Research of Image Watermarking Algorithm and Application in Eco-Tourism Digital Museums Copyrights Protection

Li-hua Wu, Wen-juan Jiang and Junkuo Cao

Abstract Digital watermarking technology being an important application of information hiding technology has become currently a hot issue in the field of digital information security. This chapter first discusses the digital copyright protection and safety requirements of the digital museum and then describes a common model of information hiding, digital watermarking technology of discrete cosine transform (referred as DCT), and its features in detail. At the same time, the chapter gives a DCT-based JPEG color image invisible watermarking algorithm, as well as swf animation file information hiding watermarking algorithm, in order to improve the information watermark security and attack resistance in the digital museum. The experimental tests show that the algorithm can better balance between imperceptibility, robustness, and security.

Keywords Digital media rights · Discrete cosine transform domain · Information hiding · Image watermarking

1 Introduction

Along with the constant development of network technology, digital museum is widely used in Internet and has its unique advantages. However, today's digital exhibits are likely to face a series of problems such as being copied, distributed, juggled, illegally obtained, and copyright infringement. Thus, the digital image copyright protection issues must be resolved under such background.

Usually, invisible image watermarks have the following two basic characteristics. The first is invisibility, and it is difficult to visually perceive the difference

L. Wu (✉) · W. Jiang · J. Cao
School of Computer Science and Technology, Hainan Normal University, HaiKou 571158, China
e-mail: lihuawu63@163.com

B.-Y. Cao et al. (eds.), *Ecosystem Assessment and Fuzzy Systems Management*,
Advances in Intelligent Systems and Computing 254, DOI: 10.1007/978-3-319-03449-2_23,

between the watermarked image and the original image. The second is robustness, and also, the embedded watermark is robust against various signal processing. Since these two characteristics contradict each other. How to take a compromise, to ensure watermark invisibility under the premise, but also embedded the powerful watermark information possible. This is an important issue in the field of digital watermarking research.

2 The General Model of Information Hiding System

The digital watermark is interdisciplinary involving digital signal processing, image processing, cryptography, communication theory and algorithm design and other fields. Its basic idea is that the original copyright information in the works (source version, the original author, owner) instead as watermark information, and it is embedded into the image, text, video, audio and other digital media works (original carrier) through a certain algorithm, but does not affect the value in use or commercial value of the embedded watermark digital media works. Digital watermarking algorithm not only can identify the relevant information of owners which is embedded in the carrier object, but also can extract the information when needed [1].

In general, the generic model for information hiding core system consists of two phases: the watermark embedding and watermarking detection or extracting, as shown in Fig. 1.

In the above model, watermarking information can be copyright message or secret data or a serial number. The public data without watermark are called original carrier such as video and audio clips. Generally, the information hiding process is controlled by the secret key. The watermarking information is hidden in public information via embedding algorithm. And detection algorithm can extract the secret watermarking information from the watermarked carrier by means of a secret key.

For all this, the digital watermark embedded into digital exhibits of the digital museum must have the following basic characteristics [2, 3]:

1. **Imperceptibility or concealment.**

The digital watermark is invisible to anyone by seeing or hearing. The ideal watermark carriers (digital media with watermark) are exactly the same as the original carrier visually.

2. **Security.**

The procedure of the watermark embedding should be confidential. The methods of embedding and detecting digital watermarking are confidential to unauthorized third parties and cannot be easily cracked. Besides, unauthorized

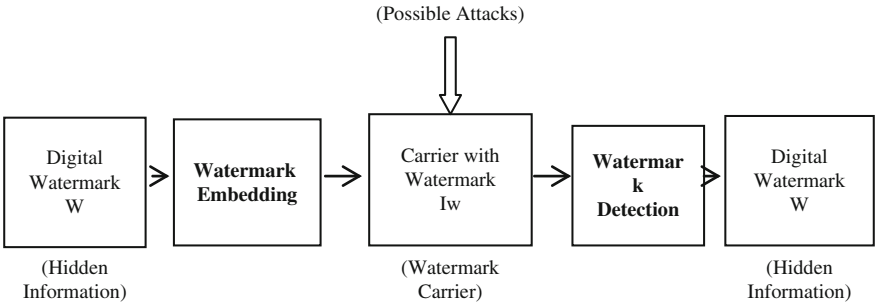

Fig. 1 The general model for information hiding core system

users cannot eliminate or destroy the watermark by changing the watermark carrier.

3. **Robustness or anti-aggressive capability.**

The digital watermark should be able to withstand a large number of physical and geometrical distortions, including intentional malicious attacks or image compression, filtering, scanning, copying, and size conversion After these operations, digital watermarking algorithm should still be able to extract watermark embedded from the watermark carrier or prove the presence of the watermark.

4. **Provability.**

The message carried by the digital watermark should be identified uniquely and certainly, so as to provide the ownership of digital exhibits with completely reliable evidence.

2.1 Digital Watermark Embedding

Assuming that original carrier is *I,* the digital watermarking is *W*, the carrier with watermark I_w, and the secret key *K*. Then, the process of watermark embedding is shown in Fig. 2.

As shown here, the common formula for the process of digital watermark embedding can be defined as follows:

$$I_W = E(I, W, K) \tag{1}$$

Among them, I_w means the data after the embedding watermark, I stands for the original carriers of data, and W refers to the watermark set. The algorithm of generating watermark G should ensure the properties of the watermark such as uniqueness, validity, and irreversibility. K stands for the secret key set (you can

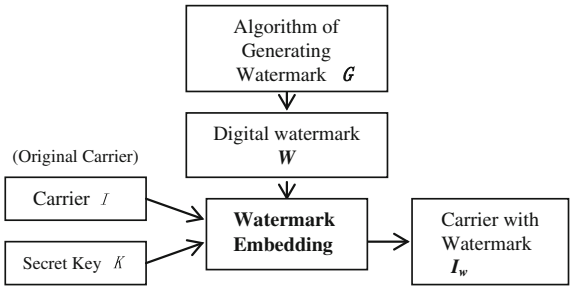

Fig. 2 The process of watermark embedding

choose the private key or public key usually). All utility systems must use a secret key and even the combination of several keys in some case. The watermarking information W is the data that can be existed in any form, e.g., random sequence or pseudo-random numbers, character or grid, binary image, gray image or color image, and 3D image. The watermarking information W can be generated by random number generator. When the digital watermark embedding stage, to find a better medium between and among intangibility, safe reliability and robustness for the digital watermark is the aim of embedding algorithm. Secret key K can be used to strengthen security, so as to avoid unauthorized restoration and rehabilitation of watermark [4].

2.2 Digital Watermarking Detection

The process of watermarking detection can be divided into two parts, as shown in Fig. 3.

Figure 3 is a sort of schematic diagram of the process of watermarking detection. Among them, remarks the extracted watermark, D indicates the watermark detection algorithm.

$\widehat{I}_W$ means the watermarking carriers of data after being attacked during transmission. The means of detecting a watermark can be divided into two kinds. The first one is extracting the embedded signal or testing the correlation verification of the embedded signal with the original information, and second is that the embedded information must be fully searching method or hypothesis testing without the original information. Generally, the result is presented in two forms: the one is exporting an extracted watermark and the other is exporting whether the monitored information contains the specified watermark [4].

As shown in Fig. 3, the common formula for the process of watermarking detection can be defined as follows:

- When there is the original carrier data,

$$\widehat{W} = D(\widehat{I}_W, I, K) \tag{2}$$

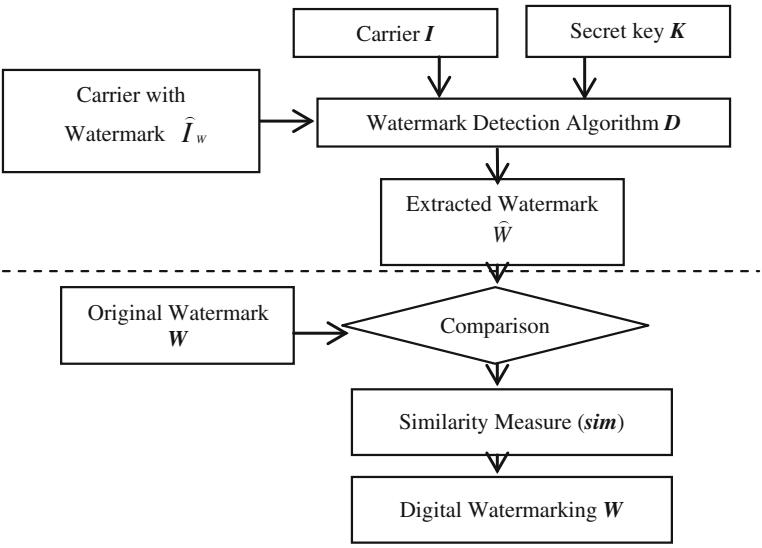

Fig. 3 The process of watermarking detection

- When there is no original information,

$$\hat{W} = D(\hat{I}_W, K) \tag{3}$$

3 Comparing Image Invisible Watermarking Algorithm

Invisible image watermarking can be classified as digital watermarking in space domain and digital watermarking in transform domain in accordance with its hiding location. Currently, the research of invisible image watermarking focuses on the technology of digital watermarking in transform domain.

3.1 Digital Watermarking in Space Domain

Essentially, the earlier digital watermarking algorithm is adopted in the space region. The digital watermarking is loaded directly in the data. The known algorithm in space is least significant bit (referred LSB) method, and its principle is that adjust the watermarking information conveyed by resolution unimportant to perception by modifying the color bit plane of digital images, to achieve the purpose of embedding the watermark.

LSB method has the advantage of a small amount of calculation and a larger amount of information hiding. But the watermarks generated are fragile and cannot resist ordinary signal processing. After the digital image is processed and transformed, pixel of the low is extremely malleable. In addition, what most algorithms introduce is the watermark similar to high-frequency noise, and it is easy to remove a watermark after low-pass filtering or loss compression operation. Hence, this algorithm has poor robustness and is not suitable for copyright protection applied to the museum of digital works.

3.2 Digital Watermarking in Transform Domain

When you choose to change middle-frequency or low-frequency component to add a watermark, large number of bits can be embedded in the frequency domain of the image without causing visual degradation. You can improve the robustness greatly. Digital watermarking in frequency domain is also known as transform domain watermarking. The basic idea of the transform domain watermarking is the first carrier signal of the data by a certain method to the frequency domain, and again after the watermark information is embedded in the frequency domain, the last of the processed signal for inversely converting the data signal back to the level of the carrier, thereby forming a final watermarked. More commonly used transform consisted of discrete Fourier transform (referred as DFT), discrete cosine transform (referred as DCT), and discrete wavelet transform (referred as DWT). Since media messages after transformation have obvious virtues of concentrated distribution of energy, good frequency division, etc., it can fit in easily with the awareness model of human visual system. Thus, the media messages after transformation can regulate the balance between the robustness and the imperceptivity easily [5].

4 Image Invisible Watermarking Algorithm of DCT

A watermarking algorithm of DCT transform domain is a research hot spot in the study of watermarking for the moment. Because DCT transform is second only to quadrature transform, and its algorithm is relatively easy to implement, DCT transform is commonly applied to image compression technology (e.g., JPEG). This also makes the watermarking based on the DCT method more resistant to JPEG compressing attack. Moreover, it makes the final watermark carrier to have good robustness.

Two-dimensional DCT transform is often used for digital picture processing. An image digital watermarking based on 2D-DCT is basically the idea that firstly divides an image into $N \times N$ parts. And then two-dimensional DCT transform is

performed on each part. Let $F(x, y)$ denote the $N \times N$ image, and then, the formula of two-dimensional DCT transform is given as follows:

$$F(u,v) = \frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{M-1} f(x,y) \quad (u,v=0) \tag{4}$$

$$F(u,v) = \frac{2}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{M-1} f(x,y)\ \cos\left[\frac{\pi}{2N}(2y+1)v\right] \quad (u,v=1,2,\ldots,N-1). \tag{5}$$

Among them, $F(u,v)$ means the high-frequency portion of transform domain based on a DCT image digital watermarking, and $F(0, 0)$ means the low-frequency portion of transform domain based on a DCT image digital watermarking;

The original image can be restored by two-dimensional DCT inverse transform. The formula of two-dimensional DCT inverse transform is given as follows:

$$\begin{aligned} F(x,y) = {} & \frac{1}{N}F(0,0) + \frac{2}{\sqrt{N}}\sum_{x=1}^{N-1} F(u,0)\cos\left[\frac{\pi}{2N}(2x+1)u\right] \\ & + \frac{2}{\sqrt{N}}\sum_{y=1}^{N-1} F(0,v)\cos\left[\frac{\pi}{\sqrt{2N}}(2y+1)v\right] \\ & + \frac{2}{N}\sum_{x=1}^{N-1}\sum_{y=1}^{N-1} F(u,v)\cos\left[\frac{\pi}{2N}(2x+1)u\right]\cos\left[\frac{\pi}{2N}(2y+1)v\right] \\ & (u,v=1,2,\ldots,N-1) \end{aligned} \tag{6}$$

After two-dimensional DCT transform, most of the energy information about images focuses on middle-frequency and low-frequency coefficients. The watermark embedded in the domain of low-frequency coefficients has good robustness. While the watermark embedded in the domain of high-frequency coefficients has good imperceptibility but may has the data lost when processing the images. Taken together, the watermark embedded in the domain of high-frequency coefficients is usually not considered. Instead as a compromise, the domain of middle frequency and low frequency is regarded as coefficient of embedment.

DCT transform converts in blocks. The size of the blocks can be flexibly determined, and we usually choose the size of 8×8. The whole image can be treated as a block to perform DCT transform, and it too may be considered as different word blocks (divided from the whole image) to perform DCT transform independently. Positive DCT transform decomposes images into spatial frequency. The type of frequency-domain coefficients represents the proportion of the frequency components in the original image.

Compared with the algorithm in space domain, the algorithm in transform domain has the following advantages:

- The embedded watermark signal in transform domain can be distributed to all pixels of the spatial domain and is favourable to ensuring invisibility of the watermark.
- In transform domain, some characteristics of the human visual system can be more easily coupled to the watermark embedding process.
- The method of transform domain can make compatible with the image compression standard of international mainstream (e.g., JPEG), thus achieving watermark embedding on compressed domain.
- Generally, the method of transform domain has very good robustness. Large number of bits can be embedded in the frequency domain of the image without causing visual degradation.
- This algorithm has the anti-attack ability for image compression the popular image filtering and noise. So it is very suitable for copyright protection of digital works.

From this, digital watermarking in transform domain is the main technological measures applied to protect the copyright of museum numeral works.

5 Experiment and Results

The digital exhibits in the digital museum are digital project of various mediums' information such as picture, video, and vector animation. To protect the copyright and the integrity of the digital exhibits in the digital museum, a variety of digital watermarking technologies should be applied comprehensively.

In the digitized data of our project, the main format is plentiful JPEG image and Flash animation generated by the panorama. In safety program of this project, the protection of the digital exhibits in the digital museum is mainly the watermarking technology for the data in the two style, they are JPE image digital watermarking and Flash animation digital watermarking. And MATLAB is selected as the simulation platform to operate digital watermark operation on the digital exhibits.

5.1 JPEG Color Image Watermark Algorithm

In MATLAB, JPEG color image is taken as an index image or a RGB image. A single RGB image can be thought of as three gray images of three component images called red, green, and blue, respectively. According to the human visual system theorem, the human eye reacts differently to the three colors, the green component image is the clearest, and the preserving image detail is the best. Therefore, in this safety program, we choose to embed the green component image in watermark. Before adding watermark to color image, we need to extract three component images via the channel splitting technique [7, 8].

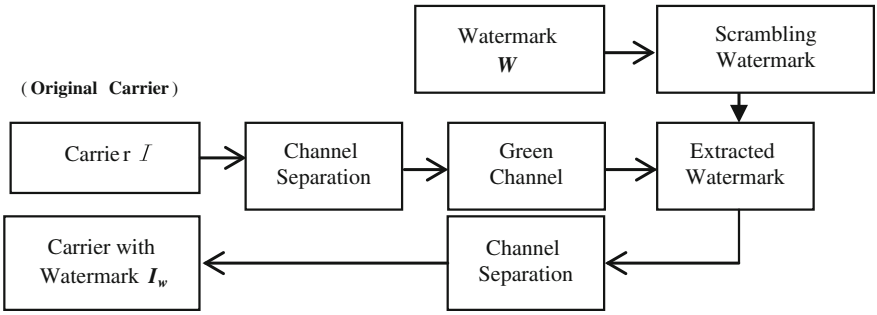

Fig. 4 Embedding process of color image digital watermark

6 Image Watermarking Embedding Algorithm

The process is illustrated in Fig. 4. During the embedding process of the watermark based on DCT transform domain algorithm. First, isolate the green component image from the original carrier image by using the channel splitting technique and then chunk this component image in the size of 8×8. Finally, perform the DCT transform. On account of focusing a great deal of energy in the low frequency by DCT transform, this DCT transform domain algorithm has a good robustness. But micro-chunking makes this advantage less obvious. At the same time considering the factors such as loss compression, we adopt the 8×8 block DCT transform.

7 Image Watermarking Extracting Algorithm

The process is illustrated in Fig. 5. When extracting the watermark, we need the participation of the original image. That is why we call it non-blind watermarking algorithm.

8 Algorithm Implementation and Results

The results of watermark embedding are shown in Figs. 6 and 7.

The results of watermark extracting are shown in Figs. 8 and 9.

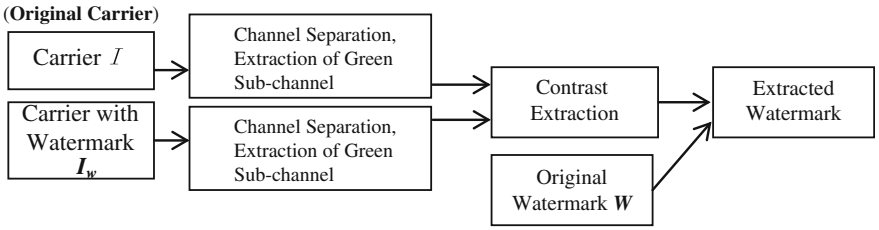

Fig. 5 Extracting process of color image digital watermark

Fig. 6 Original image

Fig. 7 Watermarked image

Fig. 8 Original watermark

Fig. 9 Extracted watermark

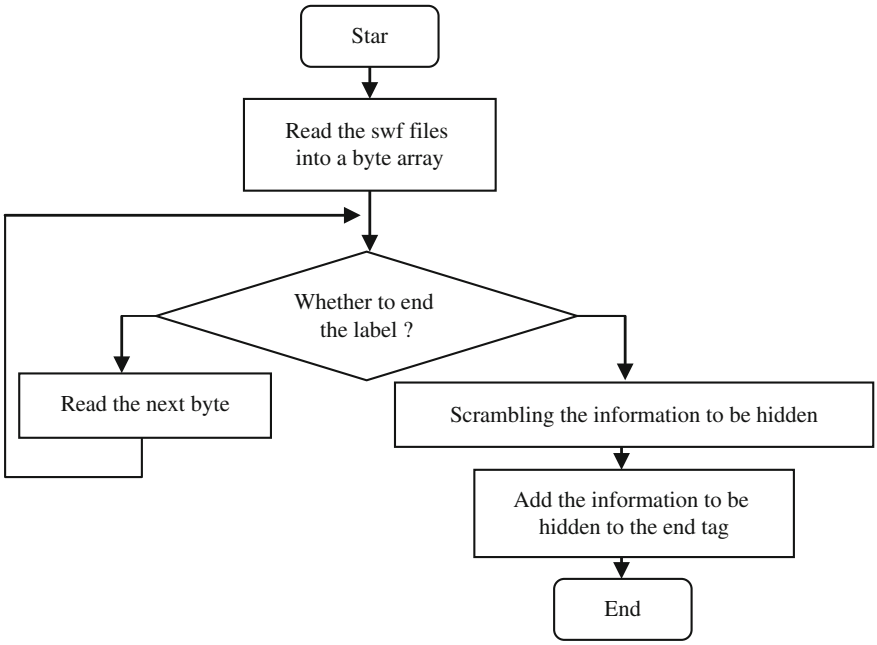

Fig. 10 The flow diagram of *swf* file information hiding

8.1 The SWF Animation Information Hiding Algorithm

Traditional methods of protecting Flash file include embedding hidden information, encrypting, and generating its exe file. These methods are unfavorahie for protecting the copyright of Flash file. While in the digital museum, the main purpose of protecting Flash file is to prevent copyright violations. Therefore, this chapter chooses the meaningful logo image information hiding technique as the topic and aims to protect its copyright and integrity.

The basic principle of the information hiding algorithm for swf animation files is that embed the hiding information in swf files through the analysis of swf file format. e.g., hiding information in the label, hiding information in the frame of the animation, hiding information by adding additional labels after the closing tag, replacing the object properties. In this chapter, we select the information hiding algorithm in which watermark image can be added after the end tag of the Flash animation to protect the Flash exhibits in digital exhibits. The player can ignore the content following the end tag; thus, the Flash animation can work well [9–13].

Watermark embedding and extraction block diagram is shown in Fig. 10, wherein the hidden information extraction process is the inverse of the information hiding.

The results of embedding hidden information of Flash animation are shown in Fig. 11.

(Extract hidden formation)

Fig. 11 Embedding hidden information of Flash animation

9 Conclusion

Experimental results show that the digital image invisible watermarking method based on the DTC domain, which is applied to encrypt digital image in the digital museum, has some distinguishing features, such as simplicity and convenience, less original image distortion, and high anti-attack. For this reason, it can protect the copyright of the digital image effectively. The Flash animation embedded in logo information image can work well. When a copyright dispute rises, it can prove and protect the copyright via extracting the hidden information. This method can be taken as reference by other industries to address the copyright of digital image.

In this study, a security digital museum copyright protection method is proposed. It is efficient for the safety management of digitalized media in the digital museum. But this method still has many could be further improved and perfected. In our digital museum, the exhibits are presented in various types, but in this security scheme, we only consider two the largest and the most important types. In further studies, various types of exhibits should be taken into consideration and require further study. Only then, it was possible to ensure the safety of the entire system.

Acknowledgments This study was supported by the Hainan Natural Science Foundation (No: 612120, 612126), the key Science and Technology Projects of Haikou City in 2010(No: 2012-017), and disciplines project of Hainan Normal University. The authors expressed their thanks together.

References

1. Zhao, X., Hao, L.: The digital watermarking summary. Comput. Eng. Des. 81–85 (2010)
2. Zong, Y.: Digital watermarking technology in digital Museum. Southeast Cult. 81–85 (2010)
3. Cao, LG., Chen, H., Cao, P.: Research on copyright protection of digital museum based on digital watermarking technology. **22**(4), 162–165 (2005)
4. Sun, SH., Lu, ZM., Niao, XM.: Digital Watermarking Technology and Application, pp. 205–207. The Science Press (2004)
5. Junling, Z.: DCT Digital Watermarking-Based Research, pp. 35–39 (2009)
6. Zhang, X., Peiliang, C.: Scrambling technology in digital watermarking. J. Circ. Syst. **6**(3), 32–36 (2001)

7. Kang, Y., Hui, X., Shi, J.: Multimedia data watermarking system and its attack. Comput. Sci. **26** (10), 44–48 (1999)
8. Fu, J.: Static image watermarking algorithm based on DCT domain. **4** (2007)
9. Zhang, X., Zhang, X.: Information hiding algorithm based flash animation. Comput. Eng. **36**(1), 181–183 (2010)
10. Dai, M.: Vector animation file data structure analysis. Jiamusi Educ. Inst. **10**, 413–414 (2012)
11. Shi, R., Qinmao, L., Liu, H.: Vector digital watermarking technology. J. Comput. Appl. **24**(8), 22–24 (2007)
12. Ding, L.: Vector digital watermarking technology research. **6** (2010)
13. Chen, Y.: MATLAB 6 the X graphical programming and the image processing. Xi'an University of Electronic Science and Technology Press (2002)