Int. J. Electron. Commun. (AEÜ) 69 (2015) 361–370

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

journal homepage: www.elsevier.com/locate/aeue

REGULAR PAPER

New fragile watermarking method for stereo image authentication with localization and recovery

Mei Yu, Jing Wang, Gangyi Jiang*, Zongju Peng, Feng Shao, Ting Luo

Faculty of Information Science and Engineering, Ningbo University, Ningbo 315211, China

ARTICLE INFO

Article history:
Received 12 January 2014
Accepted 10 October 2014

Keywords:
Stereo image
Fragile watermarking
Image authentication
Tamper localization
Self-recovery

ABSTRACT

To address issues of image authenticity verification and integrity protection, a fragile watermarking method for stereo image authentication is proposed with stereo matching technique. According to stereo matching of left and right images, non-overlapping blocks of left image are classified into non-matchable and matchable ones. Right image blocks and non-matchable blocks of left image are categorized into smooth, texture and complex blocks considering their roughness. Then, the corresponding alterable-length watermark is computed based on the results of block classification, and the destroyed blocks are recovered by using the corresponding alterable-length watermark. Besides, matchable tampered blocks of left image are recovered with the matched contents in right image. A detection technique with the part of alterable-length watermark is used to increase accuracy of tamper localization at the receiver. The disparity can be used to recover the tampered matchable block. Therefore, the quality of watermarked images is improved because of low embedding capacity. Additionally, the alterable-capacity watermark provides suitable information for smoother images with fewer bits and we obtain high quality restoration. Experimental results show that the proposed method can not only localize the tampered regions precisely but also recover the tampered regions with higher quality compared with the state-of-the-art methods.

1. Introduction

With the rapid development of three-dimensional (3D) video related technologies, more and more users would enjoy the high quality of 3D products because of a strongly sense of realism and immersion [1]. 3D videos and images are drawing increasing attention and will be applied to related commercialized fields in the near future [2]. Nevertheless, due to the growth of computer and internet technologies, digital data can be easily accessed, manipulated and tampered by using image processing tools whether it is malicious or not. Therefore, it is a great challenge to ensure the integrity of stereo image which is a typical format for representing 3D products. Watermarking technology is regarded as one of effective approaches to resolve copyright protection and authentication of images [3].

A stereo image pair consists of two images (left and right images) and is captured by two cameras from the same scene [4]. The slight difference between left and right images is called disparity, which makes images realistically and provides users binocular perception. The early researches on stereo watermarking schemes were mainly focused on copyright protection [5,6]. Yu et al. [7] built relationships between the features of blocks at the same position on left and right images of a stereo pair, and then a parity quantization was designed for embedding watermark. To improve quality of watermarked images, Niu et al. [8] achieved the optimal trade-off between the imperceptibility and robustness by taking binocular sensitivity into account. Some watermarking schemes were proposed for depth map based on rendering 3D image representations, Lin et al. [9] presented a robust stereo watermarking method to embed watermark into the color image. The watermark can be extracted from left and right images which were rendered from color image plus depth map. However, stereo image authentication watermarking methods had not been studied deeply.

Fragile watermarking had been developed for verification of image integrity and content authentication [10]. Wong et al. [11] divided image into blocks and embedded watermark into each block, but this method was lack of resilience. The fragile watermarking methods with restoration capability are more practically and comprehensively applied [12–16]. Lin et al. [12] used a three-level hierarchical structure to locate tampered regions, but this method didn't have the second chance to recover the tampered blocks whose watermark was embedded in the other destroyed blocks, which was called tampering coincidence problem [17]. In Ref. [13,14], two copies of restoration-bits were embedded

* Corresponding author. Tel.: +86 574 87600411; fax: +86 574 87600940.
E-mail address: jianggangyi@126.com (G. Jiang).

http://dx.doi.org/10.1016/j.aeue.2014.10.006
1434-8411/

into image and the second chance for block recovery was provided to solve tampering coincidence problem. Lee et al. [13] hided restoration-bits into three least-significant-bit (LSB) layers of images. Consequently, the quality of watermarked and recovered images was decreased due to the increased watermarking capacity. In Ref. [14], watermark was generated by encoding the first eleven quantized coefficients, the image content was not taken into account and the hiding space in images was wasted. To improve the quality of the watermarked and recovered images, Qin et al. [15] proposed a fragile watermarking method with restoration capability using an adaptive bit allocation mechanism. Image blocks were coded with the alterable-length based on smoothness of blocks and the corresponding watermark was embedded into the 1-LSB plane of images. Nevertheless, if the length of watermark was extracted falsely, this method could not localize or restore the tampered areas, and meanwhile, additional authentication-bits increased the watermarking payload. Huo et al. [16] proposed an alterable-capacity watermarking method which divided all the blocks into eight types according to their roughness. Watermark was generated with alterable-length, and restoration-bits were used for authentication. The types which determined the watermarking length were important to localize the tampered regions precisely.

The problems of above fragile watermarking methods with restoration capability still remain in the process of watermark embedding, tamper localization and recovery. The first concern is the contradiction between the quality of watermarked image and embedding capacity, and the quality of the watermarked image is up to the watermarking capacity. The less watermarking capacity is, the better quality of the watermarked image may be [15]. The second concern is the accuracy of tamper localization. One of the solutions is to utilize more bits to detect the tampered region, but the quality of watermarked images is reduced due to the increased watermarking payload. In Ref. [18], the restoration-bits are used to locate the tampered regions and the restoration-bits are not needed to be embedded in watermarked images. The third concern is ability of self-recovery, to address this problem, the key research activities are to restore the tampered regions by extracting effective information, and the other works use more bits to represent the restoration-bits [19]. Since a stereo image consists of left and right images and the most contents in left image are similar to the corresponding parts of right image, the destroyed block which is matchable can be recovered with its matched content, so that the watermarking capacity will be decreased observably due to the smaller embedding bits. Meanwhile, there exists binocular psycho-visual redundancy in stereo image pairs [20], which can be utilized to improve visual quality of the watermarked images.

To improve quality of the watermarked and recovered images, a fragile watermarking method for stereo image authentication with self-recovery capability is proposed in this paper. Non-overlapping blocks with size of 8×8 pixels in stereo image are divided into matchable, smooth, texture and complex blocks, according to the stereo matching process and roughness. Different number of bits are assigned to represent watermark generated based on block content and disparity. Then, the watermark is divided into three parts and embedded into three mapping blocks. At the receiver side, the fixed-length watermark is used for localizing the tampered blocks, and the recovered results with high quality are obtained by using restoration-bits and matched contents.

The rest of this paper is organized as follows. Section 2 describes the proposed stereo watermarking generation and embedding method. Section 3, the details of tamper detection and content restoration are presented. Experimental results and discussions are given in Section 4 and Section 5 concludes this paper.

2. The proposed watermarking method

In this section, we elaborate the details of watermark generation and embedding. In stereo image pair, most of the pixels in left image, which are defined as matchable pixels, are similar to the corresponding pixels in right image, which are defined as matched pixels [21]. Therefore, the tampered matchable pixels can be recovered with the aid of the corresponding valid matched pixels in the process of recovery. As is known, the pixels of smooth blocks are consistent with each other, while those of complex blocks are slightly different from each other. Restoration-bits of smooth blocks can be composed of fewer bits, while complex blocks are represented by more bits. Mean square error (MSE) is a standard of classifying the blocks, as MSE of pixels in smooth blocks is smaller than that of complex blocks. Based on the above analyses, a fragile watermarking method for stereo image authentication is proposed, and the flowchart of the corresponding watermark generation and embedding scheme is shown in Fig. 1.

Let $I_l(i)$ and $I_r(i)$ $(1 \le i \le N_1)$ denote pixel values of left and right images, where N_1 is the number of total pixels of one image, and the alterable-length watermark is generated based on blocks contents. The watermark is embedded into the 1-LSB and 2-LSB of stereo image.

2.1. Block classification

The stereo image is divided into 8×8 non-overlapping stereo blocks denoted as $\boldsymbol{B} = \{B_j | j = 1,2,\ldots,N\}$, where, $N (N = 2 \times N_1/64)$ is the number of blocks in stereo image, the 1-LSB and 2-LSB planes of each block are set to zero. In the matching process, matchable blocks in left image are denoted as **M**. The rest of the blocks in left image and all the blocks in right image are partitioned into smooth blocks, denoted as **S**, texture blocks, denoted as **E**, and complex blocks, denoted as **C**, respectively, and are determined by.

$$T_j = \begin{cases} \boldsymbol{S}, & \text{if } var_1(B_j) \le Th_1 \\ \boldsymbol{E}, & \text{if } (var_1(B_j) > Th_1) \& (var_2(B_j) \le Th_2) \\ \boldsymbol{C}, & \text{otherwise} \end{cases} \quad (1)$$

where var_1 denotes the mean square deviation of block B_j, B_j is divided into four sub-blocks with the size of 4×4, var_2 denotes average of mean square deviation for each sub-block, Th_1 and Th_2 are two thresholds, generally, the value of Th_1 is smaller than Th_2, and '&'denotes binary logic operation 'AND'. Blocks of left image are classified into **M**, **S**, **E** and **C**, and those of right image are classified into **S**, **E** and **C**.

2.2. The proposed watermark generation scheme

Alterable-capacity watermark is made up of feature bits which include four segments. The first segment includes low-frequency-bits, significant-low-frequency-bits, hypo-significant-low-frequency-bits in frequency domain, the second segment is in spatial domain and includes basic-bits, sub-basic-bits, the third and fourth segments are type-bits and disparity-bits. The main processes of generating feature bits are described as follows and shown in Table 1.

For each block B_j with the size of 8×8, a quantized discrete cosine transform (DCT) coefficients matrix is generated by using DCT and JPEG quantization table [22], and then the quantized DCT coefficients of block are arranged in zigzag order denoted as $\boldsymbol{Z} = \{z_1, z_2, \ldots, z_{64}\}$ [23]. The first ten coefficients of the vector $\boldsymbol{Z}$ are converted into binary sequence with 51 bits which are defined as low frequency bits, denoted as O_j, and the number of bits which