

Pixel-wise based Digital Watermarking Using a Multiple Sections Embedding Technique

Komwit Surachat

Abstract—A method for improving the watermark extraction performance of the digital watermarking based on the modification of image pixels is proposed in this paper. By embedding a watermark signal with a multiple sections technique in the blue channel, the accuracy of the extracted watermark can be improved. Sets of experiment are carried out to prove our proposed concept. The obtained results show that the improved performance in term of NC, compared to the previous method, is achieved by using our proposed watermarking method. The improved robustness of the proposed method against various common imaging processing based attacks also performs better. Especially in cropping attacks, at cropping 50% the results significantly improve about 0.2 on average in terms of NC value compared to previous proposed algorithm.

Index Terms—Digital watermarking, multiple sections embedding technique, image processing

I INTRODUCTION

For any risky and sensitive documents, the author/owner would need them to be fully and effectively protected at all time. Due to one main characteristic of digital multimedia i.e. the ease of copying and redistributing without significant loss of quality, problem of illegal distributions of multimedia data has been extensively increased, where the violation can simply be done without any permission from the original owner, and without any means to differentiate between the original media and the copied one. On the other hand, there're so many strategies to protect the digital media data nowadays with so many differences in terms of algorithm, complexity, performance and even security level. Digital watermarking is a kind of standard technology to maintain access control for the documents. Good introduction on digital watermarking including its essential requirements can be found on [1] and [2].

Currently, many image watermarking methods have been proposed and proved to be robust against various kinds of noises and attacks. Such methods can be classified into frequency and/or spatial domain based watermarking. In the frequency domain, the watermark embedding can be accomplished by modifying the image coefficients from its transformed domain. For instance, Badran et al. [3] proposed the methods to embed the in the Discrete Cosine Transform (DCT) based on image segmentation using Expectation Maximization (EM) algorithm. Also, Patra et al. [4] presented a based Chinese Remainder Theorem (CRT)-based Discrete Cosine Transform (DCT) domain. However,

many researches demonstrated that the frequency domain based approach was not robust enough against geometrical attack, e.g. cropping. It can survive most image compression standards e.g. JPEG compression standard, though. In contrary, for the spatial domain based approach, it is obvious that the processes of watermark embedding and extraction are simple to perform by modifying the image pixels directly.

For example, M. Kutter et al. [5] presented a method to embed a watermark signal into an image by modifying the pixel using either additive or subtractive depending on the watermark bit, and proportional to the luminance of the embedding pixel. According to their method, the blue colour channel was selected to carry the watermark bit since it is the one that human eye is least sensitive to.

Later, many researchers [6],[7] proposed the methods to improve the quality of the watermarked image by modifying the pixel depending on and proportional to the luminance of the embedding pixel. Especially in [7], T. Amornraksa et al. proposed some techniques to enhance its watermark retrieval performance by balancing the watermark bits around the embedding pixels, tuning the strength of embedding watermark in according with the nearby luminance, and reducing the bias in the prediction of the original image pixel from the surrounding watermarked image pixels. However, all the methods mentioned above encountered a deficiency when implemented with an image having a large number of high frequency components.

Our approach applies the same image watermark technique as proposed in [7] because this technique can embed large number of watermark bits into a colour image. The next section gives a brief concept of the digital watermarking based on the modifications of image pixels in the blue colour channel. Section 3 describes our proposed technique. In section 4, the experimental results are shown and discussed. The conclusion is finally drawn in section 5.

II DIGITAL WATERMARKING USING PIXEL MODIFICATION IN SPATIAL DOMAIN [7]

In the watermark embedding process, the watermark bits $w_{(i,j)} \in \{1,-1\}$ to be embedded are first permuted, using XOR operation, with a pseudo-random bit-stream generated from a key-based stream cipher to improve the balance of w around (i,j) , and the security of the embedded watermark. The result is then adjusted by a scaling factor s to control the strength of the watermark for the entire host image. The watermark embedding is performed by modifying the image pixel in the blue color channel $B_{(i,j)}$, in a line scan fashion. The modifications of the image pixel $B'_{(i,j)}$ are either additive or subtractive, depending on $w_{(i,j)}$, and proportional to the modification of luminance of the embedding pixel

Manuscript received April 15, 2012; revised May 29, 2012.

The authors are with Information and Communication Technology Programme, Faculty of Science, Prince of Songkla University (e-mail: komwit.s@psu.ac.th)

$L_{(i,j)}$. Note that, the modification of luminance $L'_{(i,j)}$ is obtained from a Gaussian pixel weighting mask. The process of watermark embedding can be represented by the following equation.

$$B'_{(i,j)} = B_{(i,j)} + w_{(i,j)}sL'_{(i,j)} \quad (1)$$

To extract the watermark signal, the following two steps are used to estimate the embedded watermark bit at (i,j) .

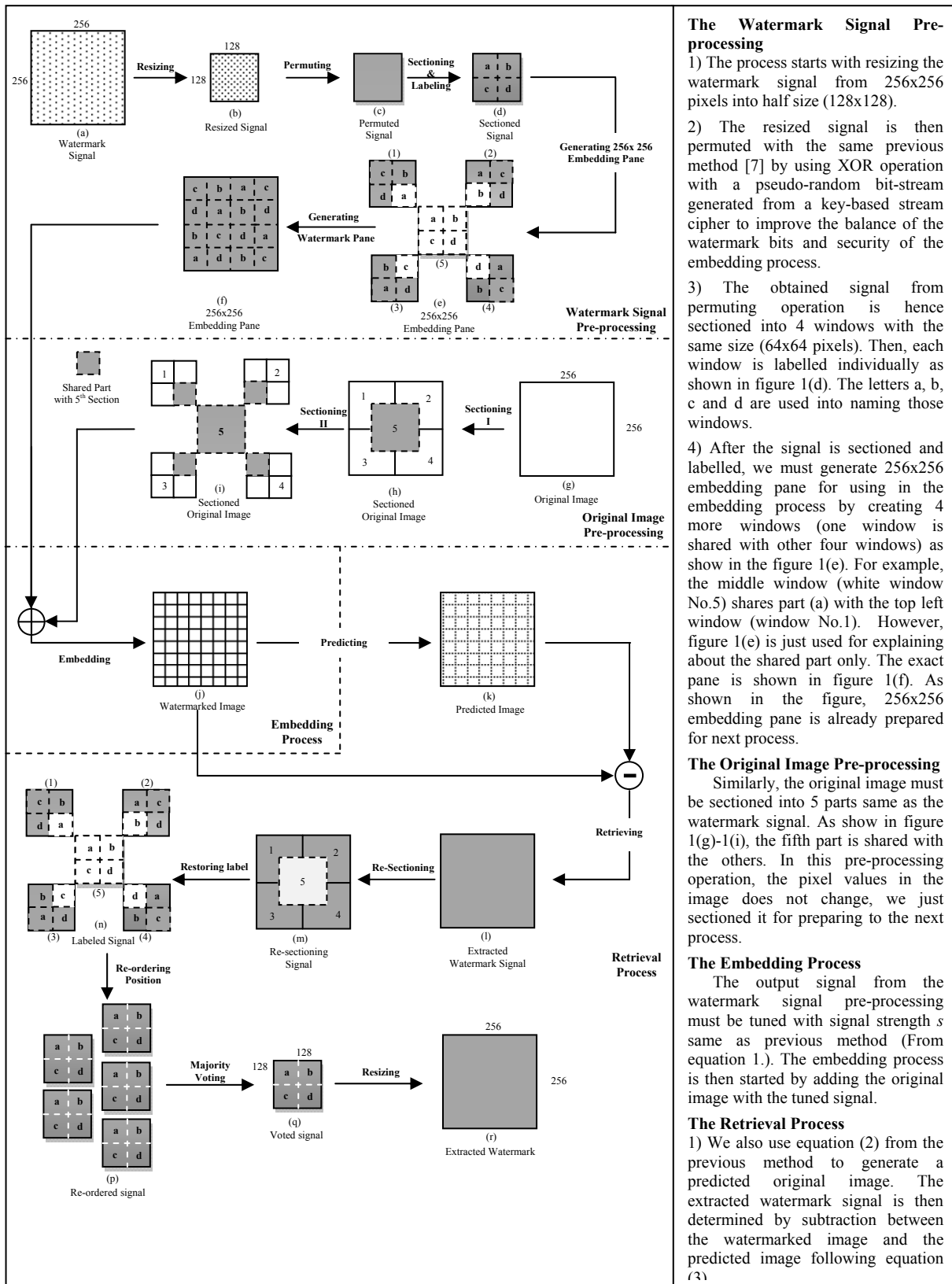


Fig. 1. Watermark embedding and retrieval process scheme

1) Each original image pixel in the chosen channel was predicted from its neighbouring watermarked image pixels in the same embedding channel. Each original image pixel in the chosen channel was predicted from its neighbouring

watermarked image pixels in the same channel. The predicted original image pixel $B''_{(i,j)}$ is determined by

$$B''_{(i,j)} = \frac{1}{8} \left(\sum_{m=-1}^1 \sum_{n=-1}^1 B'_{(i+m,j+n)} - B'_{(m_{max},N_{max})} \right) \quad (2)$$

where $B'_{(m_{max}, n_{max})}$ is a neighbouring pixel around (i, j) that most differs from $B'_{(i, j)}$.

2) The embedded watermark bit $w'_{(i, j)}$ at a given coordinate (i, j) can then be determined by the following equation

$$w'_{(i, j)} = B'_{(i, j)} - B''_{(i, j)} \quad (3)$$

where $w'_{(i, j)}$ is the estimation of the embedded watermark w around (i, j) . Since $w_{(i, j)}$ can be either 1 and -1, the value of $w'_{(i, j)} = 0$ is set as a threshold, and its sign is used to estimate the value of $w_{(i, j)}$. That is, if $w'_{(i, j)}$ is positive (or negative), $w_{(i, j)}$ is 1 (or -1, respectively). Notice that the magnitude of $w'_{(i, j)}$ reflects a confident level of estimating $w_{(i, j)}$.

III PROPOSED WATERMARKING METHOD

The embedding process consists of two sub-processes those are the watermark signal pre-processing and the original image pre-processing. The Descriptions of each process are given as follows.

IV EXPERIMENTAL RESULTS

In the experiments, we used nine standard colour images, namely ‘Lena’, ‘Tower’, ‘House’, ‘Fish’, ‘Bird’, ‘Pens’, ‘Flowers’, ‘Pepper’ and ‘Baboon’ with the size of 256×256 pixels as the original images. We also used the 256×256 pixels black & white image containing a logo ‘ICT’ as a watermark signal, i.e. by considering the black colour pixel

as -1, and white as 1. In all experiments, we evaluated the quality of watermarked image by measuring its PSNR (Peak Signal-to-Noise Ratio) and evaluated the quality of extracted watermark by measuring its NC (Normal Correlation). For both measuring methods, the higher value indicates a better quality of the result obtained.

A. Performance Comparison

In this experiment, the performance of the proposed method was evaluated to compare with the previous method in [7]. Note that, we tested the performance of the extracted watermark image by fixing a PSNR value at 35, 40 and 45dB once a time. Then, the NC value was evaluated and compared. As shown in the table 1, our proposed method performed better in all fixed PSNR values. For instance, at PSNR = 35dB, the NC value of the watermark extraction was improved ≈ 0.12 .

B. Robustness Against Attacks

Finally, the robustness of the proposed watermarking method was evaluated by applying six different types of attack. The NC values from the attacked images were then computed and compared. A list of the attacks in the experiment consisted of additive Gaussian distributed noise with zero mean at various variances, the cropping attacks at various percentage and various cropping styles, the salt and pepper noise at various densities, the blurring attack at $\theta = 11$ and various length and the contrast adjustment attack at various contrast scaling factors.

TABLE I: AVERAGE NC VALUES AT DIFFERENT TYPES OF ATTACK

Attack Types	Average NC Values		Attack Types	Average NC Values	
	Previous Method in [7]	Proposed Method		Previous Method in [7]	Proposed Method
Non-attacked Average PSNR = 35dB	0.85	0.92	Cropping to Right Corner 10%	0.83	0.91
Non-attacked Average PSNR = 40dB	0.81	0.89	Cropping to Right Corner 20%	0.81	0.89
Non-attacked Average PSNR = 45dB	0.78	0.86	Cropping to Right Corner 50%	0.76	0.89
Gaussian Noise Variance = 0.001	0.79	0.87	Salt and Pepper Noise density = 0.01	0.85	0.92
Gaussian Noise Variance = 0.005	0.74	0.82	Salt and Pepper Noise density = 0.03	0.85	0.92
Gaussian Noise Variance = 0.01	0.72	0.81	Salt and Pepper Noise density = 0.06	0.83	0.91
Cropping 10%	0.82	0.90	Blurring Theta =11 Len =2	0.80	0.87
Cropping 20%	0.78	0.89	Blurring Theta =11 Len =8	0.71	0.80
Cropping 30%	0.75	0.89	Contrast Adjustment 10%	0.84	0.91
Cropping 40%	0.72	0.89	Contrast Adjustment 30%	0.82	0.90
Cropping 50%	0.70	0.88	Contrast Adjustment 50%	0.81	0.89

As shown in Table I, our proposed method performed better in every types of attack including non-attacked image.

Especially in the cropping attack, at cropping percentage = 50 the average NC value was explicitly better than the

previous method about 0.2 and the extracted watermark image was still clearly readable by human eyes as shown in figure 2(E)- 2(F). Moreover, in the non-attacked cases, from figure 1(A) we hardly detect the difference between the

original image and the watermarked image. From our observation, the quality of the watermarked image was undoubtedly comparable to the original host image.


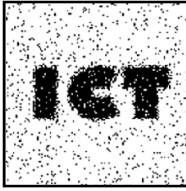
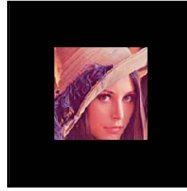

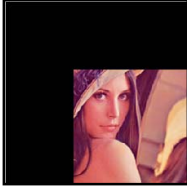



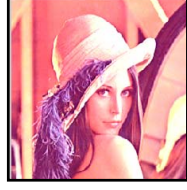
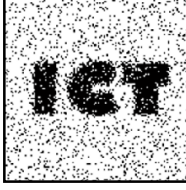
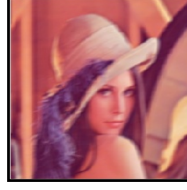

Watermarked Image/Attacked Image	Extracted Signal of Proposed Method	Watermarked Image/Attacked Image	Extracted Signal of Proposed Method
 (A) PSNR = 35db	 (B) NC = 0.95	 (C) Cropping 50%	 (D) NC = 0.92
 (E) Cropping 50%	 (F) NC = 0.95	 (G) Cropping 20%	 (H) NC = 0.92
 (I) Contrast Adjustment 50%	 (J) NC = 0.95	 (K) Blurring (Theta =11 Len =2)	 (L) NC = 0.9

Fig. 2. The resultant watermarked image and its extracted signal at different attacks

V CONCLUSION

In this paper, we have proposed a new method to improve the accuracy of the extracted watermark by using a multiple sections embedding technique. We have proposed to section the watermark image into 5 windows and embed the same watermark signal in each window individually. In addition, the majority voting method has been chosen to select the right watermark bits in extraction process. The experimental results have shown the improvement in every attack types including the non-attacked image. Especially in the cropping attack, even though the original image is cropped more than 50%, the extracted watermark signal is still clearly readable and have a high NC value. The improvement of the accuracy of the extracted watermark image at 50% cropping attack is better than the previous method [7] over 0.2 in terms of NC.

REFERENCE

[1] I. J. Cox, L. Mathew, M. Miller, A. Bloom, J. Fridrich, and T. Kaller, "Digital Watermarking and Steganography," *Morgan Kaufmann, Los Altos, CA, USA*, ISBN: 1-55860714-5, 2002.

[2] F. Y. Shih, "Digital Watermarking and Steganography Fundamental and Techniques," *CRC Press*, 2007.

[3] E. F. Badran, A. Ghobashy, and K. El-Shenawy, "DCT-Based Digital Image Watermarking Via Image Segmentation Techniques," in *Proc. of ITI 4th International Conference on Information and Communications Technology*, Alaska, USA, 2006.

[4] J. C. Patra, A. K. Kishore, and C. Bornand, "Improved CRT-based DCT domain watermarking technique with robustness against JPEG compression for digital media authentication," in *Proc. of 2011 IEEE International Conference on Systems, Man, and Cybernetics*, pp 2940 – 2945, 2011.

[5] M. Kutter, F. Jordan, and F. Bossen, "Improved Digital Signature of Colour Images using Amplitude Modulation," *Journal of Electronic Imaging*, pp 326 – 332, 1998.

[6] R. Puertpun, and T. Amornraksa, "Pixel Weighting Marks in amplitude Modulation of Colour Image Watermarking," in *Proceedings of the IEEE ISSPA*, Kuala-Lumpur, pp 194 – 197, 2001.

[7] T. Amornaksa, and K. Jantawongwilai, "Enhanced Images Watermarking Based on Amplitude Modulation," *Journal of Image and Vision Computing*, pp 111 – 119, 2006.