2012 IACSIT Hong Kong Conferences
IPCSIT vol. 30 (2012) © (2012) IACSIT Press, Singapore

Moment-preserving Based Watermarking for Color Image Authentication and Recovery

Kuo-Cheng Liu+

Information Educating Center, Taiwan Hospitality & Tourism College, Hualien, Taiwan

Abstract. In this paper, the color image authentication and recovery method using the moment-preserving method is proposed. The color image is partitioned into non-overlapping blocks for watermark embedding. The watermark for each block consists of its authentication data and the corresponding feature information that is composed of a bit map and two representative pixel values. The bit map and the two representative pixel values are computed bythe moment-preserving technique. In the proofing process, we check authentication data to obtain the results of tamper proofing. In the recovery process, the feature information of each block embedded into the color image is rebuilt for high quality recovery. The simulation results show that the proposed watermarking scheme can effectively proof the tempered region with high detection rate and can recover the tempered region with high quality and outperforms the relevant existing method.

Keywords: tamper proofing, moment-preserving technique, tamper recovery.

1. Introduction

In [1], [4], [6], watermarking methods were developed to achieve the image tamper proofing. By utilizing the embedding watermark information, the image authentication can be used to detect the tampered region. In order to authenticate the image and recover the tampered region while the image is forged, various watermarking methods [2], [3], [5] were further proposed. The watermarking schemes for tamper detection and recovery of color images can only be found in [7]-[9]. Based on a majority-vote technique takes all authentication data into account to detect tampered blocks, a watermarking schemefor color image tamper detection and recovery was proposed in [7]. In [8], the local features of imageblocks and the global features of the original colorimage are embedded into red, green, and blue color channels for authentication. Through block mapping and a color model, the recovery data bits are generated for tamper recovery. A tamper detection and self-recovery algorithm based on the robust embedding of the dual visual watermarks that usediscrete wavelet transform and singular value decomposition was proposed in [9]forcolorimages. However, the improvement of visual quality of the recovered color image is not discussed while most color image watermarking schemes concentrate on the efficiency of tamper detection.

In this paper, we propose a watermarking scheme for color images. The high visual quality of the recovered color image for the tampered image and the improvement in the proofing process are focused. Based on the moment-preserving technique, the tampered region of the color image can be recovered with two representative color vectors such that certain color moments of the block in the region can be preserved while the proofing result is obtained.

+ Corresponding author. Tel.: +886-3-8653906; fax: +886-3-8653910.
E-mail address:kcliu@mail.tht.edu.tw.

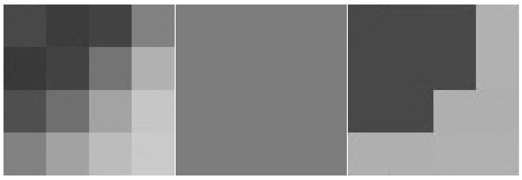

(a) (b) (c)

Fig. 1: Comparison of original image block and its recovered blocks: (a)original block; (b)recovered block by its mean values; and (c) recovered block by moment-preserving method.

2. Moment-Preserving Technique

Moment-preserving technique is able toclassify the pixels of a given image into two groups. The pixels in each group are assigned to a certain gray value such that the moment of the image can be preserved. In this technique, a threshold is selected to group the pixels with the gray values above the threshold, and other pixels with gray values equal to and below thethreshold. The threshold selection method that can be used to preserve the moment of the image is incorporated into the proposed watermarking scheme such that the tampered region of the color image can be recovered with high quality while the proofing result is obtained. Based on the moment-preserving principle, we apply the threshold selection method proposed in [10] to the watermarking scheme presented in this paper.

For the bi-level thresholding method, the objective is to select a threshold valuesuch thatthe moments of the image $I$are preserved in the thresholdedbi-level image B. B is obtained by replacing the pixels in I with specified gray values. That is, the pixels below the threshold are replaced by $t_u$and the pixels above the threshold are replaced by t_v. The following equations are achieved for the bi-level thresholding method and the threshold ,t_u, and t_v can be obtained by using the equations [10].

$$f_u t_u^s + f_v t_v^s = m_s,\ s=0,\ 1,\ 2,\ 3 \quad (1)$$

Wheref_u and f_v are the fractions of the pixelswith gray value t_u and with gray value t_v, respectively and m_s means the s-th moment of the image I.

In the watermarking scheme for authentication and recovery,the image is firstly divided into non-overlapping blocks for block mapping. The block mapping process is used to embed the feature information of one block to its mapping block. The feature information of each block is essentially the statistics of the block in the image for recovery of the tampered region. While the watermarked image is tampered by malicious attacks, the block in the tampered region can be restored by the corresponding feature information. In these works, the feature information of each block is regarded as the reduced content of the block and is actually its average intensity. Figs. 1a and 1b show the original block pattern and the recovered block pattern after recovering with the average intensity, respectively. It is obviously that the recovery quality is unsatisfied, especially when the image is treated as the evidence for the court judgment. For the tampered block, the threshold and the two representative values given by the moment-preserving technique can be adequately used to recover the block with better quality. Fig. 1c depicts the processed block patterns after applying the moment-preserving technique.

3. The Proposed Color Image Watermarking Scheme

A new watermarking scheme for color image authentication in spatial domain is devised in anattempt to match the characteristics of the color space better. Herein, the YC_bC_r color spaceis adopted for the design of the proposed watermarking scheme, since the color pixel in this space is separated into luminance and chrominance components such that thewatermark information can be easily embedded. Meanwhile, the majority of edges and texturesinthe color image appear in the luminance component where the moment-preserving method can be efficiently utilized to achieve high quality recovery. The framework of the embeddingprocessincludes block division and mapping, watermark generation, and watermark embedding.

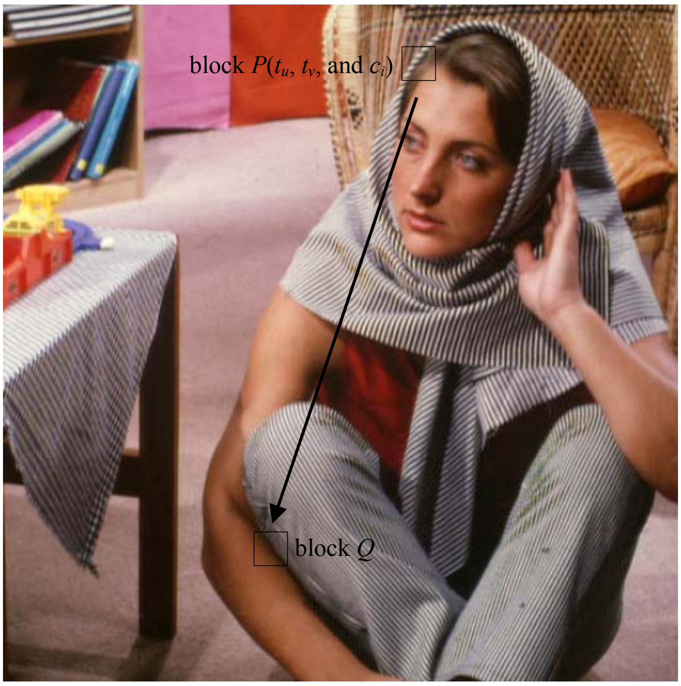


Fig. 2: The relationship between block P and its mapping block Q.

For the host image in the YC_bC_r color space, each color component is divided into non-overlapping blocks of size 4×4 to design the proposed watermarking scheme. Then, a one-to-one mappingamong blocks used in [11] is required for the watermark embedding. The feature information of each block will be embedded into its mapping block.For simplicity, the same mapping sequence is used for each color component in this paper.By using the block mapping sequence, the feature informationofblock P and its corresponding authentication data are generated and embedded into its mapping block Q (Fig. 2). The processes of watermark generation and embedding are described as follows.

1. Compute a threshold value$t$ and two representative gray values, t_u and t_v, for block P such thatthe moments of the block $P$and the moments of the thresholdedbi-level block P are equal or nearly equal.
2. Use t to generate the bit map of block P in which each bit assigned by 1 or 0 indicates whether the block pixel value is assigned to t_u or t_v.
3. Obtain the feature information, c_i i=1, 2, 3, …, 16, for representing the bit map of block P and , $x_7x_6x_5x_4x_3x_{2(2)}$ and $y_7y_6y_5y_4y_3y_{2(2)}$, for representing the two representative values of block P by truncating the two LSBs of g_x and g_y, respectively (The notation suffix $_{(2)}$ means the binary form).
4. Set the two LSBs of each pixel within block Q to zeroandcompute the average intensity of the block, denoted by κ.
5. Embed the watermark information given by Steps 3 and 5 into block Q.

The watermark proofing is then carried out by comparing the extracted authentication data with the computing authentication data. For a tampered block, denoted by Q^t, the procedure of recovering the block is to firstly find the block, R^k, where the recovery data or feature information of block Q^t is embedded. Then, the extracted feature information is used to restore the tampered block.

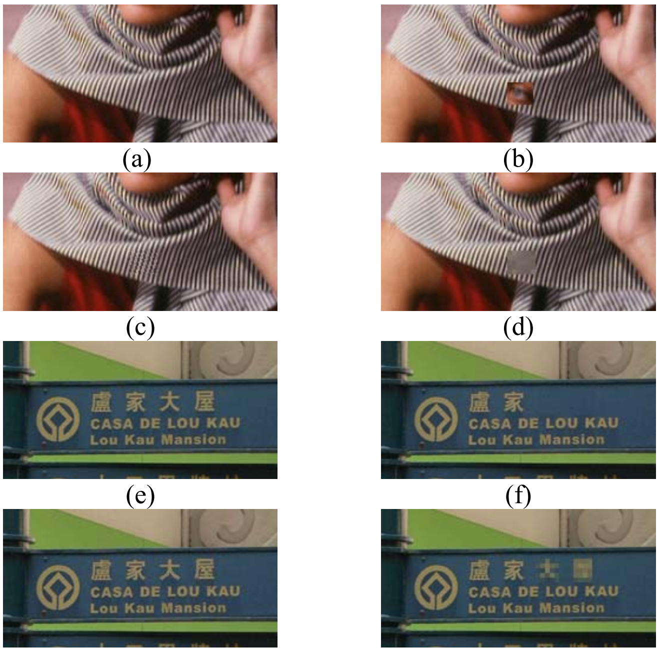
4. Simulation Results

To evaluate the validity of the proposed watermarking scheme, the results of tamper proofing and recovery for the watermarked color images are major concerned while the watermarked image is tampered by malicious attacks. The proposed scheme is also compared with the existing color image watermarking scheme to verify the superiority of the proposed watermarking scheme

Two test color images used in the simulation are presented in Figs. 3a and3b, respectively. By applying the proposed watermarking scheme to the test color image, the watermarked color image is obtained by self-embedding the watermark, including authentication data and feature information of each non-overlapping

(a) (b)

Fig. 3: Original color images for watermarking: (a) “Barbara” and (b) “Sign”



(a) (b) (c) (d) (e) (f) (g) (h)

Fig. 4: Comparison of close-up view of the recovery results for different tampered color images:
(a), (e): part of the original “Barbara” and“Sign” images, respectively;
(b), (f): tampered images of the same part;
(c), (g): recovery results (“Barbara”: 40.81dB and “Sign”:40.98dB) of the tampered images by using the proposed watermarking scheme;
(d), (h): recovery results (“Barbara”: 40.15dB and “Sign”:40.07dB) of the tampered images by using the Lin’s scheme.

block, into the test color image. The watermarked color image is indistinguishable with its original color image for human visual perception. The PSNR values of the watermarked color images are all higher than 42dB. The proposed watermarking scheme successfully embeds watermark informationinto three components of the color image in the YC_bC_r color space to achieve high quality of the watermarked color image.

To further confirm the performance of the proposed scheme in terms of the visual quality of the recovered image, the proposed watermarking scheme is compared with the representative method. Lin’s method proposed in [2] is applied to each color component for color images with 4×4 blocks for a fair comparison. Herein, a close-up view of the recovery results is illustrated in Fig. 4 to clearly verify that the recovery of the tempered region, especially the small texture region,can be obtained by the proposed scheme with high quality. Figs. 4b and 4f depict a close-up view of the tampered “Barbara” image and “Sign” image, respectively. The same part of the original color images are shown in Figs. 4a and 4e, respectively. The recovery result of the tampered “Barbara” image obtained by using the proposed watermarking scheme is shown in Fig. 4c and the result by using the Lin’s scheme is shown in Fig. 4d. It can be seen that the visual quality of the recovered image by the proposed watermarking scheme is better than that by the Lin’s scheme. The Chinese words restored by using the proposed scheme are easily recognized by human perception. Figs. 4g and 6h compare the recovery results of the tampered region on the left eye in the “Sign” image. The proposed watermarking schemeeffectively utilizes the moment-preserving method to recoverthe edge and texture information in the tampered region with high visual quality.

5. Conclusions

In this paper, a watermarking schemeusing the moment-preserving techniquefor color images has been proposed. The proposed watermarking method can be applied to color images for tamper proofing and recovery. The visual quality of the recovered color image is efficiently improved while proofing the tampered region. An effective and low-complexity tamper proofing method is also given. The proposed scheme outperforms the relevant existing scheme in deriving higher quality of the recovered color image while the watermarked image is nearly lossless with the original image.

6. Acknowledgement

The work was supported by the National Science Council, R.O.C., under contract NSC100-2221-E-278-002.

7. References

[1] H.-T. Lu, R.-M. Shen and F.-L. Chung, “Fragilewatermarking scheme for image authentication,” ElectronicsLetters, vol. 39, no. 12, pp. 898-900, 2003.

[2] 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.

[3] 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.

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

[6] 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.

[7] 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.

[8] N. Wang and C.-H. Kim, ”Color image of tamper detection and recovery using block-based watermarking,”in Proc. Int. Conf. Embedded and Multimedia Computing, 2009, pp. 1-6.

[9] N. Wang and C.-H. Kim, ”Tamper detection and self-recovery algorithm of color image based on robust embedding of dual visual watermarks using DWT-SVD,”in Proc. Int. Symp. Communications and Information Technology, 2009, pp. 157-162.

[10] W.-H. Tsai, “Moment-preserving thresholding: A new approach,”Computer Vision Graphics, and Image Processing, vol. 29, pp. 377–393, 1985.

[11] 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.