using 42% of the image area from the watermark image.



(a)

(b)

Figure 4: We used a cropped image of 50 × 230 and translate it horizontally in (a) and vertically in (b). The error obtained is fairly similar which shows that this method is invariant to translation.

We defined the Average Intensity Error Per Pixel (AEPP) when comparing the watermarked image with the original is defined as,

$$\text{AEPP} \equiv \frac{\sum |O - O'|}{N \times N}. \tag{13}$$

We found that the AEPP is 4.4 using the watermark image shown in Fig. **??**(d). This result is quite acceptable since we cannot distinguish the original image and the watermarked image perceptually.

4.1 Translation

Using the same key sequence, K with different cropping sizes over different location of the original image

The Average Pixel Error (APE) is defined as:

$$\text{APE} \equiv \frac{\sum |W - W'|}{N' \times N'}. \tag{14}$$

Our method is translational invariant since there is no significant effect under translation with a constant size as shown in Fig. 4 when we used a cropping image of 50 × 230 selected horizontally and vertically.

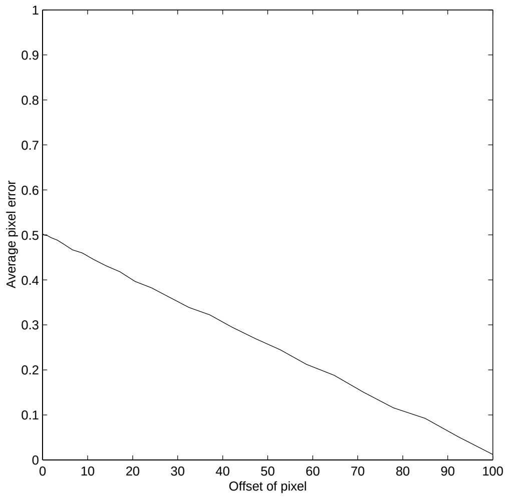


Figure 5: We now vary the size of the cropped image at the center of the image and found that the error is inversely proportional to the size of the cropped image.

4.2 Cropping

Our experiment show 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. Here we varied the size of the cropped image from 100% (256×256) to 0.39% (16×16) with the APE ranges from 0.0121 to 0.4996 respectively. It is interesting to observe that the APE under cropping is asymptotically approaching 0.5 since the watermark image retrieved becomes a random image. Furthermore, we observed that when the APE is greater than 0.295 (the cropped image size is less than 42.04%) the retrieved watermark image cannot be distinguished with the original watermark image perceptually.

Although all the retrieved watermark images contain error, these images can be post-processed to eliminate some if not all of the errors. For example, with the assumption that the watermark image contains highly structured content, simple noise filters can be used to remove these unwanted noise.

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 37% of the original image, the retrieved watermark is illegible perceptually. Even when we used the whole watermarked original image without cropping, there is still error arising from the DCT computation. This background error is about 1-2%.

From Fig. 3(c), we can see that this method embeds watermark information in content-rich (high frequency) areas of the original image since there is less error in the relatively uninteresting area, such as the white boarder surrounding the money bill.

6 Conclusion

We present a variant to the DCT-based block algorithm proposed in [3] for watermark embedding in digital images.Our method is different from [3]. Instead using inter-block relations, our algorithm uses intra-block relations to generate the output. This method seems to be more robust 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. We demonstrated the algorithm and its performance against translation and area cropping.

Our experiment show 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 area. The APE under cropping is asymptotically approaching 0.5 since the watermark image retrieved becomes a random image. Furthermore, we observed that when the APE is greater than 0.295 (the cropped image size is less than 42%) the retrieved watermark image cannot be distinguished with the original watermark image perceptually.

References

[1] 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.

[2] 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.

[3] C.T. Hsu and J.L. Wu. Hidden signatures in image. In *IEEE Int. Conf. on Image Processing*, pages 223–226, Lausanne, Switzerland, September 1996.

[4] 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.

[5] R.G. Van Schyndel, A.Z. Tirkel, N.R.A. Mee, and C.F. Osborne. A digital watermark. In *Processings of the IEEE International Conference on Image Processing*, pages 86–90, Austin, Texas, USA, November 1994.

[6] Steve Walton. Image authentication for a slippery new age. In *Dr. Dobb's Journal*, pages 18–26, April 1995.