New Multipurpose Oriented Stereo Image Watermarking Algorithm for 3D Multimedia

Wujie Zhou[1]*, Ting Luo[2], Zhongpeng Wang[1], Mingkun Feng[1], Jianfeng Weng[1], Xin Li[1]
[1]School of Information and Electronic Engineering, Zhejiang University of Science and Technology, Hangzhou 310023, China (*wujiezhou@163.com)
[2]Faculty of Information Science and Engineering, Ningbo University, Ningbo 315211, China

Abstract: - Most of digital watermarking algorithms have been designed for only single purpose. In this paper, a new multipurpose oriented stereo image watermarking algorithm is proposed for three dimensional multimedia, which can be used for copyright protection, content authentication and tamper detection in three dimensional (3D) multimedia. Specifically, host stereo image is divided into non-overlapping blocks, and the chaotic feature watermarks are generated according to the stability of low frequency coefficients and largest singular value. As there are redundancies between the left and right views of stereo image, each block of the two views is classified into matchable or non-matchable block to embed digital watermarks with different purposes. At the receiving side, using stereo marching technique as a bridge, the robust and fragile watermarks can be blindly extracted without access to the host stereo image. Meanwhile, the robustness of stereo image watermarking is improved, and a hierarchical tamper detection scheme is presented to ensure the accuracy of tamper localization. Especially, Level-2 detection is employed to improve previously obtained detection results to enhance authentication accuracy. Experimental results show that the proposed algorithm is quite robust to attacks, such as noise, filtering, JPEG compression, cropping and size scaling. Moreover, the experimental results also show that the proposed algorithm can detect tamper accurately and locate forgery effectively.

Key-Words: - Stereo image watermarking, copyright protection, authentication, multipurpose, matchable block and non-matchable block, chaotic feature watermark

1 Introduction

Three-dimensional (3D) multimedia services can provide more realistic and immersive experience to end-users by providing depth perception [1, 2], compared to traditional two-dimensional (2D) multimedia services. People can share their 3D contents easily due to the rapid growth of multimedia and networking technologies. However, 3D contents may be copied and tampered illegally, which has created a great concern on multimedia security. Watermarking technology is one of prospective solutions to protect the copyright or verifies the integrality of 3D contents by embedding watermark into contents [3, 4]. In practical applications, 3D contents may be processed by many operations such as low pass filtering, scaling, cropping and compression in the usage and transmission. Thus, the embedded watermarks should be robust against above possible attacks. On the other hand, besides the common signal processing operations, there exist malicious attacks and forgery. In these cases, the embedded watermarks must be sensitive to tamper [5, 6].

In the past decade, stereo image watermarking technology had attracted much attention [7-19]. Similar to 2D image watermarking algorithms, stereo image watermarking algorithms can be also categorized into robust and fragile algorithms according to their purposes. Robust image watermarking algorithms are generally used for copyright protection and ownership verification because they are robust to various stereo image processing operations, while fragile image watermarking algorithms are mainly applied to content authentication and integrality attestation because they are fragile to malicious tamper on stereo image [20]. In the previous studies, most of the existing stereo image watermarking algorithms were designed for single purpose only. Lee *et al.* proposed a watermarking algorithm for copyright protection of stereo vision system using adaptive matching technique [7]. Hwang *et al.* proposed stereo image watermarking algorithms based on discrete cosine transform (DCT) and discrete wavelet transform (DWT) [8, 9], but inter-relationships between two views were missed in their method. Coltuc *et al.* proposed reversible watermarking approaches for stereo image [10, 11]. In order to obtain a trade-off between robustness and imperceptivity, Niu *et al.* proposed a visual

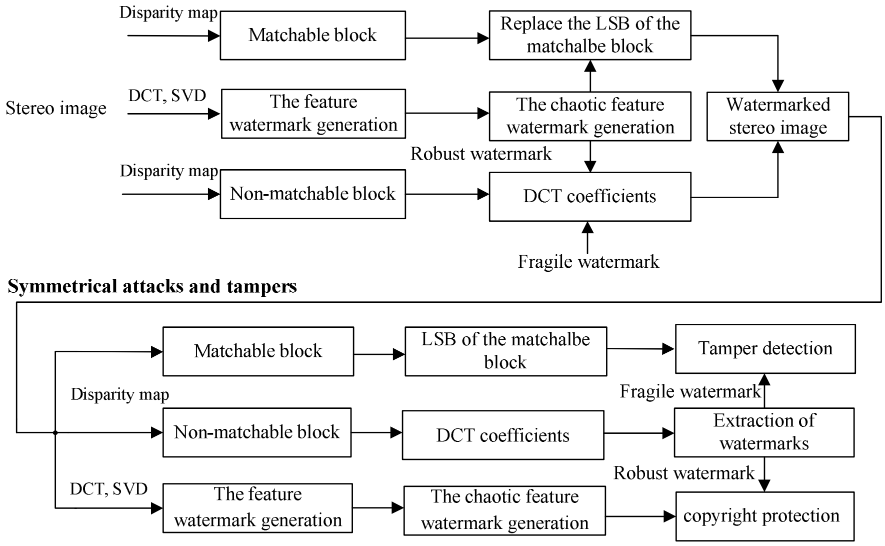

Fig. 1 Block diagram of the proposed multipurpose-oriented stereo image watermarking algorithm

sensitivity based stereo image watermarking algorithm [12]. As another representation of stereo image, stereo image is made up of a central view and its depth map, and it was also protected by embedding watermark into the central view [12, 13]. For example, Lin *et al.* embedded watermarks into DCT based central view to protect the central view and rendered views as well [13]. Kim *et al.* [14] also proposed a dual-tree complex DWT based watermarking algorithm, which is more robust than Lin's. Wang *et al.* [15] proposed a novel watermarking method, which not only protects the central views but also the rendered virtual views. Yu *et al.* employed block-wise inter-relationships between two views to embed watermark for improving robustness [16]. Above stereo image watermarking algorithms were designed for copyright protection. Recently, Luo *et al.* proposed a stereo image watermarking algorithm for authentication with self-recovery capability using inter-view reference sharing [17]. Campisi proposed an object-oriented watermarking algorithm for stereo image [18]. Moreover, Bhatmagar *et al.* proposed a stereo image coding algorithm with watermarking technique [19]. Furthermore in daily life, stereo image may suffer from common signal processing operations as well as tamper. In this case, the robust image watermarking algorithms cannot detect the tamper while the fragile image watermarking algorithms are too sensitive to tamper. Up to now, there are few algorithms, which can realize those purposes at the same time. To solve this problem, it is significant to achieve stereo image's copyright protection, content authentication and tamper detection simultaneously.

In this paper, we propose a multipurpose-oriented stereo image watermarking algorithm with stereo matching technique, for copyright protection, content authentication and tamper detection in 3D multimedia. In the proposed algorithm, host stereo image is divided into non-overlapping blocks, and DCT is applied independently to each block. In order to improve the robustness, a chaotic feature watermark is generated from judging the parity of the highest digit of the maximum singular value that is calculated from the low-frequency component of each block's DCT matrix by using singular value decomposition (SVD). Because of redundancies between the left and right views of stereo image, each block of the two views is classified into matchable or non-matchable block. Then, the fragile and robust watermarks are embedded in non-matchable blocks, and in matchable blocks only fragile watermark is embedded. Using stereo marching as a bridge, the performances of stereo image watermarking are improved. Hence, the proposed algorithm is not only robust against common signal processing attacks but also sensitive to tamper. Experimental results show the proposed algorithm's efficiency to solve the stereo image protection and authentication problems.

The rest of this paper is organized as follows. Section 2 proposes a new stereo image watermarking algorithm for copyright protection and content authentication. Experimental results are given in Section 3. Finally, the last section concludes this paper.

2 Proposed Multipurpose Oriented Stereo Image Watermarking Algorithm

Fig.1 shows the block diagram of the proposed multipurpose-oriented stereo image watermarking algorithm, which consists of four main parts, that is, disparity map and chaotic feature watermark generation, watermark embedding, watermark extraction and tamper detection.

2.1 Disparity map and chaotic feature watermark generation

Stereo image is an image pair of the same scene taken from slightly different positions at the same time. However, due to the existing occlusion regions, a few blocks in the left and right views can be non-matchable. Thus, stereo image blocks can be classified as matchable and non-matchable blocks. The feature watermarks are generated according to the stability of low frequency DCT coefficients and largest singular value. The feature watermarks and disparity map generation are described as follows

Step-a1 Left and right views of stereo image are divided into non-overlapping blocks with the size of k×k, the left and right views' blocks are denoted by $\{B_L^o(m,n) \mid m \in [1, M/k], n \in [1, N/k]\}$ and $\{B_R^o(m,n)\}$, respectively, where (m, n) denotes the position of the block in view.

Step-a2 Each block is transformed with DCT , i.e., $B_{L,m,n}^{o,dct} = dct(B_L^o(m,n))$ and $B_{R,m,n}^{o,dct} = dct(B_R^o(m,n)$, where dct(•) denotes DCT operation.

Step-a3 The k1×k1 (k1<k) upper left corners of the $B_{L,m,n}^{o,dct}$ and $B_{R,m,n}^{o,dct}$, denoted as $B_{L,m,n,k_1}^{o,dct}$ and $B_{R,m,n,k_1}^{o,dct}$, respectively, are picked up to conduct with SVD, i.e. $[U_{L,m,n,k_1}, S_{L,m,n,k_1}, V_{L,m,n,k_1}] = svd(B_{L,m,n,k_1}^{o,dct})$ and $[U_{R,m,n,k_1}, S_{R,m,n,k_1}, V_{R,m,n,k_1}] = svd(B_{R,m,n,k_1}^{o,dct})$, where svd(•) denotes SVD operation. Here, k and k1 are set to 4 and 2, respectively.

Step-a4 Let S_L,max(m,n) and S_R, max(*m,n*) be the largest singular values of the left and right views, respectively. Then, the feature watermarks, W_L,*f*(*m,n*) and W_R,*f*(*m,n*), of the left and right views are generated by judging the parity of the highest digits of S_L, max(*m,n*) and S_R, max(*m,n*), respectively, as follows

$$W_{L,f}(m,n) = \begin{cases} 1, & \text{if } \mathrm{mod}(S_{L,\max}(m,n),2) = 1 \\ 0, & \text{else} \end{cases} \quad (1)$$

$$W_{R,f}(m,n) = \begin{cases} 1, & \text{if } \mathrm{mod}(S_{R,\max}(m,n),2) = 1 \\ 0, & \text{else} \end{cases} \quad (2)$$

Step-a5 Disparity map $\{d(m,n)\}$ is defined as

$$\begin{cases} \forall \{d(m,n) \mid (S_{L,\max}(m,n) - S_{R,\max}(m, n - d(m,n)) \le T \\ \& \, (W_{L,f}(m,n) = W_{R,f}(m,n)) \, \& \, d(m,n) \in [-\gamma, \gamma]\} \end{cases}$$
(3)

where T is a matchable threshold, and γ is the maximum searching range. After the stereo matching process, most blocks in the left and right views can be established as one-to-one matching, and disparity values are recorded. However, a few blocks in one view cannot be found its matchable blocks in the other view and their disparity values are set to γ+1. Here, T and γ are empirically set to 10 and 30, respectively.

In order to improve the security of watermarking, the feature watermarks, W_L, *f*(*m,n*) and W_R, *f*(*m,n*), are pre-processed by operations such as permutation or encryption.

To do chaotic feature watermark generation, chaotic map is used, which is a function that generates unpredictable results which are sensitive to the initial conditions. That is, different initial inputs produce different outcomes. A representative logistic function is used for chaotic map, and described as follows

$$x_{l+1} = \mu \cdot x_l (1 - x_l) \quad (4)$$

where μ is a positive number that serve as a function seed, and all orbits of the chaotic map are dense in the range of the map [0, 1]. Binary processing of the chaotic sequence is described by

$$B_{cp}^{key}(l) = \begin{cases} 1 & \text{if } x_l > 0.5 \\ 0 & \text{else} \end{cases} \quad (5)$$

where $B_{cp}^{key}(l)$ is a binary sequence, its rearrange is used to get binary encryption matrix $B_{cp}^{key}(m,n)$.

According to the feature watermarks and the binary encryption matrix, we get the binary chaotic feature watermarks, $W_{L,f}^{cp}(m,n)$ and $W_{R,f}^{cp}(m,n)$, using exclusive-or (XOR) operation, denoted as $\oplus$, and express them as follows

$$\begin{cases} W_{L,f}^{cp}(m,n) = W_{L,f}(m,n) \oplus B_{cp}^{key}(m,n) \\ W_{R,f}^{cp}(m,n) = W_{R,f}(m,n) \oplus B_{cp}^{key}(m,n) \end{cases} \quad (6)$$

2.2 Watermark embedding

In this section, the fragile and robust watermarks are simultaneously embedded in the non-matchable blocks with different techniques, and while in the matchable blocks only fragile watermark is embedded.

Stereo image watermark embedding of non-matchable block in the left view will be described as an example, watermark embedding of the non-matchable block in the right view is the same as that in the left view. The main embedding process of the non-matchable blocks in the left view is described as follows

Step-b1 Obtain a binary chaotic feature watermark $W_{L,f}^{cp}(m,n)$ and block DCT coefficients $B_{L,m,n,k_1}^{o,dct}$, as represented in sub-section 2.1.

Step-b2 In order to improve the robustness of watermarking, the low-middle frequency DCT coefficients are selected for robust watermark embedding, and the detailed procedures are expressed as follows

[1] If $W_{L,f}^{cp}(m,n)=0$ and $\varphi_1 = B_{L,m,n,k_1}^{o,dct}(s_1,r_1) - B_{L,m,n,k_1}^{o,dct}(s_2,r_2) < \beta$, the block DCT coefficients, $B_{L,m,n,k_1}^{o,dct}(s_2,r_2)$ and $B_{L,m,n,k_1}^{o,dct}(s_1,r_1)$, are modified according to the following rule

[2]

$$\begin{cases} \hat{B}_{L,m,n,k_1}^{o,dct}(s_2,r_2) = B_{L,m,n,k_1}^{o,dct}(s_2,r_2) - (\beta - \varphi_1)/2 \\ \hat{B}_{L,m,n,k_1}^{o,dct}(s_1,r_1) = B_{L,m,n,k_1}^{o,dct}(s_1,r_1) + (\beta - \varphi_1)/2 \end{cases} \quad (7)$$

If $W_{L,f}^{cp}(m,n)=0$ and $\varphi_1 = B_{L,m,n,k_1}^{o,dct}(s_1,r_1) - B_{L,m,n,k_1}^{o,dct}(s_2,r_2) \geq \beta$, the block DCT coefficients, are not modified.

[3] If $W_{L,f}^{cp}(m,n)=1$ and $\varphi_2 = B_{L,m,n,k_1}^{o,dct}(s_2,r_2) - B_{L,m,n,k_1}^{o,dct}(s_1,r_1) < \beta$, the block DCT coefficients are modified in the following rule

$$\begin{cases} \hat{B}_{L,m,n,k_1}^{o,dct}(s_2,r_2) = B_{L,m,n,k_1}^{o,dct}(s_2,r_2) + (\beta - \varphi_2)/2 \\ \hat{B}_{L,m,n,k_1}^{o,dct}(s_1,r_1) = B_{L,m,n,k_1}^{o,dct}(s_1,r_1) - (\beta - \varphi_2)/2 \end{cases} \quad (8)$$

If $W_{L,f}^{cp}(m,n)=1$ and $\varphi_2 = B_{L,m,n,k_1}^{o,dct}(s_2,r_2) - B_{L,m,n,k_1}^{o,dct}(s_1,r_1) \geq \beta$, the block DCT coefficients are not modified. In the above process, $\beta = \alpha \cdot B_{L,m,n,k_1}^{o,dct}(1,1)$ is an adaptive robustness control parameter, and α is a tuning parameter, the larger the α is, the more robust the watermark is. However, the quality of stereo image will be decreased if α is too large. Therefore obviously there is a trade-off between the transparency and robustness. Here, α is set to 0.04.

Step-b3 The high frequency DCT coefficients are used for fragile watermark embedding, the detailed procedures of the fragile watermark embedding are expressed by

$$\begin{cases} \hat{B}_{L,m,n,k_1}^{o,dct}(x_1',y_1') = \tau \times B_{L,m,n,k_1}^{o,dct}(x_1,y_1) + \mu \\ \hat{B}_{L,m,n,k_1}^{o,dct}(x_2',y_2') = \tau \times B_{L,m,n,k_1}^{o,dct}(x_2,y_2) + \mu \\ \hat{B}_{L,m,n,k_1}^{o,dct}(x_3',y_3') = \tau \times B_{L,m,n,k_1}^{o,dct}(x_3,y_3) + \mu \end{cases} \quad (9)$$

where τ is a weighting parameter, and μ is an incremental parameter.

Step-b4 After the robust and fragile watermarks are embedded in the non-matchable blocks, the watermarked non-matchable blocks are inverse DCT transformed.

Fragile watermark embedding of the matchable block is described as follows:

Step-c1 Obtain binary chaotic feature watermarks, $W_{L,f}^{cp}(m,n)$ and $W_{R,f}^{cp}(m,n)$, with Eq. (6).

Step-c2 Replace least significant bit (LSB) planes of the matchable blocks, $B_L^o(m,n)$ and $B_R^o(m,n)$, using chaotic feature watermarks, $\{W_{L,f}^{cp}(m,n),\overline{W_{L,f}^{cp}(m,n)}\}$ and $\{W_{R,f}^{cp}(m,n),\overline{W_{R,f}^{cp}(m,n)}\}$, respectively. Here, $\overline{W_{L,f}^{cp}(m,n)}$ and $\overline{W_{R,f}^{cp}(m,n)}$ are $W_{L,f}^{cp}(m,n)$ and $W_{R,f}^{cp}(m,n)$'s complements, respectively.

2.3 Extraction of robust watermark

Extraction of robust watermark in watermarked stereo image is accomplished without referring to the host stereo image, which consists of matchable blocks' and non-matchable blocks' watermark extraction.

The robust watermark extraction of the left view is described as follows

Step-d1 The left and right views of watermarked stereo image are divided into non-overlapping blocks with the size of $k \times k$, the left and right views' blocks are denoted by $B_L^w(m,n)$ and $B_R^w(m,n)$, respectively.

Step-d2 Each block of the left and right views is transformed with DCT, i.e., $B_{L,m,n}^{w,dct} = dct(B_L^w(m,n))$ and $B_{R,m,n}^{w,dct} = dct(B_R^w(m,n)$.

Step-d3 Let $B_{L,m,n,k_1}^{w,dct}$ and $B_{R,m,n,k_1}^{w,dct}$ denote the $k_1 \times k_1$ ($k_1 < k$) upper left corners of $B_{L,m,n}^{w,dct}$ and $B_{R,m,n}^{w,dct}$, respectively, then they are picked up to conduct with SVD, i.e. $[\hat{U}_{L,m,n,k_1}, \hat{S}_{L,m,n,k_1}, \hat{V}_{L,m,n,k_1}] = svd(B_{L,m,n,k_1}^{w,dct})$ and $[\hat{U}_{R,m,n,k_1}, \hat{S}_{R,m,n,k_1}, \hat{V}_{R,m,n,k_1}] = svd(B_{R,m,n,k_1}^{o,dct})$.

Step-d4 Let $\hat{S}_{L,\max}(m,n)$ and $\hat{S}_{R,\max}(m,n)$ denote the largest singular values of the left and right views of the watermarked stereo image. Then, the left and right views' feature watermarks, $\hat{W}_{L,f}(m,n)$ and $\hat{W}_{R,f}(m,n)$, are generated by judging the parity of the highest digits of $\hat{S}_{L,\max}(m,n)$ and $\hat{S}_{R,\max}(m,n)$, respectively.

Step-d5 The matchable block's extracted watermark of the left view is obtained by

$$W_{L,extr}(m,n) = \hat{W}_{R,f}(m, n + d(m,n)) \tag{10}$$

Step-d6 The chaotic feature watermark of $W^{cp}_{L,extr}(m,n)$ is defined as

$$W^{cp}_{L,extr}(m,n) = \begin{cases} 1, & B^{w,dct}_{L,m,n,k_1}(s_2,r_2) \ge B^{w,dct}_{L,m,n,k_1}(s_1,r_1) \\ 0, & \text{else} \end{cases} \tag{11}$$

The non-matchable block's extracted watermark in the left view is computed as

$$W_{L,extr}(m,n) = W^{cp}_{L,extr} \oplus B^{key}_{cp}(m,n) \tag{12}$$

The robust watermark detection in the right view is the same as that in left view.

2.4 Extraction of fragile watermark and tamper detection

Extraction of fragile watermark in the watermarked stereo image is also accomplished without referring to the host stereo image, which consists of matchable blocks' and non-matchable blocks' watermark extraction. For tamper detection, a two-level hierarchical tamper detection scheme, including ***Level-1 detection*** and ***Level-2 detection,*** is applied in the proposed algorithm. The extraction scheme of fragile watermark and tamper detection is presented and described as follows.

Extraction of fragile watermark and ***Level-1 detection***: The steps are as follows:

Step-e1 Define the left and right view's identity matrices $F_L(m,n)=0$ and $F_R(m,n)=0$, respectively.

Step-e2 If $B^w_L(m,n)$ is the matchable block in left view, the chaotic feature watermark $\{W^{cp}_{L,extr}(m,n), \overline{W^{cp}_{L,extr}(m,n)}\}$ is extracted from the LSB planes of the block $B^w_L(m,n)$ directly. And extraction of the chaotic feature watermark $\{W^{cp}_{R,extr}(m,n), \overline{W^{cp}_{R,extr}(m,n)}\}$ in the matchable block $B^w_R(m,n)$ in the right view is the same as that in the left view.

Step-e3 Decrypt the extracted watermark with the correct key.

Step-e4 The identity matrices, $F_L(m,n)$ and $F_R(m,n)$, of the matchable blocks in the left and right views are computed as follows

$$F_L(m,n) = \begin{cases} 1, \hat{W}_{L,f}(m,n) \ne W_{L,extr}(m,n) \text{ or } W_{L,extr}(m,n) = \overline{W_{L,extr}(m,n)} \\ 0, \quad \text{else} \end{cases} \tag{13}$$

$$F_R(m,n) = \begin{cases} 1, \hat{W}_{R,f}(m,n) \ne W_{R,extr}(m,n) \text{ or } W_{R,extr}(m,n) = \overline{W_{R,extr}(m,n)} \\ 0, \quad \text{else} \end{cases} \tag{14}$$

Step-e5 If $B^w_L(m,n)$ is the non-matchable block, the left view's extracted watermark $W_{L,extr}(m,n)$ is retrieved by using Eqs. (11) and (12). Similarly, extraction of the watermark $W_{R,extr}(m,n)$ in the right view is the same as that in the left view. The identity matrices of the non-matchable blocks in the left and right views are updated by

$$F_L(m,n) = \begin{cases} 1, \hat{W}_L(m,n) \ne W_{L,extr}(m,n) \text{ or } (B^{w,dct}_{L,m,n,k_1}(x'_t, y'_t) - \tau \times B^{w,dct}_{L,m,n,k_1}(x_t, y_t) - \mu) > \lambda \\ 0, \quad \text{else} \end{cases} \tag{15}$$

$$F_R(m,n) = \begin{cases} 1, \hat{W}_R(m,n) \ne W_{R,extr}(m,n) \text{ or } (B^{w,dct}_{R,m,n,k_1}(x'_t, y'_t) - \tau \times B^{w,dct}_{R,m,n,k_1}(x_t, y_t) - \mu) > \lambda \\ 0, \quad \text{else} \end{cases} \tag{16}$$

where (x_t, y_t) and (x'_t, y'_t) denote coordinates of DCT coefficients, and t=1,2,3.

Step-e6 Repeat **Step-e2** to **Step-e5** until all blocks in left and right views are implemented.

Level-2 detection: For each invalid block $B^w_L(m,n)$ or $B^w_R(m,n)$ after the ***Level-1 detection*** is operated, the following steps are performed

Step-f1 If the block $B^w_L(m,n)$ in the left view can be searched to find its matchable block $B^w_R(m, n - d'(m,n))$ in the right view with stereo matching, $F_R(m, n - d'(m,n))$ is set to 1, and if the block $B^w_R(m,n)$ in the right view can search its matchable block $B^w_L(m, n + d'(m,n))$ in the left view, $F_L(m, n + d'(m,n))$ is set to 1.

Step-f2: Repeat **Step-f1** until all invalid blocks $B^w_L(m,n)$ or $B^w_R(m,n)$ are implemented.

3 Experimental results and discussions

In order to verify the effectiveness of the proposed algorithm, a series of experiments are tested on four test stereo images 'Doorflower', 'Bowling', 'Dwarves', and 'Art' with the sizes of 1108×1388, and all of them are shown in Fig. 2. Table 1 shows that more than 80% blocks are matchable for different test stereo images. From Fig. 3, it is clear that the watermarked stereo images are imperceptible to human perception. Peak-signal-to-noise-ratio (PSNR) is employed to evaluate the quality of watermarked stereo images, and the PSNR values of four stereo images are shown in Table 2. The adjacent/neighbor DCT coefficients have the certain relevance, in order to ensure the transparency of watermarking, the weighting parameter τ is set to 1 and the incremental parameter μ is set to 0.05,. Fragile watermarking is sensitivity to malicious attacks, the smallest possible parameter λ should be selected, so λ is empirically set to 0.000001 through a lot of experiments. In order to

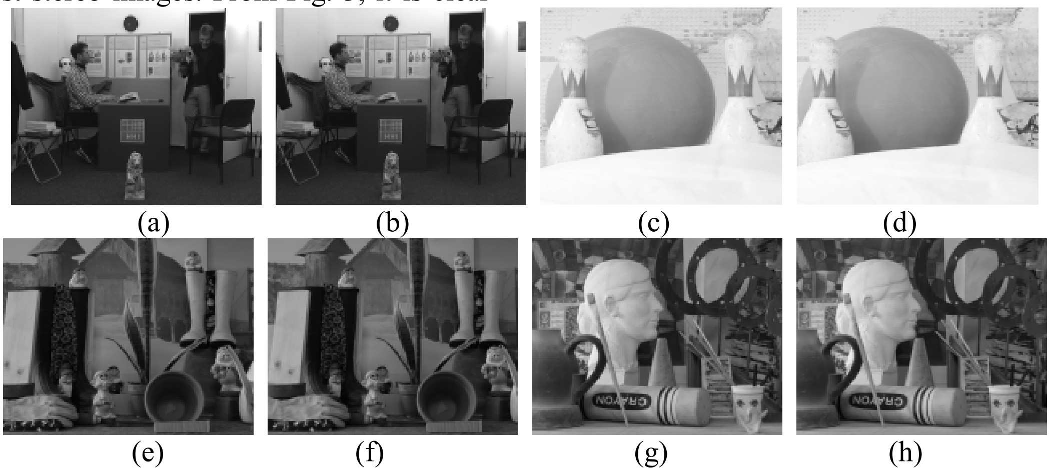

Fig. 2 Test stereo images. (a) the left view of ‘Doorflower’, (b) the right view of ‘Doorflower’, (c) the left view of ‘Bowling’, (d) the right view of ‘Bowling’, (e) the left view of ‘Dwarves’, (f) the right view of ‘Dwarves’, (g) the left view of ‘Art’, (h) the right view of ‘Art’.

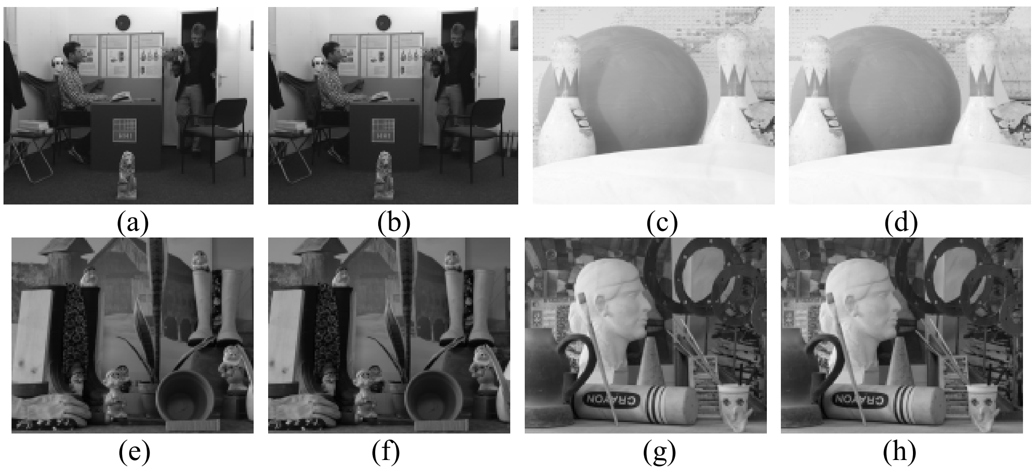

Fig. 3 The watermarked stereo images. (a) the left view of watermarked ‘Doorflower’, (b) the right view of watermarked ‘Doorflower’, (c) the left view of watermarked ‘Bowling’, (d) the right view of watermarked ‘Bowling’, (e) the left view of watermarked ‘Dwarves’, (f) the right view of watermarked ‘Dwarves’, (g) the left view of watermarked ‘Art’, (h) the right view of watermarked ‘Art’.

Table 1. The percentage of matchable blocks in test stereo images

Doorflower	Bowling	Dwarves	Art
85.69%	92.47%	81.25%	82.54%

Table 2. PSNR values of the watermarked stereo images

	Doorflower	Bowling	Dwarves	Art
PSNR value of the left view (dB)	41.930	41.172	43.474	41.462
PSNR value of the right view (dB)	42.011	41.961	43.798	41.666

ensure the transparency of the watermarked stereo image, we embed the fragile watermark into stereo image by modifying the adjacent/neighbor blocks' DCT coefficients, and the coordinates for

Table.3 The experimental results of noise attacks. (NC_L/NC_R)

Stereo image	Gaussian noise		Salt & pepper noise	
	Mean is 0, variance is 0.0005	Mean is 0, variance is 0.001	Noise density is 0.003	Noise density is 0.005
Doorflower	0.9234/0.9268	0.8982/0.9032	0.9745/0.9742	0.9596/0.9600
Bowling	0.9597/0.9597	0.9440/0.9442	0.9803/0.9800	0.9686/0.9686
Dwarves	0.8911/0.8918	0.8662/0.8657	0.9697/0.9691	0.9532/0.9528
Art	0.9322/0.9311	0.9065/0.9049	0.9726/0.9713	0.9553/0.9546

Table.4 The experimental results of filter attacks (NC_L/NC_R)

Stereo image	Median filter		Gaussian low-pass filter	
	window size is [3×3]	window size is [5×5]	window size is [3×3], $\sigma=1$	window size is [5×5], $\sigma=1$
Doorflower	0.9502/0.9547	0.8912/0.8923	0.9624/0.9667	0.9540/0.9563
Bowling	0.9816/0.9823	0.9419/0.9462	0.9874/0.9868	0.9840/0.9831
Dwarves	0.9514/0.9496	0.8538/0.8523	0.9620/0.9616	0.9482/0.9485
Art	0.9611/0.9603	0.8819/0.8782	0.9727/0.9717	0.9610/0.9590

Table. 5 The experimental results of JPEG compression attacks (NC_L/NC_R)

Stereo image	JPEG compression (QF)			
	90	75	60	45
Doorflower	0.9833/0.9837	0.9525/0.9564	0.9359/0.9393	0.9130/0.9144
Bowling	0.9889/0.9887	0.9759/0.9758	0.9658/0.9645	0.9496/0.9489
Dwarves	0.9752/0.9739	0.9364/0.9340	0.9012/0.8969	0.8713/0.8634
Art	0.9880/0.9878	0.9668/0.9645	0.9425/0.9394	0.9192/0.9149

Table. 6 The experimental results of cropping attack (NC_L/NC_R)

Stereo image	Cropping		
	Upper left corner 1/64	Upper left corner 1/8	Upper left corner 1/4
Doorflower	0.9953/0.9954	0.9954/0.9954	0.9958/0.9958
Bowling	0.9988/0.9988	0.9980/0.9979	0.9944/0.9944
Dwarves	0.9963/0.9963	0.9954/0.9951	0.9934/0.9932
Art	0.9973/0.9973	0.9949/0.9950	0.9971/0.9971

Table. 7 The experimental results of size scaling attack (NC_L/NC_R)

Stereo image	Size scaling			
	First lessen to 25%, then magnify to 400%	First lessen to 50%, then magnify to 200%	First magnify to 200%, then lessen to 50%	First magnify to 400%, then lessen to 25%
Door-flower	0.9279/0.9298	0.9846/0.9846	0.9887/0.9887	0.9902/0.9901
Bowling	0.9697/0.9714	0.9938/0.9942	0.9959/0.9963	0.9964/0.9965
Dwarves	0.8960/0.8937	0.9812/0.9810	0.9878/0.9876	0.9908/0.9906
Art	0.9245/0.9220	0.9890/0.9892	0.9924/0.9926	0.9937/0.9933

watermark embedding are selected as $(x_1=3, y_1=3)$, $(x_1'=4, y_1'=4)$, $(x_2=2, y_2=4)$, $(x_2'=3, y_2'=4)$, $(x_3=4, y_3=2)$, $(x_3'=4, y_3'=3)$, $(s_1=2, r_1=3)$ and $(s_1=3, r_1=2)$.

3.1 Symmetrical attacks and tampers

Stereo image is one pair of images (that is, left and right views) with disparity. It is totally different when we see a mono-scopic image and a stereo image. Seeing a mono-scopic image, human eyes can see the same image. However, as for a stereo image, two eyes see two images with somewhat different because of the disparity. In the experiments, symmetrical attacks consist of noise, filtering, JPEG compression, cropping and size scaling attacks in the left and right views of stereo image with the same attack levels. Symmetrical tamper is described below. If one view of stereo image is tempered, while the other view is not tampered, the attack can be authenticated by the naked eyes. Furthermore, if two views of stereo image are tampered with unreasonable disparity, the stereo image can also be authenticated. In the experiments, we presume symmetrical tamper attack that the left and right views of stereo image are modified with reasonable disparity.

3.2 Robustness test

Normalized correlation (*NC*) is used to evaluate the correlation between the feature watermark and the extracted watermark and is expressed by

$$NC_T = \frac{(\sum_{m=1,n=1}^{M/k,N/k} \hat{W}_{T,f}(m,n) \times W_{T,extr}(m,n))}{(\sqrt{\sum_{m=1,n=1}^{M/k,N/k} (\hat{W}_{T,f}(m,n))^2} \times \sqrt{\sum_{m=1,n=1}^{M/k,N/k} (W_{T,extr}(m,n)^2})} \quad (17)$$

where $\hat{W}_{T,f}(m,n)$ (*T=L,R*) and $W_{T,extr}(m,n)$ (*T=L,R*) are the feature watermark and the extracted watermark, respectively. If *NC* is close to 1, then the correlation between $\hat{W}_{T,f}(m,n)$ and $W_{T,extr}(m,n)$ is very high, otherwise, the correlation is very low.

The following experiments with the attacks, such as, noise, filtering, JPEG compression, cropping and size scaling tests, are conducted to test the robustness and efficiency of the proposed algorithm to protect copyright of stereo image.

3.2.1 Noise attack

In this experiment, we perform symmetrical noise attacks with different densities on the watermarked stereo images. Table 3 lists the experimental results of noise attacks, which means the proposed algorithm has strong robustness.

3.2.2 Filtering Attack

In this experiment, we perform symmetrical filtering attacks with different window sizes on the watermarked stereo images, the experimental results are shown in Table 4. The proposed algorithm is robust to Gaussian low-pass filter even the window size is [5×5].

3.2.3 JPEG Compression Attack

JPEG compression is a common image processing operation wherein a stereo image is compressed to reduce its storage requirements and also to reduce the bit rate in transmission. In this experiment, we perform symmetrical JPEG compression attacks with different quality factors (QF) on the watermarked stereo images. Table 5 lists the experimental results of JPEG compression attacks, which demonstrates the proposed algorithm is robust after compressing the watermarked stereo image with QF approximately equal to 45.

3.2.4 Cropping Attack

In this experiment, we perform symmetrical cropping attacks with different sizes on the watermarked stereo images, the experimental results are shown in Table 6. *NC* is close to 1, it is clear that the proposed algorithm is quite robust to cropping attack.

3.2.5 Size scaling attack

In this experiment, we perform symmetrical size scaling attacks with different magnification and lessen size scaling on the watermarked stereo images, the experimental results are shown in Table 7. It is obvious that the proposed algorithm is also quite robust to size scaling attack

3.3 Stereo image authentication and tamper detection

The performances of the proposed fragile watermarking algorithm are evaluated by the two factors mainly, (1) the security of the proposed algorithm, in other words, the capability of the proposed algorithm in resisting various attacks; (2) the accuracy of tamper localization if the watermarked stereo image is tampered. As a way to protect the contents of multimedia, the security of the watermarking algorithm is ultimately important. Moreover, the accuracy of an fragile watermarking algorithm in localizing the tampered region should be highly.

3.3.1 Copy and paste tampers

In the experiments with copy and paste attacks, the watermarked stereo image ‘Door-flower’ is modified by inserting two ‘stone lions’ in its left and right views, where the stone lions are copied from the same view of the watermarked stereo image. The tampered stereo image is shown in Figs. 4(a) and 4(b). The tamper detection results without ***Level-2 detection*** are shown in Figs. 4(c) and 4(d).

The tamper detection results with ***Level-2 detection*** are shown in Figs. 4(e) and 4(f). The results show that ***Level-2 detection*** enhances the accuracy of authentication.

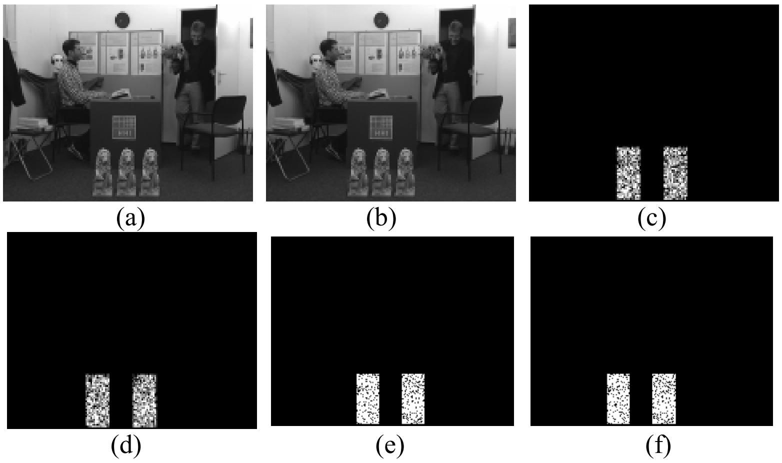

Fig. 4 Copy and paste attacks. (a) tampered left view, (b) tampered right view, (c) detected tampered region in the left view without ***Level-2 detection***, (d) detected tampered region in the right view without ***Level-2 detection***, (c) detected tampered region in the left view with ***Level-2 detection***, (d) detected tampered region in the right view with ***Level-2 detection***.

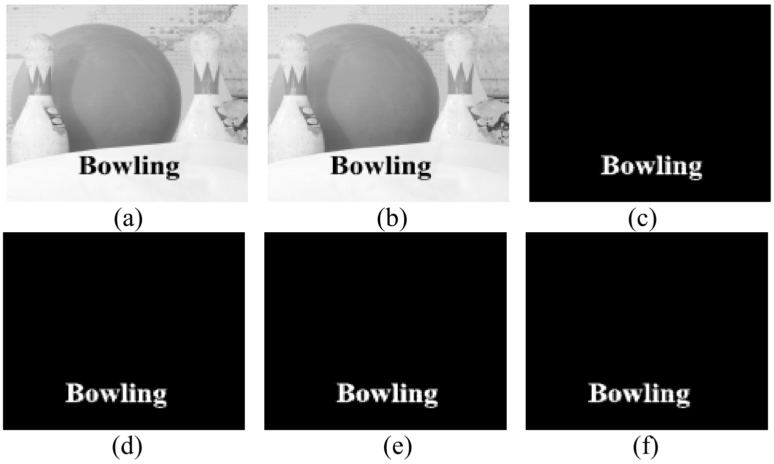

Fig. 5 Text addition.(a) tampered left view, (b) tampered right view, (c) detected tampered region in left view without ***Level-2 detection***, (d) detected tampered region in the right view without ***Level-2 detection***, (c) detected tampered region in the left view with ***Level-2 detection***, (d) detected tampered region in the right view with ***Level-2 detection***.

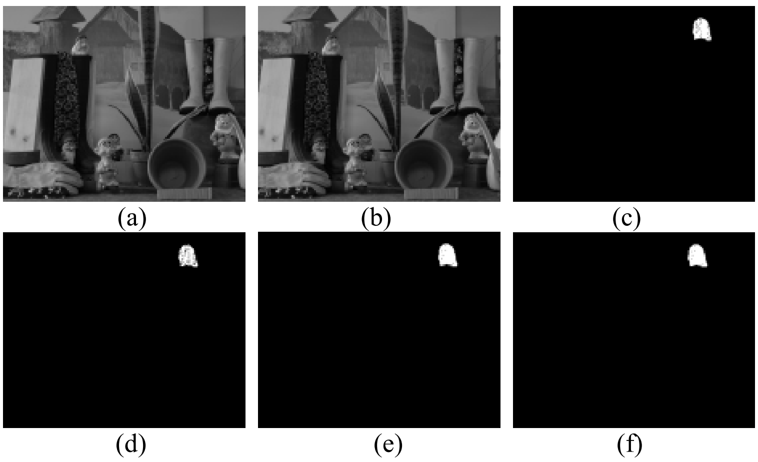

Fig. 6 Content removal. (a) tampered left view, (b) tampered right view, (c) detected tampered region in left view without ***Level-2 detection***, (d) detected tampered region in right view without ***Level-2 detection***, (c) detected tampered region in left view with ***Level-2 detection***, (d) detected tampered region in right view with ***Level-2 detection***.

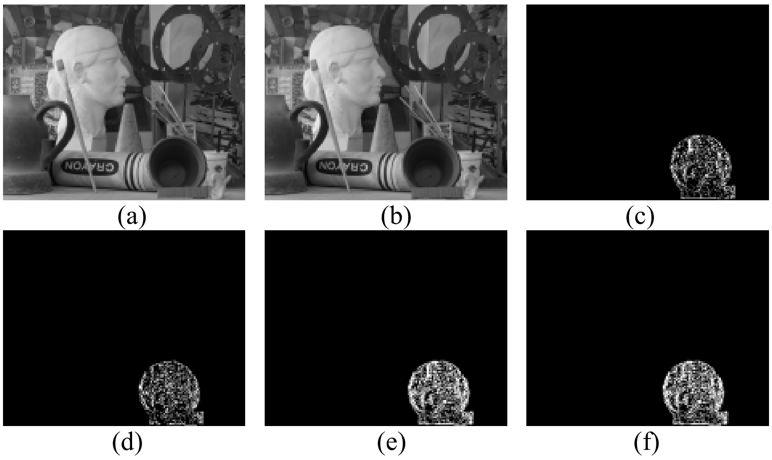

Fig. 7 Collage attack. (a) tampered left view, (b) tampered right view, (c) detected tampered region in left view without ***Level-2 detection***, (d) detected tampered region in right view without ***Level-2 detection***, (c) detected tampered region in left view with ***Level-2 detection***, (d) detected tampered region in right view with ***Level-2 detection***.

3.3.2 Text addition tamper

In this experiment, the watermarked stereo image in Figs. 5(a) and 5(b) are modified by adding the text ‘Bowling’ at the bottom of the stereo image. Detected tampered regions without ***Level-2 detection*** are shown in Figs. 5(c) and 5(d). The tamper detection results with ***Level-2 detection*** are shown in Figs. 5(e) and 5(f). The experimental results show that the proposed algorithm very effective in text addition tamper detection.

3.3.3 Content removal tamper

In this experiment, some content of the watermarked stereo image is removed without degrading the stereo image quality. The ‘dwarf’ have been removed from the watermarked stereo image. The tampered left and right views of stereo image are shown in Figs. 6(a) and 6(b). The tamper detection results without Level-2 detection are shown in Figs. 6(c) and 6(d). The tamper detection results with ***Level-2 detection*** are shown in Figs. 6(e) and 6(f). The results show that ***Level-2 detection*** enhances the accuracy of authentication.

3.3.4. Collage attack

The counterfeit left view of stereo image, as shown in Fig. 7(a) is constructed by copying the 'crock' from Fig. 3(e) and inserting theirs in relative spatial location in foreground from Fig. 3(g). Construction of the counterfeit right view of stereo image is the same as that of the counterfeit left view. Fig. 7(b) show the counterfeit right view of stereo image. Figs. 7(c) and 7(d) show the detected tampered regions without ***Level-2 detection***. Figs. 7(e) and 7(f) show the detected tampered regions with ***Level-2 detection***. The results show that ***Level-2 detection*** improves previously ***Level-1 detection*** and enhances authentication accuracy.

According to Figs. 4-7, the tampered parts of the embedded stereo image are located correctly. A 2-level hierarchical tamper detection scheme improves stereo image tampering detection accuracy and precision.

4 Conclusion

To simultaneously protect copyright and detect tamper for a given stereo image, a multipurpose-based stereo image watermarking algorithm is presented for three dimensional multimedia. The robust and fragile watermarks are embedded in stereo image with different techniques according to block types. At the receiving side, using stereo marching as a bridge, the robust and fragile watermarks can be extracted without the host stereo image. Experimental results demonstrate that the proposed algorithm is not only robust to the common signal processing attacks and but also sensitive to tampering. The major contributions of this work include the following aspects, (1) According to the stability of low frequency coefficients and largest singular value, the robustness of stereo image watermarking is improved. (2) A two-level hierarchical tamper detection scheme is presented to improve stereo image tampering detection accuracy and precision. (3) For the purpose of protection, the proposed algorithm guarantees that, no matter what kind of attack is encountered, at least one watermark can survive well. On the other hand, for the purpose of authentication, the proposed algorithm can effectively detect tamper and locate forgery.

In future work, we will focus on studying stereo image and video watermarking algorithm to realize the copyright protection and authentication. Moreover, more efforts will be focused on stereo visual attention for multipurpose-oriented stereo image watermarking algorithm to improve the robustness and transparency of watermark.

Acknowledgements

This work was supported by the Natural Science Foundation of China (Grant No. 61302112), the Zhejiang Provincial Natural Science Foundation of China (Grant Nos. LY14F010004, LY13F050005), innovative Scientific Research Project for Postgraduates in Zhejiang Province (Grant No. YK2011049), the Scientific Research Foundation of Graduate of Zhejiang Province (Grant No. YK2011049), the Zhejiang University of Science and Technology startup fund, and the Research Foundation of Education Department of Zhejiang Province (Y201224839).

References:

[4] N. Narita, M. Kanazawa, "Analysis of psychological factors for HDTV/3-D HDTV and evaluation method of their overall impressions," *IEEE Transactions on Broadcasting,* vol. 59, no.1, 2013, pp. 13-19.

[5] A. J. Woods, C. R. Harris, D. B. Leggo, "Characterizing and reducing crosstalk in printed anaglyph stereoscopic 3D images," *Optical Engineering,* vol. 52, no.4, 2013, pp. 043203.

[6] A. Chammem, M. Mitrea, F. Prêteux, "Stereoscopic video watermarking: a comparative study," *annals of telecommunications-annales des télécommunications,* vol.68, no.11-12, 2013, pp. 673-690.

[7] K. Zebbiche, K. Fouad, "Efficient wavelet-based perceptual watermark masking for robust fingerprint image watermarking," *IET Image Processing*, vol. 8, no.1, 2014, pp.23-32.

[8] F. Liu,Q. K. Fu, L. M. Cheng, "Wave-atoms-based multipurpose scheme via perceptual image hashing and watermarking," *Applied Optics*, vol. 51, no. 27, 2012, pp.6561-6570.

[9] L. Tian, N. Zheng, J. Xue, et al, "An integrated visual saliency-based watermarking approach for synchronous image authentication and copyright protection," *Signal Processing: Image Communication*, vol. 26, no. 8, 2011, pp. 427-437.

[10] M. H. Lee, K. H. Bae, J. J. Kim, E. S. Kim, "New watermark scheme for copyright protection of the stereo vision system using adaptive disparity matching algorithm," *Proc. SPIE*, vol. 5108, 2003, pp. 210-219.

[11] D. C. Hwang, K. H. Bae, M. H. Lee, E. S. Kim, "Real-time stereo image watermarking using discrete cosine transform and adaptive disparity maps," *Proc. SPIE*, vol. 5241, 2003, pp. 233-242.

[12] D. C. Hwang, K. H. Bae, M. H. Lee, E. S. Kim, "Stereo image watermarking scheme based on discrete wavelet transform and adaptive disparity estimation," *Proc. SPIE*, vol. 5208, 2004, pp. 196-205.

[13] D. Coltuc, "On stereo embedding by reversible watermarking: Further results," International Symposium on Signals, Circuits and Systems, 2007, pp. 1-4

[14] D. Coltuc, I. Caciula, H. Coanda, "Color stereo embedding by reversible watermarking," *ISEEE*, 2010, pp. 256-259.

[15] Y. Niu, W. Souidene, A. Beghdadi, "A visual sensitivity model based stereo image watermarking scheme," *EUVIP*, 2011, pp. 211-215.

[16] Y. H. Lin, J. L. Wu, "A digital blind watermarking for depth-image-based rendering 3D images," *IEEE Transactions on Broadcasting,* vol. 57, no.2, 2011, pp. 602-611.

[17] H. D. Kim, J. W. Lee, T. W. Oh, H. K. Lee, "Robust DT-CWT watermarking for DIBR 3D Images," *IEEE Transactions on Broadcasting,* vol. 58, no. 4, 2012, pp. 533-543.

[18] S. Wang, C. Cui, Niu X, "Watermarking for DIBR 3D images based on SIFT feature points," *Measurement*, vol. 48, 2014, pp. 54-62.

[19] M. Yu, A. Wu, T. Luo, G. Jiang, F. Li, S. Fu, "New block-relationships based stereo image watermarking algorithm," *ICSNC*, 2011, pp. 171-174.

[20] T. Luo, G. Jiang, X. Wang , "Stereo image watermarking scheme for authentication with self-recovery capability using inter-view reference sharing," *Multimedia Tools and Applications,* online, 2013, pp. 1-26.

[21] P. Campisi, "Object-oriented stereo-image digital watermarking," *Journal of Electronic Imaging,* vol. 17, no. 4, 2008, pp. 043024.

[22] G. Bhatnagar, S. Kumar, B. Raman, "Stereo image coding via digital watermarking," *Journal of Electronic Imaging,* vol. 18, no. 3, 2009, pp. 033012.

[23] T. Bianchi, P. Alessandro, "Secure watermarking for multimedia content protection: a review of its benefits and open issues," *IEEE Signal Processing Magazine*, vol. 30, no. 2, 2013, pp. 87-96.