Jestr Journal of Engineering Science and Technology Review 6 (2) (2013) 139-144

Research Article

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

An Improved Watermarking Algorithm to Colour Image Based on Wavelet Domain

Yinglan Fang*, Lin Tian and Bing Han

Department of Computer, North China University of Technology, Beijing, China

Received 15 May 2013; Accepted 25 July 2013

Abstract

This paper has brought forward an improved non-blind watermarking algorithm based on discrete wavelet transform. Watermarking applies special meaningful color image. Before embedded watermark, the algorithm requires needs the watermarking image and carrier image to separate color and transform discrete wavelet. Then the watermark's low frequency sub-graph and high low sub-graph are respectively embedded into carrier image using additive watermark embedding rules and iterative mixed method. The experiment results have showed that the algorithm has good concealment and improve the robustness of the algorithm.

Keywords: Colour Separation, Iteration, Mixture, Discrete Wavelet Transform

1. Introduction

In recent years, with the rapid development of multimedia and network technology, people can quickly and easily communicated the digital information to world with using variety of electronic devices such as computers, digital scanners, printers and so on. But it also makes for multimedia illegal copying of digital products, forgery and tampering with increasing, which greatly damaged the product owner's copyright and commercial interests. So digital media has brought us convenience, but also it gives us a safety hazard. Therefore the copyright protection problem of digital media has become one of the hot spot in current research. As an emerging information security technology, digital watermarking technology has brought out a new solution to improve multimedia information security and has become a hot research topic in the information security fields, many countries have carried out extensive and in-depth study to it. Digital watermarking as effective supplementary mean of traditional encryption method, it may provide for the resolution of this issue [1], [2]. Now the majority of the digital watermarking algorithm is mainly considered how to embed watermarking in gray image, but in practical applications, the color images occupy a major position, Therefore, the study of the color image digital watermarking technology has more realistic significance. In addition, the color image as the watermark can contain a wealth of information [3]. Therefore, this paper will make double color image watermarking as an entry point to research the existing various algorithms and combines with the inherent characteristics of color images, it design a double color image watermarking algorithm. The study of this technology has especially practical significance in the rapid development multimedia and network technology.

2. Related Technology

2.1 Image Scrambling Technology

Image scrambling technology is a type of technology which belongs to watermark pretreatment, its purpose is to improve the security of the watermark. And image scrambling transformation must be reversible transformation. Otherwise the scrambling transformation will make no any sense in the actual process [4]. To guarantee the security of the watermarking, the watermark image embedded into the carrier image scrambling is required prior to processing. Through the process of scrambling, it can take a watermark image become disorganized. In other words, to some extent the scrambling image is a serious distortion, but after the corresponding inverse transform, it will be restored to the original image. So only people who know the scrambling algorithms and the key can take extract the watermark into the original watermark image. Thus it enhances the security of the watermarking.

Image scrambling [5] refers to the pixels spatial location of the image to a new arrangement, but the total number of pixels and the histogram is same, so the image scrambling is a mapping of two-dimensional space. Any reversible mapping can be used to image scrambling. At present the commonly used scrambling method are Arnold transformation, magic transformation, curve transformation based on the Hilbert, affine transformation and generalized Gray code transformation, etc.

This paper algorithm uses the Arnold transform to scramble color watermark image, it is a kind of transformation put forward by V.J.Arnold in the study of the theory, also known as Cat face transform (Cat Mapping). Assumes that the watermark image pixel coordinates x, y $\in$ {0, 1, 2, .., N - 1}, then Arnold transform as:

* E-mail address: jlufangyl@163.com

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{ (mod N)} \quad (1)$$

Where, the[x', y']T is pixel point coordinates of watermarking image after Arnold transform and N is the order number of image matrix.

Using equation (1) one by one to transform the pixel coordinates of color watermarking image. When throughout all the pixels of the image point s , it will produce a "new" color watermark image. However due to the discrete digital image is a finite set of points, the image is repeated to Arnold transform, when iterative steps to a certain number steps, it will restore the original image, namely Arnold transform is periodic. Assume that "chaotic" color watermark is obtained after its k time iterations, and k can be assumed as the key to save.

2.2 Discrete Wavelet Transform (DWT)

Wavelet transform is a great breakthrough of the well-known Fourier transform and window Fourier transform. It is not only inherit and develop localized ideas of the short-time Fourier transform, but also overcomes the window size which is not vary with frequency and the lack of discrete orthogonal basis. It is an ideal signal analysis tools.

Wavelet is namely the small are wave. It is a special limited length waveform with an average of 0. It has two characteristics: First is "small", that it has compact support or similar compact support in the time domain. Second is alternating positive and negative "volatile", which the DC component is zero.

Discrete wavelet is a continuous discrete wavelet. Assumes that the wavelet transform for any function x(t) is W(a,b) , where a and b are the scale factor , $\varphi_{a,b}(t)$ is the wavelet basis function, now a, b, t can be discredited, a=2j, (j>0, j∈Z),b=KTs2j; Ts is the sampling interval time. So Wavelet function can be expressed as $\varphi_{j,k}(t) = 2^{-j/2}\varphi(2^{-j} - k)$, the discrete wavelet transform of any function x(t) is $WT_x(j,k) = \int x(t) \cdot \varphi_{j,k}(t)dt$.

Multi-resolution analysis image based on wavelet decomposition can be effectively time-frequency decomposed. Image after wavelet decomposition level can be divided into four sub-graphs. Respectively it is the low frequency sub-graph and a horizontal direction, the vertical direction and in the diagonal direction high-frequency sub-graph. The secondary decomposition of the low frequency sub-graph is further decomposed into four sub-graphs. Fig. 1 and Fig. 2 are respectively the decomposition diagrams of the original image after decomposition of one level and three levels.

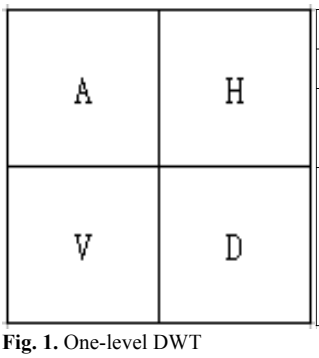

Fig. 1. One-level DWT

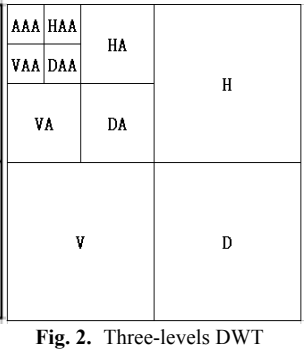

Fig. 2. Three-levels DWT

2.3 Digital Watermarking Performance Evaluation

Generally, the extracted watermark information will not be complete the same to the embedding watermark information. It will bring the watermark information assessment question to the watermarking system extraction. This needs the relevant assessment criteria to judge. The digital watermarking evaluation criterion [5] mainly includes two sides: concealment and robustness. Both of which are generally conflicting and mutual restraint. The robustness of watermarking is influenced by the watermark embedding amount, embedding strength and watermarking image size. Usually, the watermarking amount is more, the watermarking strength is greater, the robustness is better, but the concealment is less. On the contrary, when the watermark meets the high requirements of concealment, it will sacrifice robustness of the watermark and the watermark embedding capacity. As a result, we should consider both tradeoffs when designing a watermarking algorithm.

Concealment is an important evaluation standard to judge watermarking algorithm. In order to objectively and fairly evaluate the watermark algorithm, it must use effective visual image distortion measurement criteria to measure the quality differences between the original image and watermark image. Currently, the widely used quasi-image visual distortion is the peak signal noise ratio.

Robustness is referred to the capability of detecting the watermark after routine operation (such as filtering and noise and rotation and scaling and cut and etc) to digital watermarking algorithm. It is the most basic and most important characteristic of the digital watermarking technology. The robustness of measuring digital watermarking algorithm can be normalized correlation coefficient NC.

1) Peak Signal to Noise Ratio, PSNR[1-5]. It evaluates the difference between the watermarked image and the original image. It measures the ability to embed watermark, its value is higher, the watermark concealment is better. Assume that I represent the original image and I' represents the watermarked image, the PSNR formula is:

$$MSE = \frac{1}{MN}\sum_{i=1}^{i=M}\sum_{j=1}^{j=N}(I(i,j) - I^{\sim}(i,j))^2 \quad (2)$$

$$PSNR = 10 \times \lg(\frac{255^2}{MSE}) \quad (3)$$

Where, MSE is the mean square error.

2) Normalized Correlation [5] (NC). It can be used to calculate the similarity between the extracted watermark image and the original watermark image. The value of NC is larger, the extracted watermark and the original watermark is more similar. When W represents an original color watermark, W~ represents then extracted color watermark, then the formula for NC is calculated as

$$NC = \frac{\sum_{i=1}^{i=M}\sum_{j=1}^{j=M} W(i,j)W^{\sim}(i,j)}{\sum_{i=i}^{i=M}\sum_{j=1}^{j=M} W(i,j)^2} \quad (4)$$

3. Improved Algorithm Form

3.1 Improved Algorithm Design Idea

In references [6], that algorithm take all sub-graph of color watermarking after DWT embedded into carrier image using additive watermark embedding rules. It has met the basic requirements of watermarking algorithm. This paper algorithm has improved the algorithm based on references [6]. First, the low frequency sub-graph of watermarking is embedded into carrier image low frequency sub-graph using additive watermark embedding rules as references [6]. And the high frequency sub-graph of the watermarking is embedded into carrier image middle frequency sub-graph using iterative and mixed method as references [3]. Thus multiple iteration parameters can be selected in the iteration process. It not only improves the security of the watermark, but also it improves the mix proportion of watermark image in the iterative process and so as it improves the anti-attack ability of the watermark. .

3.2 Wavelet Base Choice

Because different wavelet basis has a different property, so watermark based on different wavelet basis, its robustness will vary. When DWT domain watermarking algorithm is designed, the first problem encountered is the use of which wavelet basis. It should select the wavelet basis according to watermark robustness influenced by the wavelet itself characteristic, such as regularity, vanishing moments, supporting length and wavelet image energy in the degree of concentration of the low frequency sub-graph. After calculation and experiment, we chose the Haar wavelet in Daubechies wavelet coefficients because it is a only discontinuous discrete wavelet and the only one strictly orthogonal wavelets in Daubechies wavelet. And the Haar wavelet supporting length is shortest and its decomposition and reconstruction coefficient complex is lower than other wavelet, so it can effectively overcome the rounding error problem which commonly existing in transform domain watermarking algorithm [7], [8], [9]. Another reason which select Haar wavelet transform is that it removed the 3/4 of the amount of data, but retains 97% of the energy, which can ensure maximum low-frequency sub-graph based image efficiently reply and do not lose too much energy [10] .

3.3 Watermark Embedding Process

Assume that the original images is grayscale image I with size M×M, color watermark image is the binary and meaningful image W with size N×N. So the algorithm steps are as follows.

1) To determine whether the watermark is too big by the size of original image I and color watermark image W.

2) The three color components WR, WG, WB is gotten through separating the color watermark image W. The three color components have been encrypted by Arnold scrambling. And the scrambling number can be saved as a key, denoted by k1;

3) The three color scrambled components WR, WG, WB are decomposed by one-level DWT. Each color component could get four wavelets domain's sub-graphs (shown as Fig.4) with WR(G,B)A1 , WR(G,B)H1 , WR(G,B)V1 , WR(G,B)D1 .

4) We get three color components IR, IG, IB through the color separation of the carrier image I. The three color components IR, IG, IB are decomposed by three levels DWT. Each color component could get ten wavelet domain's sub-graphs (shown as Fig.2).

5) The high frequency sub-graph (horizontal direction, vertical direction, diagonal direction) and low frequency sub-graph of color watermark are embedded into original carrier image. The specific process is as follows.

a) Using the iterative and mixed method as references [3], it takes the high frequency sub-graph $W_{R(G,B)}H_1$, $W_{R(G,B)}V_1$, $W_{R(G,B)}D_1$ of the color watermarking embedded into mediate frequency sub-graph $I_{R(G,B)}H_3$, $I_{R(G,B)}V_3$, $I_{R(G,B)}D_3$ of carrier image. The horizontal direction as an example (vertical direction and diagonal direction is similar):

$$\begin{cases} S1_{R(G,B)} = \alpha_1 \times I_{R(G,B)}H_3 + (1-\alpha_1) \times W_{R(G,B)}H_1 \\ S2_{R(G,B)} = \alpha_2 \times I_{R(G,B)}H_3 + (1-\alpha_2) \times_1 S1_{R(G,B)} \\ \tilde{I}_{R(G,B)}H_3 = \alpha_3 \times I_{R(G,B)}H_3 + (1-\alpha_3) \times S2_{R(G,B)} \end{cases} \quad (5)$$

Where, $\{\alpha_i \mid 0 < \alpha_i < 1, i = 1,2,3\}$;

b) The high frequency sub-graph $W_{R(G,B)}A_1$ of color watermarking is embedded into high frequency $I_{R(G,B)}A_3$ of carrier image using additive watermark embedding rules as references [6].

$$\tilde{I}R(G,B)A_3 = I_{R(G,B)}A_3 + \omega \times W_{R(G,B)}A_1 \quad (6)$$

Where, ω is as the embedding strength, its range is $0 < \omega < 1$

4. Experiment Results and Analysis

The above algorithm is programmed based on MATLAB. It selects 512×512 pixel color image Lena as a carrier image and 128×128 pixel color school badge as a watermark.

4.1 Non-attack Environment

The experiment in non-attack environmental result is as the follow for Fig. 3 to Fig. 6.

Fig. 3. The original image

Fig. 4. Watermarked image

Fig. 5. Watermark image

Fig. 6. Extracted watermark image

From a subjective point of view, the experiments show that whether the overall effect of the image or the local details contrast, the original image and the watermarked image is basically same. Namely after embedding watermark, the image can still maintain a good visual effect. From an objective point of view, the watermarked image and the original image's PSNR equals to 33.5788, extracted watermark image and the original watermark image's NC equals to 0.9869, it shows that the algorithm has better concealment.

4.2 Various attack environment

In order to detect robustness of the algorithm, we have attacked the watermarked image (c). Where we only consider those distortion methods that are not serious cause image such as noise attack, filtering attacks, geometric attacks (scaling, rotation, cut), JPEG compression attack. The watermark image is judged after attacked image.

1) Noise Attack

Fig. 7. Gaussian Noise (aver=0, ver=0.001NC =0.9036)

Fig. 8. Salt and Pepper Noise (density=0.001 NC =0.9819)

2) Filtering Attack

Fig. 9. Median Filtering Image NC=0.9329

Fig. 10. Wiener Filtering Image NC=0.9290

3) Geometric Attack

Fig. 11. 20° Counterclockwise Rotation NC=0.8420

Fig. 12. 40° Counterclockwise Rotation NC=0.7915

Fig. 13. Cut 1/4 NC=0.7349

Fig. 14. Cut 1/2 NC=0. 0.4873

Fig. 15. Narrow 0.5 Times NC=0.9497

Fig. 16. Expand 2 Times NC==0.9776

4) JPEG Compression Attack

Fig. 17. Quality =90% NC=0.9869

Fig. 18. Quality =60% N=C0.9358

Fig. 19. Quality =30% NC=0.8538

From attack test results can be seen that the watermark image by noise attack, filter attack and after JPEG compression attack gotten by the algorithm in this paper. Similarity NC value of the extracted watermark and the original watermark is some 0.9 value. So that the algorithm has better robustness, but the anti-geometric attack is relatively poor. This is because the wavelet transform has no rotation, translation and scaling invariance.

4.3 Comparison Result of Different algorithm

This paper algorithm is compared with the algorithm in references [6]

Table. 1 Objective data after embedding watermark

Objective Data	This paper algorithm	Ref. Algorithm
PSNR	33.5788	34.0146
NC	0.9869	0.9273

Table. 2 NC of extracted watermark by different attack

Attack Name	This paper algorithm	Ref. Algorithm
Gaussian Noise	0.9036	0.8477
Salt and Pepper Noise	0.9819	0.9219
Median Filtering	0.9329	0.8910
Resizing（ 50%）	0.9487	0.8818
70% JPEG Compression	0.9441	0.8583

It can be seen from the comparison of the data, This paper algorithm meets the requirements of concealment and robustness of watermarked image better than the algorithm in the references [6].

5. Conclusions

This algorithm puts forward an improved application algorithm based on the wavelet domain with digital image watermark technology. Using color image as a watermark, the watermark can carry more and clear copyright information, so it has more practical value. First, the algorithm uses Arnold scrambling to preprocess watermark image, which makes the watermark information to be protected by encryption. After watermarked, images maintain good visual effects. It not only completely meets the requirements of the watermark concealment, but also shows a strong robustness to resist common watermarking attacks.

Acknowledgment

The work in this paper has been supported by Natural Science Foundation of China (Grand NO: 61070030, 61111130121)and the British Royal Society of Edinburgh (RSE-Napier E4161). It is also partly supported by Beijing Government and Education Committee (Grant No. PHR201107107).

References

1. Cox I J, Kilian J,Leighton T and Shamoon T. Secure spread spectrum watermarking for images, Audio and Video [J]. In Proceedings of ICIP, Switzerland, 1996, No.3, pp.243-246
2. Cox I J, Kilian J, Leighton T, et al. Secure Spread Spectrum Watermarking for Multimedia [J]. IEEE Trans. on Image Processing, 1997, 6 (12): pp.1673-1687
3. Guicang Zhang, Rangding Wang, YuJin Zhang. Image hiding technology based on iterative mixed digital [J].Journal of Computers. 2003,26(5): pp.567-574
4. Lina Wang,Chi Guo,Peng Li. Information Hiding Technology Experiment tutorial [M].WuHan:Wuhan University Press,2004
5. Cong Jin. Digital watermarking theory and technology [M].BeiJing: Tsinghua University Press,2007
6. Xiankun Zhu. Based on double color image of wavelet domain digital watermarking algorithm [D].XiAn: Northwest Normal University,2009
7. JiuFen Liu. DaRen Huang,JunQuan Hu. Orthogonal wavelet bases of digital watermarking [J].BeiJing: Electronics and Information Technology, 2003,25(04): pp.453-459
8. YingYing Ding,Zhen Liu. Analysis and Comparison of Three Kinds of Frequency Domain Digital Watermarking Algorithm [J]. ChongQing: Packaging Engineering,2011,No.5, pp.103-107
9. XiaoZhen Mi,Yu Che,HuaJun Dong. Study and Application of Digital Watermarking Algorithm Based on Discrete Wavelet Transform and Human Visual System [J].LiaoNing: Journal of Dalian Jiaotong University, 2012.Vol 33, No.1, pp.48-52
10. XinYue Fan,ZhiHeng He,Fei Zhou. Research on the double protection of Semi-blind color digital watermarking algorithm, [J]. ChongQing: Application Research of Computers, 2013. No 3, pp.917-920