PATTERN-BASED FRAGILE WATERMARKING FOR COLOR IMAGES

Kuo-Cheng Liu

Information Educating Center, Taiwan Hospitality & Tourism College, Taiwan

ABSTRACT

In this paper, a fragile watermarking scheme for color images is proposed. Tamper proofing and high-quality recovery can be achieved by using the self-embedding watermarking scheme. The embedding information including feature information, block-edge-pattern information, and authentication information are appropriately distributed over luminance and chrominance components of the color image in the YC_bC_r color space such that the quality of the watermarked image can be better obtained. In the process of tamper proofing, a multiple-option parity check method and morphological operations. The former is used to verify authentication information for obtaining better results of tamper proofing and the later is used to further improve the neighborhood connectivity of the results. In the process of tamper recovery, the feature information of the host color image and its corresponding block-edge-pattern information are properly extracted to achieve high-quality recovery of the tampered image. The simulation results show that the proposed watermarking scheme can effectively proof the tempered region with high detection rate and can restore the tempered region with high quality.

1. INTRODUCTION

Depending on the objective of application, watermarking schemes are simply classified into fragile watermarking and robust watermarking schemes. The robust watermarking scheme is developed for copyright protection of images, while the fragile watermarking scheme is designed for image authentication. In [1]-[5], the watermarking methods for image authentication can be found. Besides tamper proofing for authentication of the image, a variety of watermarking methods were further developed to recover the tampered region [6]-[8]. Lin et al. [6] presented the block-wise and content-based watermarking method for image authentication and recovery. Authors in [7] proposed a watermarking method not only to achieve tamper detection and recovery but also to verify the ownership of the copyright. In [8], a dual watermarking scheme that provides second chance for tamper detection and recovery was proposed to increase the recovery rate while high percentage of the watermarked image was tampered.

However, a few attempts have been made to color image authentication. The color image watermarking schemes for authentication that have been relatively developed can be found in [9]-[12]. While most color image watermarking schemes concentrate on the efficiency of tamper detection, the improvement of visual quality of the recovered color image is not discussed. In this paper, we propose a self-embedding watermarking scheme for color image tamper proofing and high-quality recovery. The proposed scheme focuses on the invisibility of the embedded watermark and the quality enhancement of the recovered color image for the tampered image. In the embedding process, the authentication information created by the local mean of blocks in luminance component of the host color image is inserted into the color image. Meanwhile, the proposed scheme appropriately distributes the feature information of the host color image and its corresponding block-edge-pattern information over luminance and chrominance components of the color image such that the embedded watermark is imperceptible. In the detecting process, a multiple-option parity check method and morphological operations are incorporated to perform the efficiency of tamper proofing. The embedded feature information and the embedded block-edge-pattern information can be extracted from the watermarked image to recover the tampered regions with high quality.

2. THE PROPOSED COLOR WATERMARKING SCHEME FOR TAMPER PROOFING AND RECOVERY

For the host image in the YC_bC_r color space, each color component is divided into non-overlapping blocks of size 2×2 for designing the proposed watermarking scheme. Then, a one-to-one block mapping method is required for the watermark embedding. The feature information and block-edge-pattern information of each block will be embedded into its mapping block. For a block of number b in the luminance component, its mapping block of number b_m is generated by a 1-D transformation that is based on the dynamic system proposed in [13] and is given by

$$b_m = (b \times p) \bmod K + 1 \quad (1)$$

where mod is the modulo operation, K is the number of blocks in the color component, and $p \in [0, K\text{-}1]$ is regarded as secret key. In this paper, p and K are co-prime to achieve one-to-one mapping. For each $b \in [0, K\text{-}1]$, $b_m \in [0, K\text{-}1]$ can be obtained by Eq. (1). The block mapping sequence is constructed by all the pairs of b and b_m. For simplicity, the same mapping sequence for luminance component is also applied to chrominance components for watermark embedding in this paper.

In the process of watermark generation, the blocks in Y, C_b, and C_r color components of the host color image at each specific position are assembled for watermark embedding and named by "triple block" in this paper. The triple blocks are embedded from the top to the bottom and from the left to the right in the host image. The watermark in the triple block is composed of feature information of 16 bits, pattern

 ISSN 2076-1465

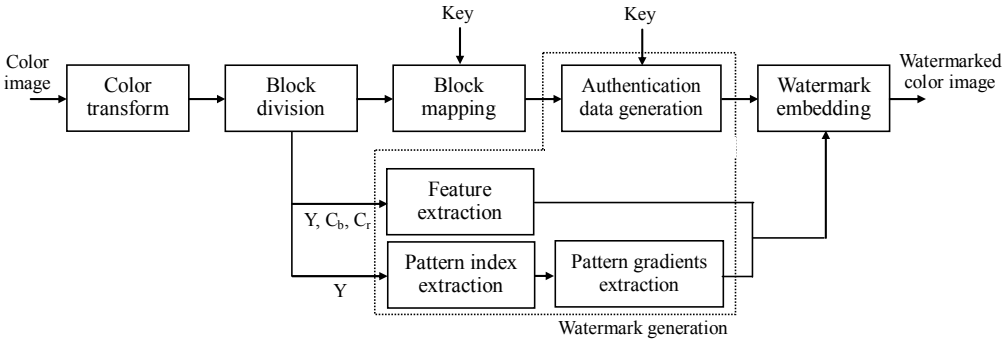


Fig. 1 The functional block diagram for watermark generation and embedding in the proposed watermarking scheme.

index of 4 bits, pattern gradient indices of 10 bits, and authentication information of 2 bits. As shown in Fig. 2 where color black represents the higher intensity level and color white represents the lower intensity level, the set of 14 block-edge-patterns is used. The pattern index for each block-edge-pattern is hence represented by 4 bits. By using the block mapping sequence, the feature information, pattern index, and pattern gradients indices of the triple block M are generated and embedded into its mapping triple block N (Fig. 3). The processes will be described as follows.

1. Compute the averages of Y, C_b, and C_r components in the triple block M, denoted by Ave_Y, Ave_C_b, and Ave_C_r, respectively.
2. Obtain the feature information of the triple block M by truncating the two LSBs of Ave_Y, the three LSBs of Ave_C_b and Ave_C_r, respectively (The notation suffix $_{(2)}$ means the binary form).
3. Find the pattern index of Y component in the triple block M by choosing the block-edge-pattern that best represents it from the pattern set.
4. Obtain the pattern gradient indices of Y component in the triple block M.
5. Set the two LSBs of each pixel within Y component of the triple block N to zero and compute the average intensity of the block, denoted by φ.
6. Generate the authentication information, in terms of parity-check bits α and β, of the triple block N as Eqs. (2) and (3)

$$\alpha = \begin{cases} \varphi_7 \oplus \varphi_6 \oplus \varphi_5, & \text{if } k_i \bmod 3 = 0 \\ \varphi_4 \oplus \varphi_3 \oplus \varphi_2, & \text{if } k_i \bmod 3 = 1 \\ \varphi_7 \oplus \varphi_6 \oplus \varphi_5 \oplus \varphi_4 \oplus \varphi_3 \oplus \varphi_2, & \text{otherwise} \end{cases} \tag{2}$$

$$\beta = \begin{cases} 0, & \text{if } \alpha = 1 \\ 1, & \text{if } \alpha = 0 \end{cases} \tag{3}$$

   where $\oplus$ is the exclusive-or operation, $\varphi_7\varphi_6\varphi_5\varphi_4\varphi_3\varphi_2\varphi_1\varphi_{0(2)}$ is in binary form of φ, $\{k_i\}$ is a pseudorandom sequence generated by a random seed that is a key of 2 bits in this paper.
7. Embed the watermark information into the triple block N.

In step 7, we propose a simple and modified parity check method of generating the authentication bit with multiple option strategy, in which the embedding authentication bits can play complementary roles in resisting various kinds of attacks. By considering the sensitivity of human visual perception to luminance and chrominance components, more watermark information bits are embedded into the chrominance components that is less sensitive than the luminance component for human eyes.

In the process of tamper proofing, the watermarked color image is firstly transformed to the YC_bC_r color space and each color component is then divided into non-overlapping blocks of size 2×2. The tamper proofing for the triple block, Q^w, is detailed as follows.

1. Extract the authentication information α^w and β^w from Q^w.
2. Set the two LSBs of each pixel within Y component of the triple block Q^w to zero and compute the average intensity of the block, denoted by φ^w.
3. Compute the parity-check bits according the pseudo-random sequence $\{k_i\}$ generated by using the key information.

$$\alpha^c = \begin{cases} \varphi_7^w \oplus \varphi_6^w \oplus \varphi_5^w, & \text{if } k_i \bmod 3 = 0 \\ \varphi_4^w \oplus \varphi_3^w \oplus \varphi_2^w, & \text{if } k_i \bmod 3 = 1 \\ \varphi_7^w \oplus \varphi_6^w \oplus \varphi_5^w \oplus \varphi_4^w \oplus \varphi_3^w \oplus \varphi_2^w, & \text{otherwise} \end{cases} \tag{4}$$

$$\beta^c = \begin{cases} 0, & \text{if } \alpha^c = 1 \\ 1, & \text{if } \alpha^c = 0 \end{cases} \tag{5}$$

4. Mark Q^w invalid if α^c and α^w are unequal or β^c and β^w are unequal; otherwise, mark it valid.
5. Generate a binary image, I_b, to mark the location of valid and invalid blocks, on which the bit corresponding to the location of the valid block is set to "0" and the bit corresponding to the location of the invalid block is set to "1".
6. Perform morphological operations on the binary image and give the final tamper detection result as

   $I_{fb} = erode(\, dilate(\, I_b, SE\,), SE\,)$

   where *dilate* is the dilation operation, *erode* the erosion operation, and *SE* the structuring element. Herein, the 3×3 standard 8-connected structuring element is adopted. The rule of *dilate* is that the output is set to "1" if any of the binary pixels under the slide window of the structuring element is "1". On the other hand, the rule of *erode* is that the output is set to "0" if any of the binary pixels under the slide window of the structuring element is "0".

In step 6, two fundamental morphological operations, including dilation and erosion, are sequentially applied to I_b

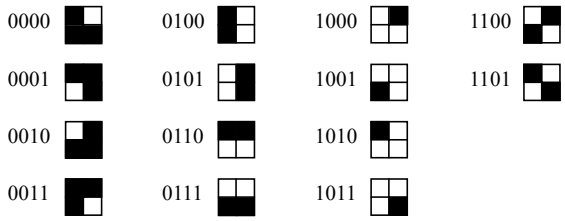


Fig. 2 Set of block-edge-patterns and the corresponding pattern indices.

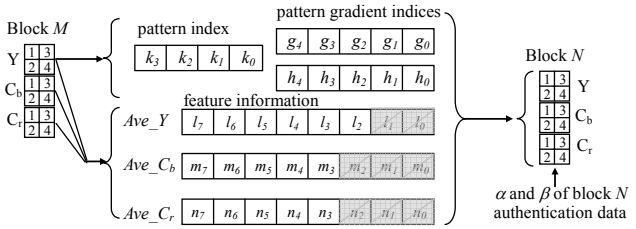


Fig. 3 Binary watermark generation and embedding for the triple block M and its mapping triple block N consisting of pixels 1, 2, 3, and 4 in Y, C_b, and C_r components (gray region means the truncating bits).

to improve the neighborhood connectivity of the invalid region. Dilation can effectively link the contour of the invalid region in the binary image, while erosion can remove the noise on the boundary of the invalid region in the binary image.

The recovery of the tampered image is followed by the tamper proofing. For a tampered triple block, denoted by Q^t, the procedure of recovering the tampered triple block is summarized in the follows.

1. Use the key information and Eq. (1) to find the triple block, S^w, where the recovery data of Q^t is embedded.
2. Skip the recovery of Q^t if the triple block S^w is invalid.
3. If the triple block S^w is valid, extract the two LSBs of each pixel within Y component and the three LSBs of each pixel within C_b and C_r components of S^w to obtain the recovery data represented by binary form.

3. SIMULATION RESULTS

To justify the validity of the proposed watermarking scheme, the simulation of embedding watermark in color images of 512×512 pixels is conducted, where color pixels are represented in 24-bit YC_bC_r format. The performance in terms of the quality of the watermarked image and the recovered image is inspected. In the experiments, a variety of color images are used for watermark embedding. The PSNR values of all the watermarked color images are shown in Table I. The high PSNR values of the watermarked images mean that a large amount of the watermark information (i.e., the reduced content of the host color image) can be invisibly embedded into the color image by the proposed watermarking scheme without degrading the visual quality.

Through detecting and restoring the changed content of the watermarked color image, the performance of tamper proofing and recovery of the proposed watermarking scheme can be identified. In the experiments, the attack procedure of the watermarked image is implemented by removing symbols from the image, inserting patterns into

Table. I PSNR of the color watermarked image obtained by using the proposed fragile watermarking scheme.

Image	PSNR of the watermarked images
Sign	40.02dB
Sail	40.23dB
Zuerist	40.59dB
Pepper	39.84dB
Monarch	40.18dB

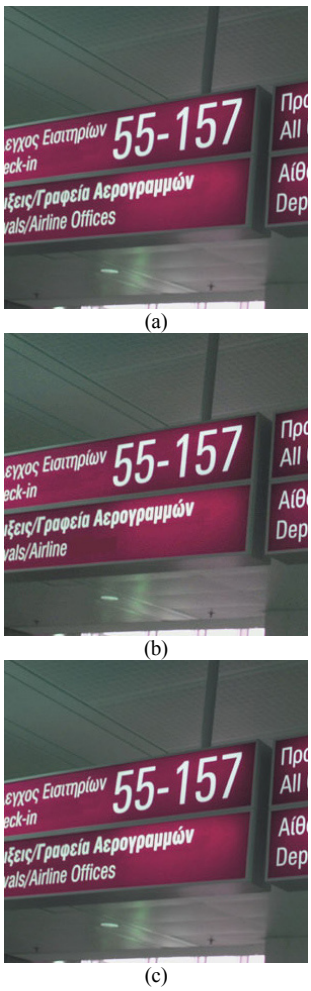
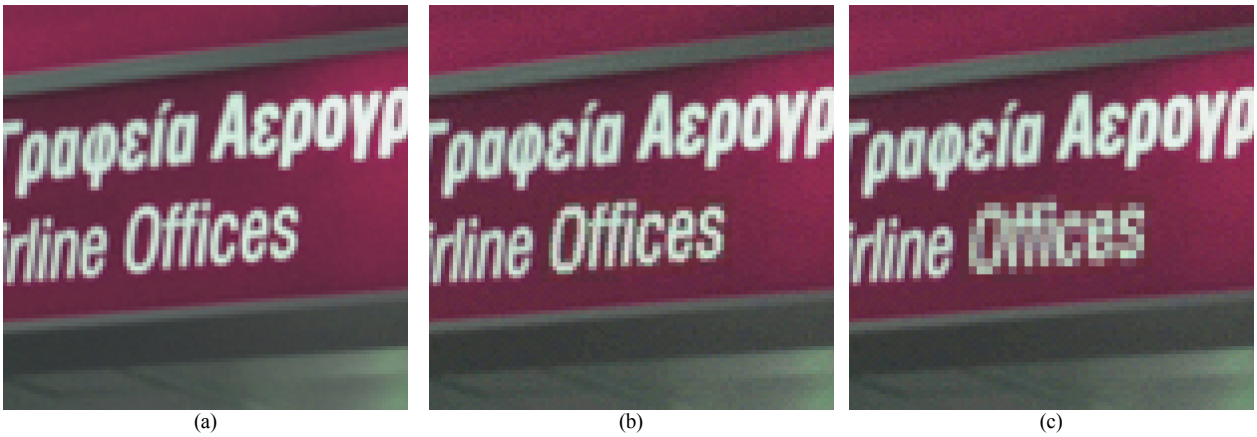


Fig. 4 Tamper proofing and recovery of the tampered "Sign" color image (a) original "Sign" color image, (b) tampered "Sign" color image, and (c) recovered image (PSNR=39.68dB).

the image, or modifying colors in the image. The original "Sign" color image is shown in Fig. 4a where an English word "Offices" on its watermarked image is removed to simulate the attack procedure. The tampered "Sign" color image is shown in Fig. 4b. The result of the tamper proofing is given in Fig. 4c. It is clearly shown that the removed region can be completely detected by means of the multiple-option parity check method and the morphological operations. Meanwhile, the tampered region is fully restored by the proposed watermarking scheme. The PSNR of the recovered "Sign" image is 39.68dB. The proposed scheme indeed successfully integrates the feature information and its corresponding block-edge-pattern information of the "Sign" color image to recover the tampered image.



(a) (b) (c)

Fig. 5 Close-up view of part of the recovered "Sign" image for comparison. (a) part of the enlarged original "Sign" image, (b) the same part of the recovered "Sign" image (PSNR=39.68dB) given by the proposed watermarking scheme, and (c) the same part of the recovered "Sign" image (PSNR=38.11dB) given by the proposed watermarking scheme without using the block-edge-pattern.

In the simulation results, the improvement of the recovery quality by incorporating the block-edge-pattern information should be verified. The recovery quality achieved by the proposed scheme without using the block-edge-pattern information is compared. In Fig. 5, a close-up view of part of the recovered "Sign" image obtained by using the proposed watermarking scheme is compared with that obtained by using the proposed watermarking scheme without utilizing the block-edge-pattern information, while the watermarked "Sign" image is attacked as shown in Fig. 4b. Part of the enlarged original "Sign" image is shown in Fig. 5a. In fig. 5b, the same part of the recovered "Sign" image (PSNR=39.68dB) obtained by using the proposed watermarking scheme is depicted. The same part of the recovered "Sign" image given by the proposed watermarking scheme without using the block-edge-pattern information is shown in Fig. 5c at the PSNR of 38.11dB. It can be found that the visual quality of Fig. 5b is obviously better than that of Fig. 5c, so the high visual quality of the recovered color image can be successfully achieved by using the proposed pattern-based fragile watermarking scheme.

4. CONCLUSIONS

Based on the fact that the embedded watermark is indeed the reduced image generated from the host color image, a self-embedding watermarking scheme for color image tamper proofing and recovery in the spatial domain is proposed in this paper. A simple structure of the watermark information has been organized for the proposed watermarking scheme. The watermarked color image that is visually indistinguishable with the host image is obtained by adequately distributing the watermark over luminance and chrominance components of the host color image. A multiple-option parity check method is successfully incorporated with morphological operations to perform tamper proofing with high detection rate. The method of recovering the tampered image from the extracted watermark information has also been devised for the quality improvement of the restored color image. The proposed scheme outperforms the relevant existing scheme in deriving not only higher quality of the watermarked color image but also higher quality of the recovered color image.

REFERENCES

[1] H.-T. Lu, R.-M. Shen and F.-L. Chung, "Fragile watermarking scheme for image authentication," *Electronics Letters*, vol. 39, no. 12, pp. 898-900, 2003.

[2] X. Zhou, X. Duan, and D. Wang, "A semi-fragile watermark scheme for image authentication," *Proc. the 10th Int. Multimedia Modelling Conf.*, 2004, pp. 374-377.

[3] X. Wu, J. Hu, Z. Gu, J. Huang , "A Secure Semi-Fragile Watermarking for Image Authentication Based on Integer Wavelet Transform with Parameters," *Proc. Australian Workshop on Grid Computing and E-Research*, vol. 44, 2005, pp. 75-80.

[4] C.-T. Li and Huayin Si, "Wavelet-based fragile watermarking scheme for image authentication," *Journal Electron. Imaging*, vol. 16, no. 1, 013009, 2007.

[5] H.-J. He, J.-S. Zhang, and F. Chen, "Adjacent-block based statistical detection method for self-embedding watermarking techniques," *Signal Processing*, vol. 89, no. 8, pp. 1557-1566, 2009.

[6] P.-L. Lin, C.-K. Hsieh, and P.-W. Huang, "A hierarchical digital watermarking method for image tamper detection and recovery," *Pattern Recognition*, vol. 38, pp. 2519–2529, 2005.

[7] S. D. Lin, Y.-C. Kuo, and M.-H. Yao, "An image watermarking scheme with tamper detection and recovery," *Int. Journal of Innovative Computing, Information and Control*, vol. 3, no. 6, pp. 1379-1387, 2007.

[8] T.-Y. Lee and S. D. Lin, "Dual watermark for tamper detection and recovery," *Pattern Recognition*, vol. 41, no. 11, pp. 3497-3506, 2008.

[9] C. Gaël, C. Dinu, and T. Alain, "Watermarking and authentication of color images based on segmentation of the xyY color space," *Journal of Imaging Science and Technology*, vol. 50, no. 5, pp. 411-423, 2006.

[10] Z. Peng and W. Liu, "Color image authentication based on spatiotemporal chaos and SVD," *Chaos, Solitons & Fractals*, vol. 36, no. 4, pp. 946-952, 2008.
[11] M. S. Wang and W. C. Chen, "A majority-voting based watermarking scheme for color image tamper detection and recovery," *Computer Standards & Interfaces*, vol. 29, pp. 561-571, 2007.
[12] H. Mirza, H. Thai, and Z. Nakao, "Color image watermarking and self-recovery based on independent component analysis," *Lecture Notes in Computer Science*, vol. 5097, pp. 839-849, 2008.
[13] G. Voyatzis, I. Pitas, "Chaotic mixing of digital images and applications to watermarking," in *Proc. European Conf. Multimedia Applications Services and Techniques*, 1996, pp. 687–689.