Int. J. Electron. Commun. (AEÜ) 70 (2016) 77–84

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

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

Binocular visual characteristics based fragile watermarking scheme for tamper detection in stereoscopic images

Wujie Zhou [a,b,*], Lu Yu [a], Zhongpeng Wang [b], Mingwei Wu [b], Ting Luo [c], Lihui Sun [b]

[a] Institute of Information and Communication Engineering, Zhejiang University, Hangzhou 310027, China
[b] School of Information and Electronic Engineering, Zhejiang University of Science & Technology, Hangzhou 310023, China
[c] College of Science & Technology, Ningbo University, Ningbo 315211, China

ARTICLE INFO

Article history:
Received 12 May 2015
Accepted 12 October 2015

Keywords:
Stereoscopic image
Watermarking
Binocular visual characteristics
Authentication
Tamper detection

ABSTRACT

In the past decade, various fragile digital watermarking techniques have been proposed for monoscopic image authentication and temper detection. In this paper, a novel binocular visual characteristics based pixel-wise fragile watermarking scheme for stereoscopic image authentication and tamper detection is proposed. The scheme consists of two processes: embedding of the stereoscopic image authentication message and tamper detection. In the watermark embedding process, the binocular just noticeable difference (BJND) model is used for guiding watermark embedding, which is convenient for achieving a balanced relationship between watermarking capacity and visual transparency. In the tamper detection process, a probability theory and an algorithm of binocular disparity are employed to improve previously obtained detection results and to enhance authentication accuracy. Moreover, to improve the security of the proposed scheme, MD5 hash function and chaotic map are used. Experimental results reveal that the proposed scheme is not only secure, but also achieves superior tamper detection for different attacks.

1. Introduction

Stereoscopic images are acquired from two slightly different perspectives. One can perceive a stereoscopic image in three dimensions (3D) when the left and right views of the stereoscopic image are viewed by the respective eye of the end-user [1]. In recent times, stereoscopic images are being used in many applications such as flight simulators for pilot training, robot vision, medical surgery, military surveillance, virtual reality games, and autonomous navigation [2]. With the rapid developments in Internet and computer technology in recent years, it has become possible to easily access, manipulate, and tamper with stereoscopic images in open networks without the permission of the original authors [3]. Precision and integrity of stereoscopic images is important, and in this regard, digital watermark technology is considered a reliable and effective solution for authentication [4].

Several previous studies have made some progress in watermarking techniques for stereoscopic images especially in the field of copyright protection [5–7]. In [5], Lee et al. proposed a watermarking scheme based on discrete cosine transform (DCT) for copyright protection of stereoscopic images. Hwang et al. used an MPEG video watermarking scheme to embed watermarks into the DCT [6] and discrete wavelet transform (DWT) [7] coefficients of the decomposed right view. In [8], Coltuc et al. proposed a reversible watermarking scheme for stereoscopic images for storage and bandwidth reduction; however, inter-correlations between the two views were missing. To improve the performance of a stereoscopic image watermarking scheme, the features of stereoscopic images need to be excavated and utilized [9–12]. Campisi proposed a proof of concept for a watermarking scheme for stereoscopic images, wherein he makes use of the extracted depth information [9]. Chammenm et al. embedded watermarks into the disparity computed from the left and right views while maintaining an adequate trade-off between robustness and transparency [10]. Niu et al. proposed a visual sensitivity model guided stereoscopic image watermarking scheme, wherein watermarks are embedded in the DCT domain to make the watermarking scheme as robust and invisible as possible [11]. Yu et al. took advantage of the block inter-relationships between two views for embedding watermarks in order to improve robustness [12]. Recently, watermarking schemes based on depth-image-based rendering have been proposed [13,14]. Lin et al. embedded watermarks into the DCT based center view; this method protects the center view and rendered views as well [13]. In addition, Kim et al. proposed a dual-tree

* Corresponding author at: School of Information and Electronic Engineering, Zhejiang University of Science & Technology, Hangzhou 310023, China. Tel.: +86 571 85070303.
E-mail address: wujiezhou@163.com (W. Zhou).

http://dx.doi.org/10.1016/j.aeue.2015.10.006
1434-8411/

complex wavelet transform based watermarking scheme that is more robust than Lin's [14]. Besides copyright protection, verification of the integrity and authenticity of the image content is another important purpose of a watermark; however, stereoscopic image watermarking schemes rarely focus on ensuring authenticity.

Most of the existing fragile watermarking schemes ensure authenticity verification for monoscopic images captured from a single camera. In general, fragile watermarking techniques can be categorized into two major classes: pixel-wise and block-wise fragile watermarking schemes. The main idea in block-wise fragile watermarking schemes is that the original image is divided into non-overlapping blocks and each block contains its own watermarking information. For example, one of the first block-wise authentication scheme was proposed by Walton [15]. He divided the image into 8×8 non-overlapping blocks and embedded the checksum in the least significant bit (LSB) of every block. Subsequently, many block-wise fragile watermarking schemes have been proposed [16–19]. If the target image is altered, the image content and the watermark extracted from the tampered blocks do not match with the other blocks, therefore the tampered blocks can be detected. In general, block-wise fragile watermarking schemes are only capable of detecting a major alteration or replacement. Moreover, these schemes can only identify tampered blocks and not tampered pixels. Therefore, some pixel-wise fragile watermarking schemes have been proposed to resolve this problem, wherein the watermarking information derived from host pixels is embedded into the host pixels themselves. Therefore, tampered pixels can be identified by the absence of the watermarking information they are expected to contain. For example, Zhang et al. proposed a statistical scheme for a pixel-wise fragile watermarking scheme for cases when the tampered area is not too extensive [20]. Hsu et al. proposed a pixel-wise based scheme that decreases the probability of mistakes in tamper detection, and enhances the accuracy of authentication. To improve the security of pixel-wise fragile watermarking schemes [21], Rawat et al. proposed a chaos based watermarking scheme for image authentication and tamper detection [22]. Teng et al. analyzed the security of watermarking scheme [22] and proposed an improved scheme to enhance the security of fragile watermarking scheme [23]. In addition, Zhang and Wang [24] proposed a fragile watermarking scheme combining block-wise and pixel-wise techniques. Their scheme can not only detect the blocks containing tampered content, but also locate the tampered pixels. For digital images, modification of content and modification of watermark are not the same. Content removal tampering destroys the integrity and authenticity of an image, while watermark removal tampering does not affect the authenticity of the image. Therefore, the verification process in a watermarking system should be able to detect and localize exactly where the content is tampered. However, the aforementioned fragile watermarking schemes are unable to distinguish between content removal tampering and watermark removal tampering.

In our previous work [4], block-wise fragile watermarking scheme was proposed, which have some shortcomings: (1) only identify tampered blocks and not tampered pixels, (2) unable to distinguish between content removal tampering and watermark removal tampering, and (3) the relationship between watermarking capacity and visual transparency have not been thoroughly explored. In this paper, a novel binocular visual characteristics based pixel-wise fragile watermarking scheme for stereoscopic image tamper detection is proposed. In order to achieve a balanced relationship between watermarking capacity and visual transparency, the binocular just noticeable difference (BJND) model is applied, which helps guide watermark embedding without degrading the stereoscopic image. A stereoscopic image presents two offset views; therefore, its total watermarking capacity is more than that of a monoscopic image. Moreover, because most of the pixels in the two views of a stereoscopic image match with binocular disparity, when the target image is tampered with, the left and right views are often modified symmetrically with reasonable binocular disparity; the inter-correlations in the modifications, in such cases, help improve the performance of tamper detection. This study aims to integrate binocular visual characteristics and probability theory to improve image tamper detection accuracy and precision. Further, MD5 hash function and chaotic map are employed for improving the security of the proposed scheme. The effectiveness of the proposed scheme is verified through a series of attacks.

The remainder of this paper is organized as follows. In Section 2, the proposed watermarking scheme, including the watermark embedding and tamper extraction is explained. Experimental results are presented in Section 3. Finally, conclusions are drawn in Section 4.

2. Proposed binocular visual characteristics based fragile watermarking scheme

In this section, we explain the proposed watermarking scheme. Let us consider I_l and I_r as the original left and right views of a stereoscopic image of size $M \times N$, and $\hat{I}_l$ and $\hat{I}_r$ as the tampered left and right views of the stereoscopic image of size $M \times N$. The coordinates of the content pixel is (x,y) and the corresponding mapping coordinates of the watermark pixel is (i,j).

2.1. Logistic chaotic map

In the self-embedding watermarking scheme, the watermark embedding position of each pixel is randomly distributed over the entire stereoscopic image. Therefore, this study adopts a random sequence generated by a logistic chaotic map to obtain a one-to-one pixel-mapping sequence. The steps of generating the pixel-mapping sequence are as follows.

Step a1: A random sequence $B=(b_1, b_2, \ldots, b_N)$ of length N is generated using the following logistic chaotic map [25].

$$b_{n+1} = \mu \cdot b_n(1 - b_n), \quad b_n \in (0, 1) \tag{1}$$

where $n=0, 1, \ldots$ is the map iteration index and μ is a system parameter. If $3.5699456 < \mu \leq 4$, then the logistic chaotic map becomes chaotic. In this state, the sequence is non-periodic, non-convergent, and very sensitive to the initial value of b_0. Moreover, all the orbits of the logistic map are dense in the range of the map [0,1].

Step a2: An index ordered sequence $A = \{a_1, \ldots, a_i, \ldots, a_N\}$ such that $b_{a_1} \leq b_{a_2} \leq \cdots \leq b_{a_N}$ is obtained by sorting $\hat{B} = \{b_1, b_2, \ldots, b_N\}$.

Step a3: The index of the content pixel is set as $p(m)$ and its corresponding mapping index of watermark inserting pixel as $p(a_m)$.

Step a4: All pairs of $p(m)$ and $p(a_m)$ are recorded to form the one-to-one pixel-mapping sequence.

Step a5: $p(m)$ and $p(a_m)$ are reset to two dimension pixel-mapping coordinates.

2.2. Watermark embedding

The BJND model measures the perceptible minimum distortion threshold of binocular vision for a stereoscopic image; this has been verified through many psychophysical experiments [26]. In the following, the derivation of the BJND model is summarized. By incorporating the luminance and contrast masking effects, as well