Stereo Image Watermarking Method for Authentication with Self-Recovery Capability

Jing Wang[1], Gangyi Jiang[1,2], Fen Chen[1], Xingbin Zeng[3], Xiaodong Wang[1], Mei Yu[1,2], Yo-Sung Ho[4]

1. Faculty of Information Science and Engineering
Ningbo University
Ningbo, China
jianggangyi@126.com

2. National Key Lab of Software New Technology
Nanjing University
Nanjing, China

3. Ningbo Sunrun Electronic Information Science and Technology Development Co., Ltd
Ningbo, China

4. Department of Information and Communication,
Gwangju Institute of Science and Technology
Gwangju, South Korea

***Abstract*—To address issues of content authenticity verification and integrity protection, a stereo image watermarking method based disparity is proposed. Firstly, the stereo image blocks are classified into eight types according to the smoothness of it, and the alterable-length recovery bits are generated. The recovery bits include foremost bits, detail bits, type bits and disparity bits. Foremost bits are embedded twice for improving quality of recovery. Moreover, disparity is embedded as well for recovery further. At the receiver side, recovery bits extracted from watermarked stereo image not only localize tampered regions, but also recover them. The visual quality of the watermarked stereo image is imperceptible due to the low embedding volume. Experimental results show that the proposed method can detect tamper precisely and provide high restoration quality.**

Keywords-stereo image; fragile watermarking; tamper localization; self-recovery

I. INTRODUCTION

With the development of three dimensional (3D) video and image technologies [1], the challenging task of protecting 3D products becomes more and more important. Digital watermarking [2] has been used as one of the effective approaches for the solution of the copyright and authentication problems which restrict the development of 3D video and image industry. Various digital watermarking methods have been proposed and are sorted into three categories: robust, fragile and semi-fragile watermarking.

Robust watermarking method has been used for ownership verification. Fragile and semi-fragile watermarking methods are proposed for checking the authenticity and integrity [3]. Fragile watermarking is sensitive to any slight alterations. Semi-fragile watermarking techniques are robust to some manipulations such as JPEG compression and Gaussian low-pass filtering [4], and sensitive to malicious attack, such as cropping and content replacement. The goal of this work is on fragile watermarking.

Fragile watermarking methods have been developed in recent years. Wong [5] divided a host image into small blocks and embedded the watermark into each block. The fragile watermarking techniques, which not only locate the fake region, but also recover the tampering region, are more practically and comprehensively applied. To accurately identify the tampered blocks, Lin et al. [6] proposed a hierarchical digital watermarking scheme for tamper detection and recovery, and he used a 3-level hierarchical structure to locate the tampered regions, but there was no second chance to recover tampered blocks whose watermark bits embedded in the other block were destroyed. To overcome this problem, Qian [7] hided the restoration-bits into the 3-LSB layers of the host image to improve the reconstructed image quality, the quality of recovered image was improved, but the quality of watermarked image decreased due to the increased watermark payload. In [8], the quantized DCT coefficients of each block replaced the 2-LSB of another block. If the image was tampered, the restoration-bits could be extracted and used to restore the tampered regions, but the quality of the recovered image was not high enough. To improve the reconstruction quality, Qin [9] proposed a fragile watermarking method with content restoration capability using an adaptive bit allocation mechanism. The image blocks were coded with the dynamic lengths based on the blocks degree of smoothness and the watermark were embedded into the 1-LSB plane of the cover image. Nevertheless, if the bits of type indicator were changed in the decoding of watermark, the method could not localize or restore the tampered regions.

Above watermarking methods are all focused on monocular images, few fragile watermarking methods for 3D media had been proposed. A stereo image consists of a pair of images: left and right images composing the same scene are taken by two cameras corresponding to the left and right eye-views. The slight difference between the left and right images is called disparity, which makes stereo image realistically, and the images have relationship with each other. Stereo image watermarking method is different from the monocular image watermarking.

In this paper, we propose a fragile watermarking method with self-recovery capability. The proposed method divides the host images into blocks based their degree of roughness, and allocates dynamic lengths to represent the watermark. At the receiver side, the tampered blocks are localized and restored with high quality by making use of the disparity and recovery bits.

II. PROPOSED WATERMARKING ALGORITHM

To address the content authenticity verification of stereo image and on the basic of analyzing Huo's method [10], stereo image watermarking method for authentication with self-recovery capability is proposed. Let $I_l(i,j)$ and $I_r(i,j)$ ($1\le i\le M$, $1\le j\le N$) denote the pixel values of left and right images with the size of $M\times N$, and generate the dynamic lengths watermark bits based content. The watermark bits are embedded into 1-LSB and 2-LSB of images. The proposed watermarking method consists three sections including watermark embedding, tamper detection and content restoration.

A. Watermark Embedding

The left and right images are divided into non-overlapping blocks Z_i and Y_i with size of 8×8. Set the 1-LSB and 2-LSB of images are zero. Transform image block into the frequency domain by using discrete cosine transform (DCT), and quantize the DCT coefficients according to the JPEG quantization. The quantized DCT coefficients are arranged in zigzag order from low-frequency to high-frequency, Fig.1 gives an illustration of the watermark embedding process.

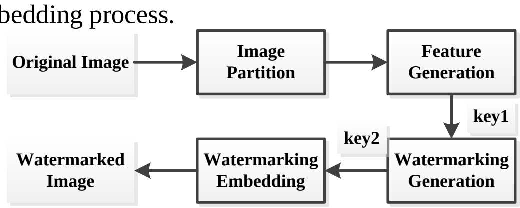


Figure 1. Watermarking embedding flowchart.

The alterable-length bits of the block Z_i include foremost-bits F_i, type-bits T_i, disparity-bits X_i and detail-bit D_i, the block Y_i includes foremost-bits F_i, type-bits T_i, and detail-bit D_i. The length of F_i, T_i, X_i, is 20, 3 and 5 respectively, the length of D_i depends on the type of the block.

The method of generating F_i, T_i, X_i, D_i is described as follows. Foremost-bits F_i are produced with the binary sequence of first three coefficients in zigzag order. The number of bits which are distributed to denote the coefficients is shown in Fig.2. For instance, the DC is converted into binary number with 8 bits; the number of F_i is 20. Type-bits T_i are determined by the number of non-zero coefficients in quantized matrix. Let X_k (k=0,1,…,7) denote the block type index. If the number of non-zero coefficients falls into the scope of the number of non-zeros as shown in Tab.I, the k is the corresponding type block. The type-bits are the k of binary number with 3 bits. The detail bits is the binary sequence of quantized DCT coefficients of which the number depend on the type of the block, and the number of bits which are used to represent the coefficients is based on the Fig.2. For instance, the type of the block is X_4, the number of coding coefficients is 18 and the coding sequence consists 83 bits. The block disparity of left image in the reference of right image is computed. If the block is matched well, the disparity-bits are represented with 5bits.

The blocks of left and right image are classified into eight types and seven types based on the roughness of block content and disparity respectively. The alterable-length watermark L_i and R_i of block can be described respectively by

$$L_i=C(Z_i)= F_i \parallel F_i \parallel (T_i \parallel D_i \parallel B_i) \quad (1)$$

$$R_i=C(Y_i)=F_i \parallel F_i \parallel (T_i \parallel D_i) \quad (2)$$

Where, C(.) represents the coding operation, ‖ denotes the concatenation of bits.

TABLE I. CODING INFORMATION FOR DIFFERENT TYPES OF BLOCKS

Type block	Number of coding	Number of non-zeros	length
X_0	3	[0~1]	23
X_1	10	[2~5]	54
X_2	11	[6~7]	57
X_3	12	[8~10]	63
X_4	18	[11~15]	75
X_5	80	[16~19]	83
X_6	94	[20~23]	97
X_7	98	[24~64]	101

8	6	5	4	3	2	2	2
6	5	4	3	2	2	2	0
5	4	3	2	2	2	0	0
4	3	2	2	0	0	0	0
3	2	2	0	0	0	0	0
2	2	0	0	0	0	0	0
2	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Figure 2. Tables for assigning the number of bits for coded coefficients.

After watermark bits are generated, the process of embedding consists of four steps.

Step1: Generate a pseudorandom binary matrix P={ $p_{i,k}|$ i=1,2,...,N, k=1,2,...,121}by the key1 .The watermark bits of left and right image are obtained by

$$w_{i,h}^{L} = p_{i,h} \oplus L_{i,h}, h = 1,2,\cdots,lengh + 20 \quad (3)$$

$$w_{i,h}^{R} = p_{i,h} \oplus R_{i,h}, h = 1,2,\cdots,lengh + 20 \quad (4)$$

where "$\oplus$"denotes the OR operation.

Step2: A pseudorandom matrix A={$a_{t,i}$|t=1,2,3, i=1,2,…,N} is generated by the key2 , sort A and obtain the index matrix M={$m_{t,i}$|t=1,2,3, i=1,2,…,N}, that is, the first, second and third mapping block of Z_i is $Y_{i',1}$,$Y_{i',2}$ and $Y_{i',3}$ in right image, similarity, $Z_{i',1}$,$Z_{i',2}$ and $Z_{i',3}$ are the mapping blocks of Y_i , where, $i'= m_{t,i}$.

Step3: Divide the watermark into three parts, the first part consist 20 bits, the second part consists 10 bits, and the remaining bits are belonged to the third part.

Step4 : Embed the three parts watermark of block Z_i into the mapping block $Y_{i',1}$,$Y_{i',2}$ and $Y_{i',3}$ and embed the three parts watermark of block Y_i into the mapping block $Z_{i',1}$,$Z_{i',2}$

and $Z_{i,3}{}'$. If the number of the watermark bits is larger than 64, embed watermark into the 1-LSB and 2-LSB, otherwise, the watermark bits are embedded into the 1-LSB。

B. Tamper Detection

The watermark bits are extracted to authenticate the test image and localize the damaged regions. Furthermore, the detected damaged regions will be recovered. The process of extracting the embedded bits from the 2-LSB plane of test image is the inverse process of embedding. Authentication and localization of the damaged blocks are determined by comparison the extracted authentication-bits and calculated-bits. Let G and G_i denote the received image and block with the size of 8×8, E_i and Hi denote the authentication-bits and calculated-bits respectively. The verification process consist the following steps.

Step1: For each block G_i, detection indicators could be calculated as follows:

$$g_i = \begin{cases} 0, & if\ \ E_i = H_i \\ 1, & otherwise \end{cases} \tag{5}$$

Step2: Let β_i represents the tampering log and the optimization result can be shown as follows:

$$\beta_i = \begin{cases} 1, & if\ \ g_i = 1 \,\&\, \delta_i \geq \eta_i \,\&\, \delta_i > 0 \\ 0, & otherwise \end{cases} \tag{6}$$

Where, δ_i and η_i represent the watermark consistency of eight neighborhood characterization. $\delta_i = \sum_{\varepsilon} g_{\varepsilon}, \varepsilon \in N\_8(i)$ and $\eta_i = \sum_{t=1}^{3} g_{a_{t,i}} / 3$

Step3: For each valid block after Step2, mark this block invalid if there are five or more neighboring invalid blocks in its eight-neighborhood.

C. Content Restoration.

After detecting the test image, all blocks are marked as valid or invalid. If the block is tampered, we recover the destroyed regions with the recovery watermark and the relationship of stereo image. The recovery process of left and right test images are as follows:

If the block of right image is tampered, verify its second and third mapping block. If the mapping blocks are valid, decoding the extracted recovery bits, then reverse quantization and DCT. Otherwise, we verify its first mapping block, if the block is valid, we use the foremost information to recover the tampered block; otherwise, the tamper are recovered by the image inpainting method [11].

If the block of left image is tampered, verify its second and third mapping block. If the mapping blocks are valid, decoding the extracted recovery bits, if the block has a matched block in right image, we use the matched block to recover it. Otherwise, we reverse quantization and DCT to recover the tampered block. If the blocks is tampered, we verify its first mapping block, If the block is valid, we use the foremost information to recover the tampered block; otherwise, those tampering coincident blocks are recovered by the image inpainting method.

III. EXPERIMENTAL RESULTS AND ANALYSES

Experiments are conducted on four stereoscopic image pair with the size 640×480 named "Altmoabit", "Akko_kayo", "Laundry" , and "Art", and left images are shown in Fig.3.

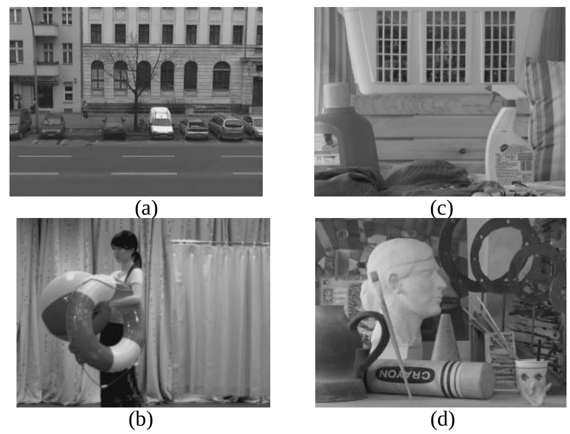


Figure 3. Original left images of four stereoscopic images: (a) Altmoabit, (b) Akko_kayo (c) Laundry (d) Art

Four stereoscopic image pairs are watermarked by using the proposed method. Tab.II lists the PSNR of watermarked images. Because of binocular suppression based asymmetrical stereo image [12], the watermarked stereo images are imperceptive. Watermarked images of "Altmoabit" are shown in Fig.4.

TABLE II. PSNR COMPARISONS FOR WATERMARKED IMAGES

	Quality of watermarked image(dB)			
	Altmoabit	***Akko_kayo***	***Laundry***	***Art***
Left	47.06	47.24	47.01	47.03
Right	49.51	49.79	48.96	49.22

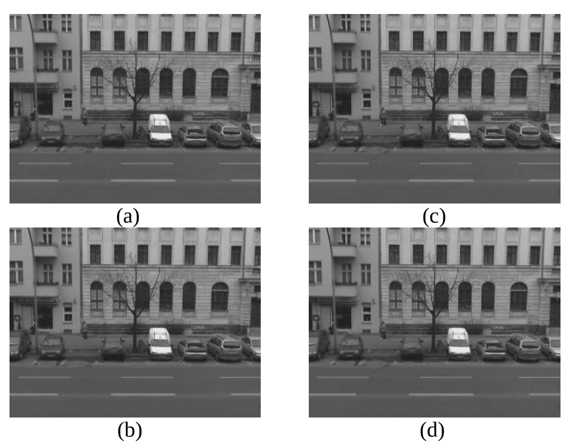


Figure 4. Watermarked stereo image: (a) original left image, (b) watermarked left image, (c) original right image, (d) watermarked right image:

A. Crop Attack

Four stereoscopic image pairs are cropped with the size 120×120, and the stereo image “Altmoabit” is used as example of the experiment. The stereo watermarked images, which are altered, are shown in Fig.5 (a) and (e), and the experiment results are shown in Fig.5. The detection results which are labeled with white are shown in Fig.5 (b) and (f). The restored images using are shown in Fig.5(c) and (g), the corresponding PSNR values of restored images are 39.22dB and 39.47 dB, respectively.

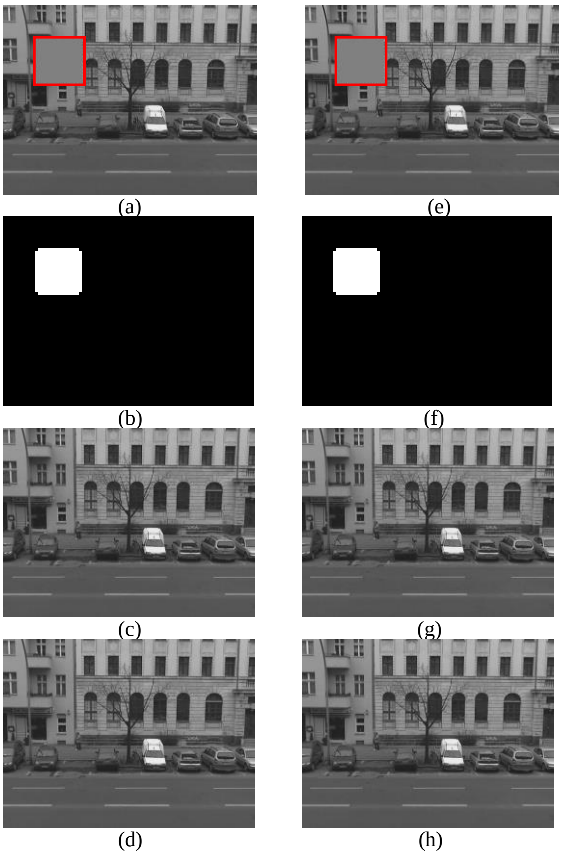


Figure 5. Results of symmetric crop attacks: (a) crop attack in left image, (b) detected result in (a), (c) restored left image (PSNR=39.22dB), (d) original left image, (e) crop attack in right image, (f) detected result (d), (g) restored right image (PSNR=39.47dB), (h) original right image.

We also conducted experiments under the condition that the size of tampered region is different as shown in Fig.6 (a) ~ (d). The restored images are shown in Fig.6 (e) ~ (h).

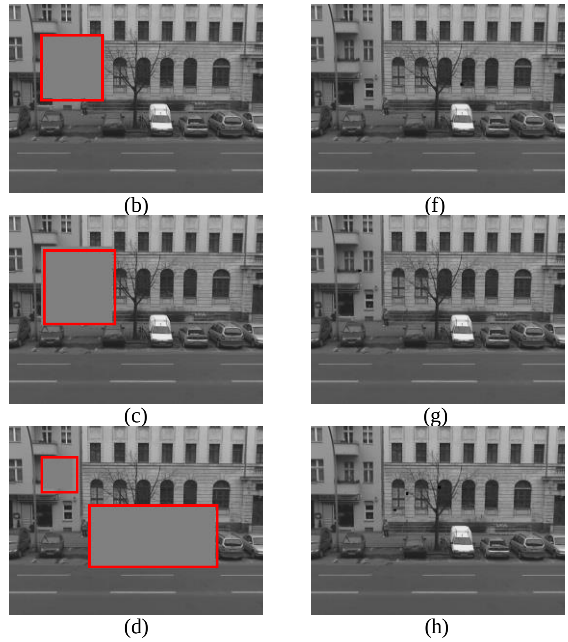
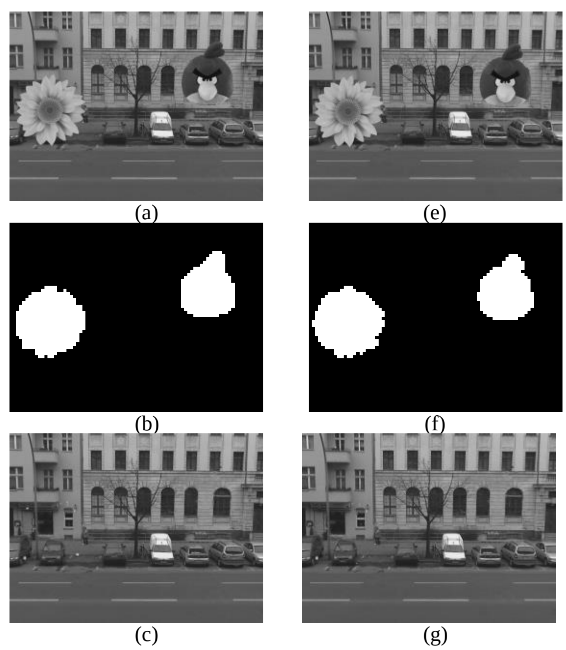


Figure 6. Results of symmetric crop attacks with different size: (a) crop attack1 in right image, (b) crop attack2 in right image, (c) crop attack3 in right image, (d) crop attack4 in right image, (e) restoredattack1 (PSNR=42.55dB), (f) restored attack2 (PSNR=37.25dB dB), (g) restored attack3 (PSNR=36.18dB), (h) restored attack4 (PSNR=33.75dB).

B. Collage Attack

Collage attack is introduced by J.Fridrich. The tampered images in Fig.7 (a) and (e) are generated by pasting the ‘bird’ and ‘flower’ in stereo image “Altmoabit”. All fake blocks are localized, as shown in Fig.7 (b) and (f). The restored images are shown in Fig.7(c) and (g), and corresponding PSNR values are 33.92dB and 34.09dB.



(d)

(h)

Figure 7. Results of symmetric collage attacks: (a) collage attack in left image, (b) detected result in (a), (c) restored left image (PSNR=33.92dB), (d) original left image, (e) crop attack in right image, (f) detected result in (e), (g) restored right image (PSNR=34.09dB), (h) original right image.

IV. CONCLUSIONS

In this paper, a stereo image watermarking method based on disparity map for stereo image authentication and restoration is proposed. Watermark bits are embedded into host images. We utilize the degree of smoothness to categorize the blocks, and the type of complex blocks is allocated more bits, on the contrary of smooth blocks. On the receiver side, the calculated watermark and extracted watermark are compared to localize the tampered blocks. The ability to restore the tamped region is improved due to the foremost-bits embedded twice. Meanwhile, that the watermark volume is reduced due to recovery watermark including disparity leads to improve the transparency of the watermarked image. The experimental results also show that the proposed method can localize and recover the destroyed regions well. In future probe, more efforts will be focused on consideration of watermarking embedding among the stereo image to improve the quality of recovered images.

ACKNOWLEDGMENT

This work was supported by Natural Science Foundation of China (61171163, 61071120, 61271270, 61271021, 61111140392), the Zhejiang Scientific and Technical Key Innovation Team Project (Grant No.2010R50009), Natural Science Foundation of Ningbo (2012A610045), The Outstanding (Postgraduate) Dissertation Growth Foundation of Ningbo University (grant PY20120007).

REFERENCES

[1] M. Tanimoto, M. Tehrani, T. Fujii, and T. Yendo, “FTV for 3-D Spatial Communication,” Proceedings of the IEEE, vol. 100, pp: 905-917, 2012.

[2] X. D. Li, “JPEG-Compression-Attack Resistant Image Quantization Watermarking Algorithm in DWT Domain,” Journal of Optoelectronics•Laser, vol. 23, no. 2, pp: 342-348, 2012.

[3] A. Haouzia, and R. Noumeir, “Methods for Image Authentication: A Survey,” Multimedia tools and applications, vol. 39, pp: 1-46, 2008.

[4] X. Qi, and X. Xin, “A Quantization-Based Semi-Fragile Watermarking Scheme for Image Content Authentication,” Journal of visual communication and image representation, vol. 22, pp: 187-200, 2011.

[5] P. W. Wong, and N. Memon, “Secret and Public Key Image Watermarking Schemes for Image Authentication and Wwnership Verification,” IEEE Transactions on Image Processing, vol. 10, no. 10, pp: 1593-1601, 2001.

[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, no. 12, pp: 2519-2529, 2005.

[7] Z. X. Qian, G. R. Feng, X. P. Zhang, and S. Z. Wang, “Image Self-embedding with High-Quality Restoration Capability,” Digital Signal Processing, vol. 21, no. 2, pp: 278-286, 2011.

[8] C. L. Li, Y. H. Wang, B. Ma, and Z. X. Zhang, “A Novel Self-recovery Fragile Watermarking Scheme Based on Dual-Redundant-Ring Structure,” Computers & Electrical Engineering, vol. 37, no. 6, pp: 927-940, 2011.

[9] C. Qin, C. C. Chang, and P. Chen, “Self-Embedding Fragile Watermarking with Restoration Capability Based on Adaptive Bit Allocation Mechanism,” Signal Processing, vol. 92, no. 4, pp: 1137-1150, 2012.

[10] Y. Y. Huo, H. J. He, and F. Chen, “Alterable-Capacity Fragile Watermarking Scheme with Restoration Capability,” Optics Communications, vol. 285, no. 7, pp: 1759-1766, 2012.

[11] M. Elad, J. L. Starck, P. Querre, and D. L. Donoho, “Simultaneous Cartoon and Texture Image Inpainting using Morphological Component Analysis (MCA),” Applied and Computational Harmonic Analysis, vol. 19, no. 3, pp: 340-358, 2005

[12] X. Wang, G. Y. Jiang, J. M. Zhou, Y. Zhang, Z. J. Peng, F. Shao, and M. Yu,“Visibility Threshold of Compressed Stereoscopic Image: Effects of Asymmetrical Coding,” The Imaging Science Journal, vol. 61, no. 2, pp: 172-182, 2013.