Copyright protection in digital museum based on digital holography and discrete wavelet transform

Zhibin Li (李志斌)[1,2], Fei Xia (夏 飞)[2], Gang Zheng (郑 刚)[1], and Junyong Zhang (张军勇)[1]

[1]*College of Optics and Electronics Engineering, University of Shanghai for Science and Technology, Shanghai 200093*

[2]*Faculty of Electric and Automatic Engineering, Shanghai University of Electric Power, Shanghai 200090*

Received October 8, 2007

A new method to protect the copyright of digital museum based on digital holography is proposed. The Fresnel hologram of watermark image is embedded in the object to be protected through discrete wavelet transform (DWT). After the watermark detection, the copyright information appears in the reconstructed hologram. With the higher redundancy feature in the hologram, the proposed technique can actually survive several kinds of image processing. Experimental results prove that the presented method has good robustness in image protection.

OCIS codes: 090.1760, 100.2000, 100.3010, 100.7410.

With the rapid development of multi-media technique and computer networks, it is very important to construct digital museum for protecting precious resources. However, the precious digital contents are easier and faster to be duplicated, modified and redistributed than before. Hence, digital content protection has become one of the most important and urgent issues. Recently, digital watermarking techniques, complement to cryptography, are growing at an exponential rate. Watermarking is a method of hiding authorized mark pattern information in a host image to achieve perceptual invisibility and thus retrieving the hidden mark information from the host image to prevent copying and protect copyright. Copyright watermarking is a type of robust digital watermarking. It embeds an identical copyright message, so-called watermark, which indicates the owner's or creator's identification, into each copy of the digital content. The characteristics to be considered in copyright watermarking include the capacity of the information that can be extracted after a watermark is embedded, the imperceptibility of the embedded information, and the robustness which prevents the embedded information from being removed intentionally or even unintentionally[1−4].

Watermarking techniques can be usually classified into spatial domain techniques and transform domain techniques. In the former the watermark is encoded by directly modifying pixels, whereas in the latter the watermark is encoded by altering some frequency bins obtained from transforming the image in the frequency domain. Spatial domain techniques are less complex, but they are less robust to tampering and attacks than transform domain techniques which place the watermark signal in the most perceptually significant components of a transform domain (Fourier transform, cosine transform, wavelet transform)[2,4,5]. Cox *et al.* explained the advantages of frequency-based method. The insertion of a watermark under this regime makes the watermark robust to signal processing operations[1]. To more effectively hide a robust watermark, the approach to mask the watermark should possibly utilize the characteristics of the human visual system (HVS). A widely used technique exhibiting a strong similarity to the way that the HVS processes images is discrete wavelet transform (DWT)[3]. Many watermarking algorithms have been developed that embed the watermark in the wavelet transform domain[6].

As is well known, holography can be used to record the complete amplitude and phase information of an object via interferometric procedures, and can also be used for information security, including various security holograms that are extensively adopted in credit cards, passports, and trade mark applications to prevent illegal readout and retrieval. More recently, a new three-dimensional (3D) watermarking technique has been suggested[5,7], in which hologram as watermark data is embedded into the cover image, for improving the performance of conventional watermarking system against some attacks such as noise, cropping, and so on. Hologram is an interference pattern containing whole information of an object and can be reconstructed only with partial data, even though some of the embedded hologram data are lost by some possible attacks. It is worth pointing out that the parameters such as distance and wavelength used to embed a watermark are only governed by a watermark designer or copyright holder, but unknown to authorized users and also unknown to unauthorized third-party users. Therefore, the watermark should be secure in the sense of secret parameters. A virtual-optical imaging scheme (VOIS) as a watermarking structure was proposed by Peng *et al.* to embed a watermark into a content image to construct a watermarked image in 3D space[5]. Deng *et al.* introduced a cascaded Fresnel digital holography (CFDH) technique to hide information. In this technique, the reconstructed image of copyright is produced by two sub-holograms located at different positions along the illuminating beam. But the reconstructed image is degraded with the number N of phase quantization decreasing[8].

In this letter, we describe a new digital holographic copyright watermarking scheme based on DWT, in which the watermark is constructed with a digital Fresnel hologram of the copyright information, and thus the hologram is embedded into a cover image with DWT. Detection of the hidden copyright information in a possibly watermarked image is performed with a digital hologram reconstruction. To show the usefulness of the proposed scheme, some simulation experiments have been carried out and the results are compared with those of the conventional methods in terms of robustness for some possible attacks.

The Fresnel diffraction formula is used to generate the hologram and obtain the reconstruction for copyright information. As illustrated in Fig. 1, the optical phenomena in the recording and reconstruction stages of in-line holography can be expressed by the theory of wave optics, and hence

$$u_z\left(x, y, z; u_0\left(\xi, \eta\right)\right) = u_0\left(x, y\right) \otimes P_z(x, y) \qquad (1)$$

can be employed for theoretically and numerically obtaining the light intensity distributions on the hologram plane and the image plane[9,10]. In Eq. (1), $\otimes$ represents convolution, u_z is the light amplitude on the hologram plane, $u_0\left(\xi,\eta\right)$ is called the transparency function which expresses the distribution of opaque objects and transparent space on the object plane, $P_z(x, y)$ represents the Fresnel diffraction kernel,

$$P_z(x, y) = \frac{\exp\left(jkz\right)}{j\lambda z}\exp[\frac{jk}{2z}(x^2 + y^2)],$$

where λ is the wavelength of illuminating light and j denotes the imaginary unit. The Cartesian coordinates on the object plane, the hologram plane and the image plane are respectively denoted by (ξ, η), (x, y), and (x_z, y_z). z is the distance between the object plane and the recording plane, and z' is the reconstructed distance.

The interference fringes on the hologram plane are formed according to the shape and layout of copyright image on the object plane, and the fringes are expressed by

$$I_z = u_z u_z^*, \qquad (2)$$

where the asterisk represents the complex conjugate, I_z is the light intensity and u_z is the light amplitude on the hologram plane, given by $u_z\left(x, y, z; u_0\left(\xi, \eta\right)\right)$.

Next, in the stage of image reconstruction, the real image on the image plane can be formed according to the intensity

$$I_{z'} = u_{z'} u_{z'}^*, \qquad (3)$$

where $u_{z'}$ is the light amplitude on the image plane, given by $u_{z'}\left(x_z, y_z, z'; I_z\left(x, y\right)\right)$.

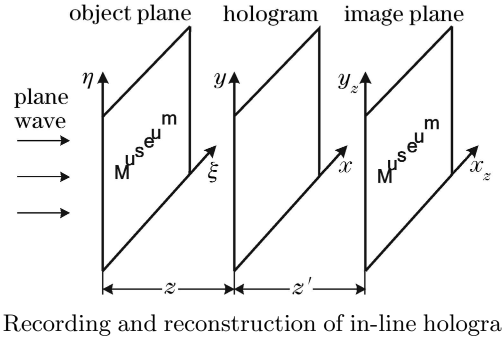

Fig. 1. Recording and reconstruction of in-line holography for watermark image.

The digital hologram can be numerically calculated from object plane using Eqs. (1) and (2). The image reconstruction is digitally and numerically carried out from the observed hologram pattern, expressed by $I_{z'}$, using Eqs. (1) and (3).

Most watermarking algorithms transform the host image into a domain that facilitates embedding of the watermark information in a robust and imperceptible way. In this letter, we focus on watermarking algorithms operating in the wavelet domain. The proposed method embeds watermark by decomposing the host image and the watermark using wavelet transform. It has been experimentally indicated that human vision reacts with different sensitivity to each frequency band, which is divided into several narrow band channels[11]. Human eye is less sensitive to noise in high frequency subbands. To embed the watermark robustly and imperceptibly, HVS characteristics are used in selecting the significant coefficients and adding the watermark to these coefficients.

HVS is less sensitive to changes in the neighborhood of the edges than in the smooth regions of the image. The characteristics are used in selecting the significant coefficients to which the watermark is added. We adopted an approach similar to the method presented by Reddy *et al.*[4]. Our aim is to test the validity of the Fresnel hologram as the watermark.

The host image and the watermark image are wavelet decomposed respectively. After the significant coefficients from each subband are selected based on the weight factors, the watermark is added to all selected wavelet coefficients. The algorithm for embedding watermark image is formulated as follows (for simplification, we only decompose the host image in 2-level wavelet).

Step 1: Decompose the host image by 2 levels and the watermark image by 1 level using DWT (as shown in Fig. 2). LL_2, HL_2, LH_2, HH_2, HL_1, LH_1, HH_1 represent the coefficients of each band of host image. WL_1, WH_1, WV_1, and WD_1 represent coefficients of low frequency, coefficients of horizontal high frequency, coefficients of vertical high frequency and coefficients of diagonal high frequency at level 1 of watermark respectively.

Step 2: For more invisible watermark, WL_1 is embedded in coefficients of low-low band at level 2 of host image using

$$\mathrm{ML}_2'(i, j) = \mathrm{ML}_2(i, j) + \alpha w(i, j)\mathrm{WL}_1(i, j). \qquad (4)$$

The watermark strength is controlled by α, and the weight factor for wavelet coefficients is $w(i, j)$[2]. The

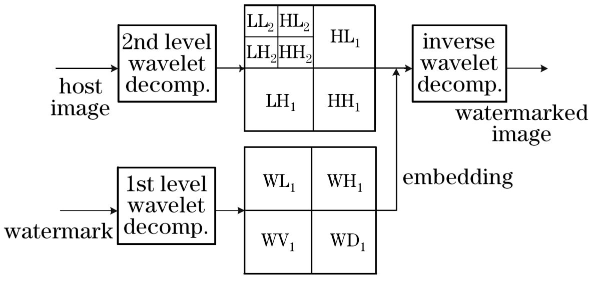

Fig. 2. Watermark embedding.

coefficients which have weight factors more than threshold value are considered as significant coefficients and are used for embedding the watermark.

Step 3: For more robust watermark, the watermark bits WH_1, WV_1, and WD_1 are repeatedly added to the selected coefficients HL_1, LH_1, and HH_1,

$$\mathrm{MH}_1'(i,j) = \mathrm{MH}_1(i,j) + \alpha w(i,j)\mathrm{WH}_1(i,j), \quad (5)$$

$$\mathrm{MV}_1'(i,j) = \mathrm{MV}_1(i,j) + \alpha w(i,j)\mathrm{WV}_1(i,j), \quad (6)$$

$$\mathrm{MD}_1'(i,j) = \mathrm{MD}_1(i,j) + \alpha w(i,j)\mathrm{WD}_1(i,j). \quad (7)$$

Step 4: After embedding watermark bits, 2-level inverse wavelet transform of the image is found out to get the watermarked image.

For watermark recovery from watermarked image, both the original and the watermarked images are needed. The steps for watermark extraction are as follows.

Step 1: Both original and watermarked images are 2-level wavelet decomposed to find out the coefficients of different scales in high frequency and two sets of coefficients in low frequency, LL_2 and WLL_2.

Step 2: Calculate the coefficients of the watermark in low frequency with LL_2 and WLL_2,

$$\mathrm{WL}(i,j) = \frac{\mathrm{ML}_2'(i,j) - \mathrm{ML}_2(i,j)}{\alpha w(i,j)}, \quad (8)$$

where $\mathrm{ML}_2'(i,j)$ is the suspicious image in low band[2].

Step 3: Subtract the corresponding coefficients of high-low, low-high and high-high bands in the same scale between the two images. The mean of those differences are the coefficients of watermark in high frequency.

Step 4: Take 1-level inverse wavelet transform of the coefficients obtained in Steps 2 and 3 to form the extracted watermark.

In order to demonstrate the theoretical predictions of the digital holographic watermarking scheme, we digitally implement it in cyberspace with numerical simulations. A series of simulation experiments are tested under the environment of MATLAB7.0. In the numerical experiments, we select the virtual optical wavelength $\lambda = 632.8$ nm, $z = z' = 0.5$ m, the images with 512×512 pixels. In the proposed method, the original copyright object is transformed into the hologram as watermark image and reconstructed from the watermark image with correct parameters through a computational pickup process, as shown in Figs. 3(a)—(c). To detect the copyright image we need to reconstruct from watermarked image with correct parameters z' and λ. It should be noted again that the parameters z' and λ keep secret to unauthorized users so that it would be very difficult to get the copyright information without correct values of these two parameters, as shown in Figs. 3(d) and (e).

Next, the watermark generated from the copyright image of Fig. 3(b) is embedded into the original host image of Fig. 4(a). The watermarked image is shown in Fig. 4(b). From the received watermarked host image, the embedded watermark is extracted through the extraction process and the result is shown in Fig. 4(c). Figure 4(d) shows the reconstructed copyright image from the retrieved watermark. We can see that the copyright information is retrieved from the watermarked image with two correct parameters. And it is blind to unauthorized users.

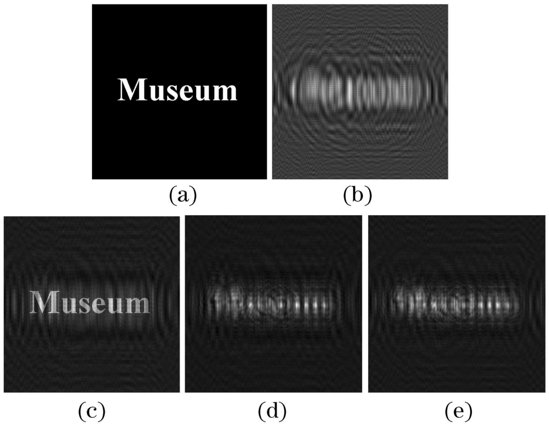

Fig. 3. Watermark embedding and reconstruction based on digital holography. (a) Information of watermark (binary, 512×512 pixels); (b) hologram of watermark; (c) reconstruction of watermark information; (d) reconstruction at $z' = 0.51$ m, $\lambda = 632.8$ nm; (e) reconstruction at $z' = 0.5$ m, $\lambda = 500$ nm.

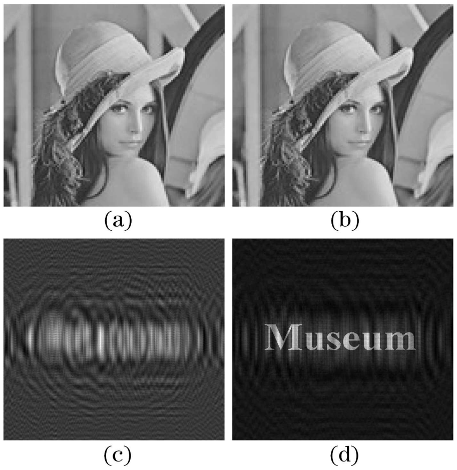

Fig. 4. Computer simulation experiment. (a) Host image (gray level, 512×512 pixels); (b) watermarked image; (c) retrieved watermark; (d) reconstruction of copyright information.

Figure 5 shows some experimental results on extraction of copyright image from the watermarked host image attacked by four kinds of conventional watermarking method. Four images of Figs. 5(a), (c), (e), and (g) show the host images watermarked with hologram of copyright image and attacked by smooth filtering, noises, cropping and JPEG compression respectively. Four images of Figs. 5(b), (d), (f), and (h) show the copyright images extracted from these watermarked images. From Fig. 5(d), it is found that the extracted copyright data ‘Museum’ is not clear and contaminated with noises and its quality is degraded. In Figs. 5(b) and (f), the extracted copyright information can be distinguished although it is darker.

From the test results, these attacked methods do not degrade the image quality of the copyright information so much, because the watermark images themselves are

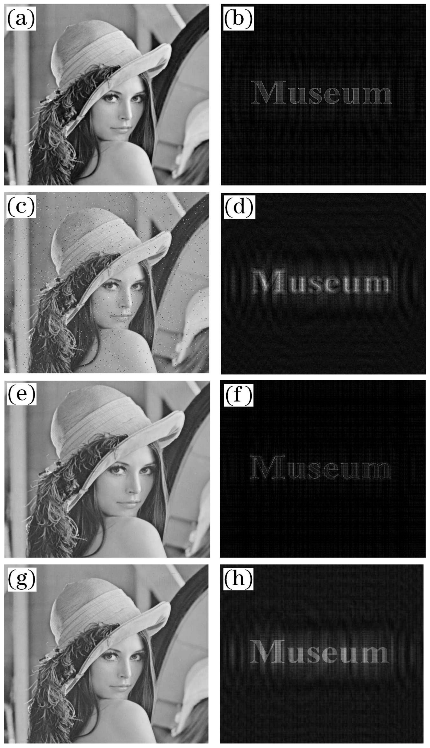

Fig. 5. Robustness simulation experiments. (a) Watermarked image with smooth filtering; (b) reconstruction of (a); (c) watermarked image with noise adding; (d) reconstruction of (c); (e) watermarked image with cropping; (f) reconstruction of (e); (g) watermarked image with JPEG compression; (h) reconstruction of (g).

not the final copyright data in the proposed method, although the final copyright information is generated form these watermark images. Here, the extracted watermark images, for example that in Fig. 4(c), might look meaningless, but through an additional processing according to Eq. (3), they can turn out to be meaningful for the use of copyright identification. The results shown in Fig. 5 reveal that embedded copyright data can be most exactly extracted, although the watermarked images are severely attacked by some methods. Accordingly, these experimental results could finally suggest the robustness of the proposed digital holographic watermarking scheme against attacks.

In conclusion, a new digital holographic watermarking scheme based on DWT, employing a Fresnel hologram of copyright image as the watermark data, has been proposed. The property of the holographic watermark can support a robust reconstruction of the watermark image even though there will be some data losses in the embedded watermark by attacks. Simulation experimental results imply that the watermark embedded with the proposed method should be difficult to remove even if watermarked image is attacked. This technique will find application in protection of copyright of digital museum.

This work was supported by the Program of Shanghai Municipal Education Commission under Grant No. 05LZ12. Z. Li's e-mail address is thermal_li@163.com.

References

1. I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, IEEE Trans. Image Processing **6,** 1673 (1997).
2. M. Barni, F. Bartolini, and A. Piva, IEEE Trans. Image Processing **10,** 783 (2001).
3. K. R. Kwon and A. H. Tewfik, Proc. SPIE **4675,** 334 (2002).
4. A. A. Reddy and B. N. Chatterji, Pattern Recogn. Lett. **26,** 1019 (2005).
5. X. Peng, L. Yu, and L. Cai, Opt. Commun. **226,** 155 (2003).
6. P. Meerwald and A. Uhl, Proc. SPIE **4314,** 505 (2001).
7. S. Kishk and B. Javidi, Opt. Express **11,** 874 (2003).
8. S. Deng, L. Liu, H. Lang, W. Pan, and D. Zhao, Chin. Opt. Lett. **4,** 268 (2006).
9. U. Schnars and W. Jüptner, Appl. Opt. **33,** 179 (1994).
10. T. Kreis, M. Adams, and W. Jüptner, Proc. SPIE **3744,** 54 (1999).
11. I. Lee, J. Kim, Y. Kim, S. Kim, G. Park, and K. T. Park, in *Proceedings of APCCAS 94* 619 (1994).