Watermark in color image

Ren-Junn Hwang, Chuan-Ho Kao and Rong-Chi Chang
Department of Computer Science and Information Engineering, TamKang University,
Tamsui, Taipei, 251, Taiwan, R.O.C.
victor@mail.tku.edu.tw, chk64@ms17.hinet.net, roger@mail.mine.tku.edu.tw

Abstract

There are more and more productions to be saved as digital form. In digital world, we can keep the production will not going off forever. But it also has some disadvantages that people can do a copy very easily. Watermark is an important protection method in digital media nowadays. When one media was public or put on the network, it is very easy to be copied or misappropriated. The author can prove he own the media by use open algorithm and security key to extract the watermark. So one watermark technique must resist some attacks and cannot influence the quality of image. It is usually used to embed watermark in spatial domain and frequency domain. Each of them has specialized skills. In this paper, we propose an image watermark technique based on spatial domain in color image. We have some experimental results in this paper. It can prove our method can resist some attack.

Key words: digital watermark, spatial domain.

1. Introduction

There are very various watermark techniques to adapt various digital media. We can use very kind of watermark, like one message or a logo or a trademark. We select different watermark and technique according to media and the state of environment. The image which we select want to embed watermark is called stego-image. The stego-image is an original image that does not do any change. The image, is called cover-image, was embedded data or information into image.

In watermark topic, there are two major research aspects. One aspect is using spatial domain, they change the pixels value directly. It is like LSB(Least Significant Bit) method, people can change all the least bit in each pixel value to embed their information. [1,3,6] The advantage of the aspect of spatial domain is it can contain bigger capacity. Thus, this method adapts big size media. Besides, we usually can embed and extract watermark easily and quickly. But the robustness of watermark is often weaker than the technique of frequency domain. The other command spatial domain methods include Kutter's method [4].

The other aspect is based on frequency domain. [2] The method will change pixel value to frequency and employ the feature of frequency to embed data. For example, people often embedded their watermark on the image based on a JPEG model. First, they will cut the image as 8*8 non-overlapping blocks. Then uses the discrete cosine transformer (DCT) to transform each block. Final, they will use quantization table to scale the DCT

Proceedings of the First International Symposium on Cyber Worlds (CW'02)
0-7695-1862-1/02 $17.00 © 2002 IEEE

coefficients. After it, people can embed their watermark to these coefficients. People often embed their watermark into the middle frequency components. It is because the robustness of watermark is weakly in the higher frequency components. In lower frequency, it will reduce more quality of image. In spatial domain, it can resist more attack and raise the robustness. The common methods are based on discrete cosine transformation and discrete wavelet transformation.

Although computer science technique is developing fast and deep, we hope to solve problem easily. In this paper, we propose a method based on spatial domain. We will explain the embedding and extraction method in chapter 2. In chapter 3, we will do some experiments and show the result. The conclusion is in the chapter 4.

2. The embedding and extraction method

The cover image C is a 24-bit true color image. Then, we calculate the saturation of each pixel as our embedding location. It is because in one color image, human visual system cannot detect the few difference in saturation. The transform equation is in Equation 1. [5] The size of cover image is m×n. The data D, which is embedded in C, is x×y monochrome image.

$$C = \{c_{ij} \mid 0 \leqq i < m, \quad 0 \leqq j < n, c_{ij} \in [0, 100] \}, \tag{1}$$

$$D = \{d_{ij} \mid 0 \leqq i < \mathrm{x}, \quad 0 \leqq j < \mathrm{y}, d_{ij} \in [0, 1] \} \tag{2}$$

It is the embedding step as follow:

Step-E1: Randomly select one number S.

Step-E2: Generate one string different numbers named A = { a_1, a_2, …, $a_{m\times n}$ } based on the seed S. Each value a_i ranges between 1 and $m\times n$. For any two different integer numbers $a_{i,}$ and a_j in A, and their neighbor eight pixels should not be overlap. In other words, $a_{i,}$ and a_j block are different.

Step-E3: Compute the average of nine pixels value of a_i block in A. Then, we sort this nine pixels value and compute the average of minimum five pixels value Min_{ave} and maximum four pixels value Max_{ave}. Calculate the difference of Min_{ave} and Max_{ave}. According to the value of each d_i bit, we alter some pixels in C as the following steps. C' is the stego-image embedded the data D in C.

Step-E4: Decide a threshold value t. If the embedded data d_i is 0, then add the Min_{ave} and reduce the Max_{ave} until the difference of Min_{ave} and Max_{ave} is close to zero. If the embedded data d_i is 1, then reduce the Min_{ave} and add the Max_{ave} until the difference of Min_{ave} and Max_{ave} is bigger than $2t$.

Step-E5: Stego-image C' is the image generated by Step-E4.

Step-E6: Collect the Randomly selected number S as key to extract the watermark.

It is the extract embedding step as follow:

$$C' = \{ c'_{ij} \mid 0 \leqq i < m , 0 \leqq j < n , \quad c'_{ij} \in [0, 100] \} \tag{3}$$

Step-D1: Generate the set A based on the seed S as Step-E2.

Step-D2: Extract each bit d_i based on its correspondence value a_i as the following steps.

Step-D3: If the difference of Min_{ave} and Max_{ave} is bigger than the threshold t, then the extract data $d'_i = 1$, otherwise $d'_i = 2$.

Step-D4: Integrate all the bits d'_i extracted by Step-D3, and make up the embedded data D'.

3. Experimental Results

This section shows the experimental results. In our experiment, we did a homemade logo as watermark, shown in Figure 1. It contains 16900 bytes. We select Lena, F16 and Pepper as the cover images. They are 24-bit true color 512×512 pixels images. In experimental process, we select 1.3 as the threshold value t in Step-E4. The stego images, shown in Figure 2, which is embedded watermark.

We use the PSNR (Peak Signal to Noise Ratio) value to evaluate the quality of image by our method. It is a popular method to evaluate the difference between the decompressed image and its original image.

$$\mathrm{MSE} = \left(\frac{1}{m \times n}\right) \sum_{i=0}^{i<n} \sum_{j=0}^{j<m} (c'_{ij} - c_{ij})^2, \qquad (4)$$

$$\mathrm{PSNR} = 10 \log_{10} \frac{255^2}{\mathrm{MSE}} \mathrm{dB},$$

All the images which be embedded data are upper than 40dB.

In robustness experiment, we did the some attacks to test the watermark robustness. The attacks is include scale, JPEG compression, smooth, cropping and noise. The results are in Figure 3.

4. Conclusion

In this paper, we proposed a watermark technique based on spatial domain in color image. We embed watermark in saturation on the HSI space. It is easy to embed and cannot be detect easily. It can save the high quality with image. Besides, it can resist some attacks. We hope we can raise watermark robustness that watermark can resist more strong attack, like geometry attack and stirMark.

5. Reference

[1] BENDER, W., GRUHL D., MORIMOTO, N. and LU, A.: "Techniques for data hiding", IBM System Journal, 1996, 35(3&4), pp. 313-336.

[2] Chiou-Ting Hsu and Ja-Ling Wu, “Hidden Digital Watermarks in images”, IEEE Transactions on Image Processing, Vol. 8, No 1, January 1999, pp.58-68.

[3] J.C. Liu and S.Y. Chen, “Fast two-layer image watermarking without resorting to original image and watermark ”, Proc. of joint Conference of International computer Symposium, pp. 231-238, Taiwan, Republic of China, 2000.

[4] Martin Kutter, Frederic Jordan, and Frank Bossen, “Digital Signature of Color Images using Amplitude Modulation”, J. Electron. Imaging 7(2), April 1998, pp. 326-332.

[5] Timothy K. Shih, Ching-Sheng Wang, and Chuan-Ho Kao, “An Intelligent Content-based Image Retrieval System based on Color, Shape and Spatial Relations”, Proceedings of the National Science Council, ROC, Part A: Physical Science and Engineering, Vol. 25. No. 3, May 2001.

[6] Yeuan-Kuen Lee and Ling-Hwei Chen, “An Adaptive Image Steganographic Model Based on Minimum-Error Replacement”, Proceedings of the Ninth National Conference on Information Security, May. 14-15, 1999, Taichung, Taiwan, pp. 8-15.

$$H = \arctan 2(\sqrt{3}(G-B),(2R-G-B))$$

$$S = 1 - \frac{\min(R,G,B)}{I}$$

$$I = \frac{(\mathrm{R}+\mathrm{G}+\mathrm{B})}{3}$$

Equation 1: The Calculate of Saturation Equation(R、G、B is the value of red, green and blue color in bitmap image. H、S、I is the value of Hue、saturation and illumination transform from R、G、B)

Figure 1: watermark logo

(a) PSNR: 43.45 (b) PSNR: 47.92 (c) PSNR: 48.07

Figure 2: stego image

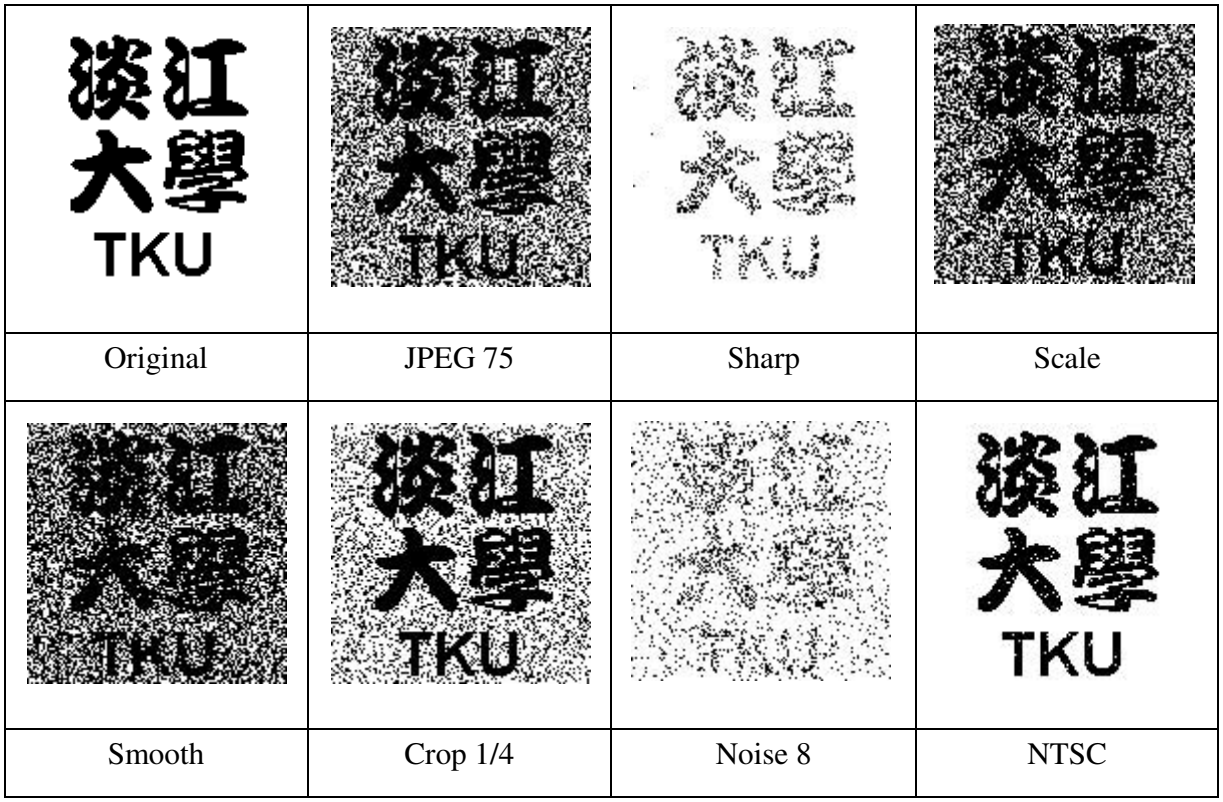

Figure 3: The result as stego image be attacked by various destroy