

A New Robust Watermarking Scheme for Color Image in Spatial Domain

Ibrahim Nasir, Ying Weng, Jianmin Jiang
School of Informatics, University of Bradford, UK
{ianasir, Y.Weng, J.Jiang1}@Bradford.ac.uk

Abstract

*This paper presents a new robust watermarking scheme for color image based on a block probability in spatial domain. A binary watermark image is permuted using sequence numbers generated by a secret key and Gray code, and then embedded four times in different positions by a secret key. Each bit of the binary encoded watermark is embedded by modifying the intensities of a non-overlapping block of 8*8 of the blue component of the host image. The extraction of the watermark is by comparing the intensities of a block of 8*8 of the watermarked and the original images and calculating the probability of detecting '0' or '1'. Tested by benchmark Stirmark 4.0, the experimental results show that the proposed scheme is robust and secure against a wide range of image processing operations.*

Index Terms— Watermarking, Spatial domain, Gray code, Watermark.

1. Introduction

The watermark is a signal embedded into the host media to be protected, such as an image or audio or video. It contains useful certifiable information for the owner of the host media, such as producer's name, company logo, etc; the watermark can be detected or extracted later to make an assertion about the host media. There are two important properties of a watermark; the first is that the watermark embedding should not alter the quality and visually of the host image and it should be perceptually invisible. The second property is robustness with respect to image distortions. This means that the watermark is difficult for an attacker to remove and it should be also robust to common image processing and geometric operations, such as filtering, resizing, cropping and image compression. [5, 13]. Overviews on image watermarking techniques can be found in [3, 9, 13].

Watermarking techniques can be classified into two categories: spatial domain and transform domain techniques. In spatial domain technique [6, 8, 10, 15, 16, 17], the watermark embedding is achieved by directly modifying the pixel values of the host image. The most

commonly used method in the spatial domain technique is the least significant bit (LSB). In [10], the least significant bit (LSB) of each pixel in the host image was modified to embed the secret message. In [15], the watermark is embedded in saturation on the HIS (hue, saturation, intensity) color space. The results in [15] show that the proposed method can only resist some attacks. In [6], the watermark is embedded into DC components of color image directly in spatial domain. The results show that the proposed method provided robust performance, except for images with high frequency components attacked by rotate-scaling operations. In [17], the proposed method based on chaotic maps in order to encrypt the embedding position and to determine the pixel bit for embedding in host image. In [8], a watermarking scheme is presented based on embedding the watermark into the original image in spatial domain by dividing the original image into different block size and adjusting brightness of a block according to the watermark. [16] proposes a spatial domain probability block based watermarking method for color image, which is divided into blocks of size 8*8 and the intensities of all pixels in the block are modified in order to embed a watermark bit. In this method the number of total bits of the watermark must be less or equal to the half of the total number of 8*8 blocks and redundant information is added to the watermark using convolutional code. The disadvantage of using convolutional code is that it is required a constant high amount of decoding operations, even if few or no errors occurred [7]. The proposed methods [8, 16] are quite robust against some common image processing operations, such as median filter, scaling and rotation; however, they are less robust to cropping attack because the watermark bits are embedded into the whole image hence some data must be lost in cropping.

In transform domain technique [1,2,11,14], the host image is first converted into frequency domain by transformation method such as the discrete cosine transform (DCT), discrete Fourier transform (DFT) or discrete wavelet transform (DWT) ,etc. then, transform domain coefficients are modified by the watermark. The inverse transform is finally applied in order to obtain the watermarked image. In [11], the watermark is embedded into the DCT coefficients of subimages, which are

obtained by subsampling the original image. Due to the complicated calculations of forward and inverse transform, these methods generally are more complex and involved higher computational costs than spatial domain methods; however, transformation domain methods are more robust against attacks than spatial domain methods [14]. Some proposed methods in frequency domain focus on embedding two or three watermarks. In [1], proposed algorithm based on embedding the watermark image three times in different frequency bands that are low, medium and high; result of that the watermark can not be totally destroyed by either low pass, medium or high pass filter. In [2], two complementary watermarks were embedded into the host image in order to make it difficult for attackers to destroy both of them.

The main motivation of this paper is based on the idea proposed in [16]. In this paper, we propose a spatial domain-watermarking scheme based on a block probability. The watermark is a binary image, which is permuted using a secret key and Gray code. The permuted watermark is embedded four times in different positions in the blue component of color image in order to overcome of the mentioned disadvantage in [8, 16].

The rest of the paper is organized as follows. Section 2 describes the proposed watermarking method and in section 3, the experimental results are discussed. Finally, some conclusions are drawn in section 4

2. Proposed watermarking method

In our scheme, a binary logo image is used as the original watermark W of size pixels 32×32 , which is shown in Fig. 1(a). In order to construct a good watermark for embedding, the original watermark is permuted to obtain a pseudo random sequence, which uncorrelated to the original watermark as shown in Fig.1 (b). This is done by performing bit wise EX-OR operation between the original watermark bits and random bits, which generated using a secret key, and then the output sequence, is encoded using Gray code. The permutation process of the watermark W is described as follows:

$$W = \{W(i, j), 1 \leq i \leq 32, 1 \leq j \leq 32, w(i, j) \in (0,1)\}$$

K is the chaotic binary sequence, which is the secret key

$$K = \{k(i, j), i \leq 1 \leq 32, 1 \leq j \leq 32, k(i, j) \in (0,1)\}$$

$$W' = W \oplus K \quad \text{where } \oplus \text{ denotes XOR operation.}$$

The permuted watermark W'' is obtained by applying Gray code to W'



Fig. 1 (a) Original watermark. (b) Permuted watermark
2.1 Watermark embedding

The proposed watermark embedding scheme is shown in Fig.2. In the proposed method, the watermark image is a binary image where as the host image is an 8 bit color image. The watermark is embedded four times as shown in Fig.3 in different positions. The four embedded positions are chosen to hide the watermarks in order to be robust against cropping attack from the bottom, the top or the left or the right side of the watermarked image. The blue component is chosen to hide the watermark because it is less sensitive to human eyes. Suppose the original color image H with size of 512×512 pixels, which to be protected by the binary watermark W of size pixels 32×32 , the original image H is divided into a non-overlapping blocks of 8×8 and each bit of the encoded watermark is embedded in a block, therefore one watermark is required 1024 blocks. The embedding process is described as follows:

Step 1: The watermark W is permuted as described in section 2.

Step 2: The original image H is decomposed into R, G, and B components and then the B component is divided into a non-overlapping blocks with size of 8×8 pixels.

Step 3: A private key is used to determine the positions of embedding the watermark

Step 4: The encoded watermark W'' is embedded in the blue component B. For each encoded watermark bit, a block of 8×8 is modified as follows:
if $W''=1$;
for all the pixels of the 8×8 blocks
{ $I'=I + \lambda$ }
If $W''=0$;
For all the pixels of the 8×8 blocks
{ $I'=I - \lambda$ }

Where I' is the modified pixel intensity and I is the original intensity and λ is a constant.

Step5: The modified block of pixels is then positioned in its original location of the host image and then step 3 and 4 is repeated until all encoded watermark bits W'' are embedded.

Step6: After embedding the all encoded watermark bits four times, the R, G, and B' components are composed to obtain the watermarked image.

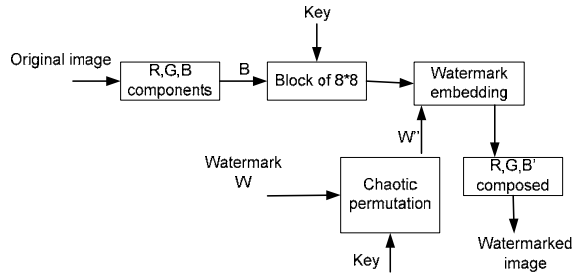


Fig. 2. The proposed watermark embedding scheme

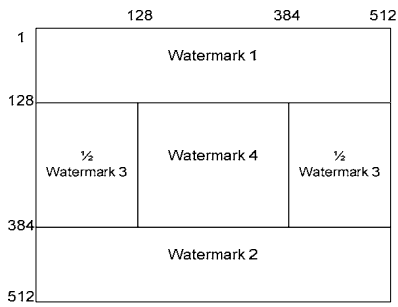


Fig. 3. The proposed watermarks embedded positions

2.2 Watermark extraction

The proposed watermark extraction is shown in Fig. 4. It is required the original host image and the original watermark, therefore, it is a non blind watermarking scheme. The proposed extraction is based on the probability (P1, P0) of detecting '1' or '0' bit, which can be obtained by comparing each pixel (I') in a block of 8*8 of the watermarked image with the corresponding pixel (I) in the original image and then the probability of detecting '1' or '0' bit is calculated as follows:

$$P1 = P1 + 1/64 \quad \text{if } I' > I$$

$$P0 = P0 + 1/64 \quad \text{if } I' \leq I$$

According to the probability (P1, P0), the extracted watermark bits W'' can be decoded as follows:

$$W'' = 1 \quad \text{if } P1 \geq P0$$

$$W'' = 0 \quad \text{if } P1 < P0$$

The extracted watermark bits for the four watermarks are decoded using Gray code and then, the decoded bits are XOR with random bits, which generated using the same secret key that was used during the watermark embedding. The decoded watermark bits are reordering to images $W'1, W'2, W'3, W'4$. Together with the extraction of visual image watermark, we calculate the normalized cross correlation between the original watermark image W and the extracted watermarks $W'1,$

$W'2, W'3, W'4$ to make a binary decision on whether a given watermark exists or not. We choose 0.5 as the threshold for watermark decision. The normalized cross correlation is defined by

$$NCC = \frac{\sum_i \sum_j W_{ij} W'_{ij}}{\sum_i \sum_j (W_{ij})^2}$$

Where W_{ij} and W'_{ij} are the pixel values at the position (i, j) of the original and the extracted watermark by that $1 \leq (i, j) \leq 32$, respectively.

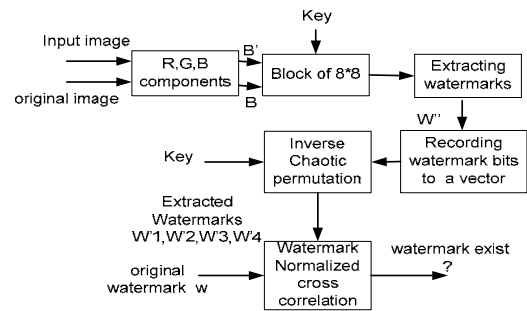


Fig. 4. The proposed watermark extraction scheme.

3. Experimental results

To verify the effectiveness of the proposed method, a series of experiments was conducted. In the experiments, the original image 'Lena' and 'Peppers', are 8 bit color images of size 512*512 pixels, are used as test images, where as the watermark image is a binary image of size 32*32 pixels. The embedding strength $\lambda=5$. Fig.5 (a) and (b) show the original host image and the original watermark respectively, Fig.5 (c) and (d) show the watermarked image and the extracted watermark, respectively. Peak signal to noise ratio (PNSR) and the mean square error (MSE) are used to evaluate perceptual distortion of our watermark scheme. The equations used are defined as follows:

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right)$$

$$MSE = \frac{1}{3 \times m \times n} \sum_{i=1}^m \sum_{j=1}^n \left[\left(r(i,j) - r^*(i,j) \right)^2 + \left(g(i,j) - g^*(i,j) \right)^2 + \left(b(i,j) - b^*(i,j) \right)^2 \right]$$

Where $r(i, j)$, $g(i, j)$ and $b(i, j)$ represents a color pixel in location (i, j) of the original image, $r^*(i, j)$, $g^*(i, j)$ and $b^*(i, j)$ represents a color pixel of the watermarked image and m, n denote the size pixels of these color images. To test the robustness of the proposed scheme, some typical signal processing attacks, such as filtering, scaling, salt and pepper noise, cropping, JPEG compression and rotation are performed. We also test our algorithm by benchmark StirMark 4.0. For image scaling operation, before watermark extraction, the image is rescaled to the original size. The experimental results of Lena and Peppers images are shown in table 1. It can be seen that our algorithm can successfully resist attacks by median filter, scaling, cropping, randomly removal of some rows and some columns, small combination of scaling with small rotation angle, self-similarities and JPEG compression with quality 50%. The extracted watermarks can be identified and declared correctly.

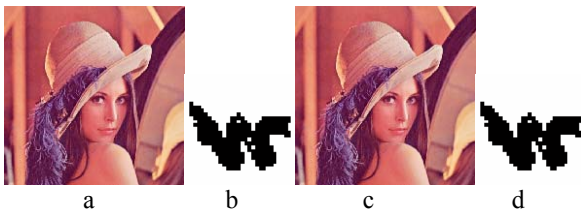


Fig.5 (a) Original image; (b) Original watermark; (c) Watermarked image; (d) Extracted watermark.



Fig. 6 (a) JPEG compressed watermarked Q=75 (b) Extracted watermark NCC=0.82

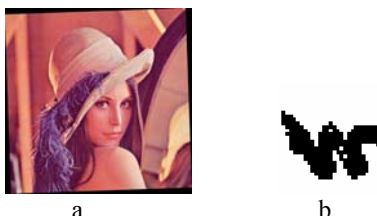


Fig. 7 (a) Watermarked image after rotation by 2° (b) Extracted watermark NCC=1.0

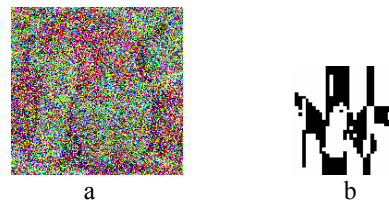


Fig. 8 (a) Watermarked image under salt and pepper noise attack (intensity=0.7) (b) Extracted watermark NCC=0.71



Fig. 9 (a) Watermarked image scaled by 0.5 (b) Extracted watermark NCC=0.65

Fig. 10, 11, 12 and 13 show the results of cropping attack. It can be seen clearly that the watermark can be extracted correctly under various cropping attack, even when the watermarked image cropped by 50% of the whole image with the cropped portions discarded and then the remaining 50% put in the center area; or when the 25% of the whole image remained from the top; or from the bottom of the watermarked image or when the watermarked cropped on both side by 25%. The experimental results show that our proposed method achieves better performance for cropping attack than the proposed methods reported in [6, 13].

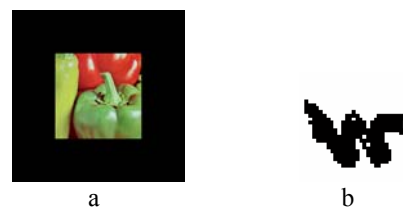


Fig. 10 (a) Cropped watermarked by 50% NCC=1.0

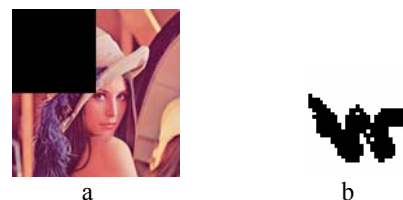


Fig. 11 (a) One quarter cropping (b) Extracted watermark NCC=1.0



Fig. 12 (a) Cropped watermarked by 75%
(b) Extracted watermark NCC=1.0

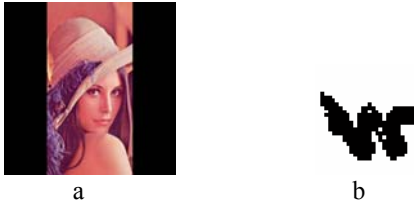


Fig. 13 (a) Cropped watermarked on both side by 25%
(b) Extracted watermark NCC=1.0

Table 1 Experimental results with StirMark 4.0 for Lena and pepper images.

| Attacks | Lena | | pepper | |
|-------------------------|---------|------|---------|------|
| | PSNR | NC C | PSNR | NC C |
| Median filter 3*3 | 33.1158 | 1.0 | 28.3363 | 1.0 |
| Median filter 5*5 | 30.4024 | 1.0 | 27.8916 | 1.0 |
| Median filter 7*7 | 28.2670 | 0.75 | 27.0367 | 0.66 |
| Rotation-scaling 0.25 | 28.3914 | 0.57 | 25.7149 | 0.54 |
| Rotation-scaling - 0.25 | 27.0801 | 0.77 | 25.3343 | 0.53 |
| Rotation-cropping 0.25 | 28.9753 | 0.67 | 26.3418 | 0.59 |
| Rotation-cropping -0.2 | 27.7384 | 0.60 | 23.8967 | 0.54 |
| Rotation_0.25 | 27.7403 | 1.0 | 25.5672 | 0.72 |
| Rotation_0.50 | 24.9223 | 1.0 | 25.3258 | 0.47 |
| Rotation_2 | 24.9164 | 1.0 | 25.4636 | 1.0 |
| Rotation_5 | 25.850 | 1.0 | 25.3258 | 0.48 |
| Rotation_30 | 25.2916 | 1.0 | 26.1606 | 0.87 |
| Rotation_45 | 27.0273 | 0.65 | 24.7497 | 0.70 |
| Rotation_90 | 27.4131 | 0.72 | 24.8407 | 0.56 |
| Scale_0.5 | 30.5809 | 1.0 | 29.3092 | 0.65 |
| Scale_2 | 32.4054 | 1.0 | 32.9208 | 0.84 |
| Remov_lines_10 | 30.9449 | 0.98 | 29.4699 | 0.88 |
| Remov_lines_50 | 31.1036 | 0.84 | 29.9368 | 0.82 |
| Remov_lines_70 | 31.0548 | 1.0 | 29.818 | 0.77 |
| Remov_lines_100 | 31.0357 | 0.85 | 29.6425 | 0.53 |
| JPEG_80 | 37.8811 | 1.0 | 35.8599 | 0.74 |
| JPEG_50 | 35.3131 | 0.55 | 34.0990 | 0.50 |
| Cropping_50 | 6.38680 | 1.0 | 7.30900 | 1.0 |
| Croppig_75 | 8.50010 | 1.0 | 9.30930 | 1.0 |
| Ss1 | 31.7797 | 1.0 | 32.5068 | 1.0 |
| Ss2 | 32.7193 | 0.69 | 34.3274 | 0.66 |
| Ss3 | 30.6569 | 1.0 | 30.3038 | 0.72 |

We also compare our results with the results obtained in [6,8] and it can be observed from table 2 that our method has better value for PSNR and our method is more robust to the attack of appalling median filter 3*3 and rotation by 12 degree and scaling by 0.5.

Table 2 Comparison of results of PSNR and NCC of using various attack methods

| Attack method | Somchok's method | | Proposed method | |
|-------------------|------------------|---------|-----------------|---------|
| | Lena | Peppers | Lena | Peppers |
| PSNR dB | 32.21 | 32.32 | 38.92 | 39.10 |
| Median filter 3*3 | 0.99 | 1.00 | 1.00 | 1.00 |
| JPEG 75% | 0.99 | 0.99 | 0.82 | 0.72 |
| JPEG 50% | 0.99 | 0.99 | 0.55 | 0.50 |
| Rotate | 0.84 | 0.81 | 1.00 | 1.00 |
| Scaling | 0.94 | 0.92 | 1.00 | 0.65 |

As indicated in table 3, our method performs better than Huang's method for self-similarities and cropping attacks

Table 3 Correlation coefficient of extracted watermark computed from different watermarking methods after median filter, self-similarities, cropping and rescaling operations.

| Watermarking method | Attack operation | | | | | | |
|--|-------------------|------|------|------|---------|-----------|---------|
| | Median filter 7*7 | SS1 | SS2 | SS3 | crop25% | scale 0.5 | scale 2 |
| Huang's method for Lena (PSNR=44.06 dB) | 0.76 | 0.89 | 0.97 | 0.82 | 0.65 | 0.92 | 0.97 |
| Propose method for Lena (PSNR=38.9260 dB) | 0.75 | 1.0 | 0.69 | 1.0 | 1.0 | 1.0 | 1.0 |
| Huang's method for Peppers (PSNR=42.23 dB) | 0.81 | 0.94 | 0.93 | 0.50 | 0.57 | 0.88 | 0.90 |
| Propose method for Peppers (PSNR=39.0641 dB) | 0.66 | 1.0 | 0.66 | 0.72 | 1.0 | 0.65 | 0.84 |

4. Conclusions

A robust watermark scheme based on a block probability for color image is presented, which operates in spatial domain by embedding the watermark image four times in different positions in order to be robust for cropping attack. The extraction of the watermark depends on the original image, so it is a non-blind watermarking scheme. The experimental results show that our scheme is highly robust against various of image processing operations such as, filtering, cropping, scaling, compression, rotation, randomly removal of some rows and columns lines, self-similarity and salt and paper noise. It is also secure scheme, only the one with the correct key can extract the watermark.

5. References

- [1] L. M. Cheng, L. L. Cheng, C. K. Chan, and K. W. Ng, "Digital watermarking based on frequency random position insertion," presented at Control, Automation, Robotics and Vision Conference, vol. 2, pp. 977-982, 2004.
- [2] L. Chun-Shien, H. Shih-Kun, S. Chwen-Jye, and L. Hong-Yuan Mark, "Cocktail watermarking for digital image protection," *Multimedia, IEEE Transactions on*, vol. 2, pp. 209-224, 2000.
- [3] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," *Proceedings of the IEEE*, vol. 90, pp. 64-77, 2002.
- [4] Fabien A. P. Petitcolas, Ross J. Anderson, and M. G. Kuhn., "Attacks on copyright marking systems," *Proc. Information Hiding, 2nd Int. workshop, Portland, Oregon, USA*, vol. LNCS 1525 Springer-Verlag, ISBN 3-540-65386-4, pp. 218-238, April 14-17, 1998.
- [5] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceedings of the IEEE*, vol. 87, pp. 1079-1107, 1999.
- [6] P. S. Huang, C. S. Chiang, C. P. Chang, and T. M. Tu, "Robust spatial watermarking technique for colour images via direct saturation adjustment," *Vision, Image and Signal Processing, IEE Proceedings -*, vol. 152, pp. 561-574, 2005.
- [7] K. Hueske, J. Geldmacher, and J. Gotz, "Adaptive decoding of convolutional codes," *Advanced in radio science*, vol. 5, pp. 209-214, 2007.
- [8] S. Kimpan, A. Lasakul, and S. Chitwong, "Variable block size based adaptive watermarking in spatial domain," presented at Communications and Information Technology, ISCIT 2004. IEEE International Symposium on, vol. 1, pp. 374-377, 2004.
- [9] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *Signal Processing Magazine, IEEE*, vol. 17, pp. 20-46, 2000.
- [10] Y. K. Lee and L. H. Chen, "High capacity image steganographic model," *Vision, Image and Signal Processing, IEE Proceedings -*, vol. 147, pp. 288-294, 2000.
- [11] W. Lu, H. Lu, and F.-L. Chung, "Robust digital image watermarking based on subsampling," *Applied Mathematics and Computation*, vol. 181, pp. 886-893, 2006.
- [12] F. A. P. Petitcolas, "Watermarking schemes evaluation," *I.E.E.E. Signal Processing*, vol. 17, no. 5, pp. 58-64, September 2000
- [13] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," *Proceedings of the IEEE*, vol. 87, pp. 1062-1078, 1999.
- [14] A. A. Reddy and B. N. Chatterji, "A new wavelet based logo-watermarking scheme," *Pattern Recognition Letters*, vol. 26, pp. 1019-1027, 2005.
- [15] H. Ren-Junn, K. Chuan-Ho, and C. Rong-Chi, "Watermark in color image," *Proceedings of the first International Symposium on Cyber Worlds*, pp. 225-229, 2002.
- [16] B. Verma, S. Jain, D. P. Agarwal, and A. Phadikar, "A New color image watermarking scheme," *Infocomp, Journal of computer science*, vol. 5,N.2, pp. 37-42, 2006.
- [17] X. Wu and Z.-H. Guan, "A novel digital watermark algorithm based on chaotic maps," *Physics Letters A*, vol. 365, pp. 403-406, 2007.