Adaptive Watermarking Algorithm for Digital Image Based on Discrete Cosine Transform

Xinguo Zou[1]
1Department of Information Science and Technology, Shandong University of Political Science and Law, Jinan, PR China
e-mail:Xgjn08@163.com

Na Li[2]
2 Shandong Provincial Key Laboratory of computer Network, Shandong Computer Science Center, No19 Keyuan Road, Jinan, PR China
e-mail: lina@keylab.net

***Abstract.*--In this paper, an adaptive watermarking algorithm is proposed for digital image based on Discrete Cosine Transform. The algorithm uses the common resampling method (bilinear interpolation) to adaptively adjust the size of the binary watermark, and scrambles it via the encryption key, finally embeds it into the luminance component of the DCT intermediate frequency coefficients of digital image. Watermark detection does not require the original carrier image, that is, the detection is more convenient when digital image is posted and propagated on the Internet, by implementing a blind detection of hidden information. The experiments show that the algorithm has invisibility and strong robustness, effectively resisting noise adding, cropping, filtering, and other common attacks.**

Keywords: Watermarking, Digital Image, Discrete Cosine Transform

It is essential to protect the copyright of digital information (including image, audio and video) since they can be copy and stored so easy. With the development and prevalence of network and digital multimedia, people have paid more attention to digital watermark technology [1] as an efficient way of copyright protection. Watermark technology has been developed more than twenty years with many theories and algorithms proposed. It allows the embedding of a signature in a digital document in an imperceptible manner.

Current information hiding algorithm, due to the different position of the embedded watermark, is divided into two main streams: the spatial domain and transform domain [2,3]. Spatial domain method is relatively simple because of using arithmetic and logical operations on the original data to embed watermark. However these algorithms usually do not have the robustness against image translation, scaling, rotation, filtering and also are vulnerable to external noise. Transform domain method is strong resistance to attacks because of embedding watermark after data transformation, such as discrete cosine transform(DCT), wavelet transform, Fourier Transformation, etc. Thereinto watermarking technology in DCT domain has been widespread concerned because it is compatible with international compression standards and easy to implement via simple calculation [4].

Generally, the watermark should have several basic characteristics [5] as copyright logo, namely imperceptibility, robustness, provability, embedding capacity. Here embedding capacity has a great influence on the robustness of the watermarking algorithm. In theory, the larger the capacity, the anti-attack performance of the watermarking algorithm is stronger. Therefore, adaptive adjustment of the embedded watermark, depending on the size of digital image, can improve the robustness of the watermarking algorithm because people can take full advantage of the embedding capacity for digital image.

In this paper, we present an adaptive watermarking algorithm for digital image using bilinear interpolation and realize the blind detection. The algorithm uses the common resampling method (bilinear interpolation) to adaptively adjust the size of the binary watermark, scrambles it via the encryption key, and embeds it into the luminance component of the DCT intermediate frequency coefficients of digital image. The algorithm has the following characteristics: (1) it generate adaptive watermark based on the size of carrier image, so as to improve the robustness of binary watermark; (2) the watermark is embedded in the DCT coefficient of intermediate frequency, which can effectively resist common attacks, such as Gaussian noise-adding, salt and pepper noise-adding, cropping, Wiener filtering, JPEG compression;(3) the watermarking detection is simple and fast, and does not require digital image. The experiments show that the algorithm has good invisibility and strong robustness.

I. WATERMARKING PRE-PROCESSING

A. Adaptive generation of watermark

We use the image resampling method, bilinear interpolation, to adaptively generate binary watermark from the point of view of the image processing. The principle of bilinear interpolation is shown in Figure 1. Bilinear interpolation is an extension of linear interpolation for interpolating functions of two variables (e.g. x and y) on a regular 2D grid. The interpolated function should not use the term of x 2or y 2, but xy. The key idea is to perform linear interpolation first in one direction, and then again in the other direction. Although each step is linear in the sampled values and in the position, the interpolation as a whole is not linear but rather quadratic in the sample location.

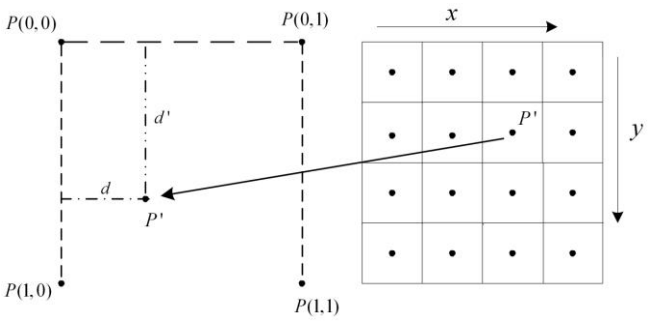

Figure 1. Idea of bilinear interpolation.

Suppose that we want to find the value at the point $P'(x, y)$. It is assumed that we know the values at the four points $P(0,0)$, $P(0,1)$, $P(1,0)$, $P(1,1)$. So the bilinear interpolation is performed by the following equation:

$$P'(x, y) = P(0,0)\cdot(1-d)\cdot(1-d') + P(0,1)\cdot d\cdot(1-d') + P(1,0)\cdot d'\cdot(1-d) + P(1,1)\cdot d\cdot d' \quad (1)$$

For any binary image watermark, which can be seen as a template, the adaptive adjustment of the size can make the full use of embedding capacity and improve robustness, using the bilinear interpolation.

B. Arnold scrambling

Arnold's cat map is a chaotic map from the torus into itself, named after Vladimir Arnold, who demonstrated its effects in the 1960s using an image of a cat. One of this map's features is that image being apparently randomized by the transformation but returning to its original state after a number of steps periodically. The Arnold transform that is applied to every pixel in the image is given by the formula in matrix notation:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \left(\mathrm{mod} \quad N\right) \quad (2)$$

where $(x, y) \in \{0,1,2,\ldots,N-1\}$ are the pixel coordinates from original image and (x', y') are corresponding results after Arnold scrambling.

Arnold scrambling is applied to binary image, that is watermarking pretreatment, and randomized image is embedded as watermarking to produce watermarking image. When the watermarking is needed to be detected, Arnold scrambling can be used again to make the randomized watermarking return to its original state with periodicity. The number of steps in Arnold scrambling can enhance the security of algorithm. At the same time Arnold scrambling can make watermarking more strongly robust against cropping operation [6].

II. ALGORITHM DESIGN

A. Embedding algorithm

Watermark embedding algorithm has five steps hereinafter:

a)Assuming the digital image size is $M \times N$, the size of the binary watermark will be adjusted to $(N/8)\times(N/8)$ using bilinear interpolation if $M > N$. Then Arnold scrambling is implemented on the adjusted watermark. The number of iterations seems as the encryption key which only the copyright owner knows. The watermark after pre-processing is denoted as $W(i, j) \in \{0,1\}, i = 0,1,\ldots, M/8-1, j = 0,1,\ldots, N/8-1$.

b) We use random sequence generator to generate two two-dimensional pseudo-random sequences subject to uniform distribution, denoted as $k1, k2 \in \{0,1\}$. The size of each sequence is 3×3. It requires two sequences $k1, k2$ are not relevant or have a little correlation.

c)The human eye is least sensitive to the luminance component of digital image, compared with two other components chromaticity and saturation. Taking into account the invisibility of the watermarking algorithm, the watermark is embedded into the luminance component of the DCT coefficients of digital image.

d)DCT is implemented on two-dimensional image, block size of 8×8. Each DCT coefficient block is denoted as $D(u,v), u = 0,1,\ldots 7, v = 0,1,\ldots 7$, and modified one as $D'(u,v)$.We modify the DCT coefficient blocks in the lines *3 ~ 5* and the columns *3 ~ 5*, in accordance with the following formula:

$$D'(u,v) = \begin{cases} m(u,v) + \alpha * k1(u,v) & W(i, j) = 0 \\ m(u,v) + \alpha * k2(u,v) & W(i, j) = 1 \end{cases} \quad (3)$$

where $m(u,v)$ indicates the mean value of each DCT coefficient block in the lines *3 ~ 5* and the columns *3 ~ 5*. And α is the embedding depth factor, the value of a positive real constant.

e)The inverse DCT is applied to the luminance component of the watermarked blocks. Then we combine the watermarked luminance-component with other components of the original image to obtain a restored watermarked-image.

B. Detection algorithm

Watermark detection algorithm has three steps hereinafter:

a)DCT is implemented on the color image to be detected, block size of 8×8.

b)The DCT coefficient blocks in the lines *3 ~ 5* and the columns *3 ~ 5* is denoted as $D^*(u,v), u = 3,\ldots,5, v = 3,\ldots,5$. We calculate the correlation coefficient of $D^*(u,v)$ and $k1, k2$, which is denoted as $pk1, pk2$. If $pk1 > pk2$, then $W^*(i, j) = 0$, and if $pk1 < pk2$, then $W^*(i, j) = 1$. Here $W^*(i, j)$ is detected encrypt watermark.

c)We implement anti-Arnold scrambling on the detected encrypt watermark to get the final binary watermark extracted.

III. EXPERIMENT RESULTS

We select color image peppers (512×512 pixels) as digital image. The watermark is a binary image (32×32 pixels), shown in Figure 2 (a) (b). The watermark after Arnold scrambling is shown in Figure 2 (c). The pseudo random sequence $k1, k2$ is generated by the encrypt key. The correlation coefficient between $k1, k2$ is less than 0.5. The watermarking algorithm is tested respectively in the case of malicious attacks and no attacks.

In order to evaluate the quality of image, we calculate peak value signal-to-noise ratio (PSNR) with the formula:

$$PSNR = 10\log_{10}\frac{255^2}{\frac{1}{N\times N}\sum_{i=1}^{N}\sum_{j=1}^{N}[f(i,j)-f'(i,j)]^2} \quad (4)$$

where N is the size of image, $f(i,j), f'(i,j)$ is the pixel gray value of carrier image and pending detection image respectively [7]. The bigger the value of PSNR, the better the quality of pending detection image is. PSNR $\geqslant$ 48dB represents that the image quality is excellent, without noticeable changes. PSNR between 35dB~48dB represents good, and between 29dB~35dB belongs to the acceptable range. The critical point is 25dB. The image has generated an obvious interference when PSNR is below a critical value [8].

In order to evaluate the robustness of watermarking algorithm, the comparability between original watermark W and detected watermark W* is calculated with the formula hereinafter:

$$NC = \frac{\sum_i\sum_j W_{ij}\times W_{ij}^*}{\sum_i\sum_j W(i,j)^2}, i=1,2,\ldots,m,\ j=1,2,\ldots,n \quad (5)$$

where m×n is the size of binary image watermark.



(a) Digital image. (b) Binary watermark. (c) Watermark after Arnold scrambling

Figure 2. Host image and watermark pre-processing.

A. watermarking detection without attacks

We detect the watermark in the case of no attacks and the results are shown in Figure 3. Here PSNR = 40.8181dB means that digital image maintain the quality after watermark embedding with $\alpha = 0.005$. We make experiments for the embedding depth factor α within a reasonable range of PSNR and NC values. The dynamic value of α is shown as table1.



(a) Watermarked image. (b) Detected watermark. (c) Final Watermark with anti-Arnold.

Figure 3. Results of no attacks.

B. watermarking detection with attacks

In order to verify the robustness of the proposed algorithm, we make experiment against several hostile attacks with $\alpha = 0.125$, such as Gaussian-noise adding (local variance=0.05), salt pepper noise adding (density=0.1), cropping, JPEG compression (quality=90). The simulation results shown in Figure 4~Figure 7. The results show that the proposed watermarking method is not visible and robust to hostile attacks.

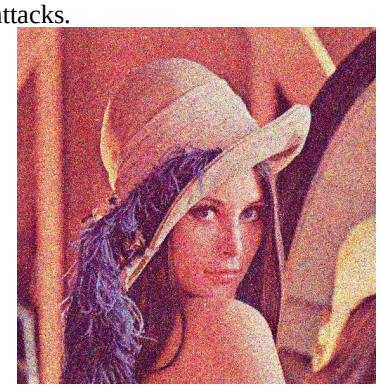


Figure 4. Gaussian noise(v=0.05) PSNR= 14.8992 NC= 0.9477

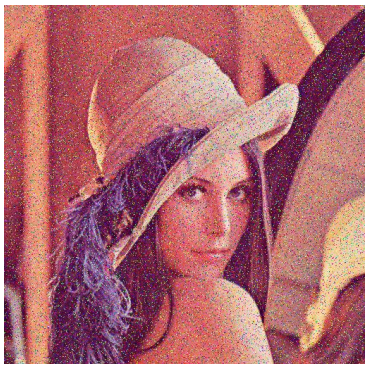


Figure 5. salt pepper noise(D=0.1) PSNR= 15.1233 NC= 0.9666

Figure 6. cropping(192:380,192:380) PSNR= 13.9108 NC= 0.8590

Figure 7. JPEG compression PSNR= 33.8626 NC= 0.9927

IV. CONCLUSIONS

This paper presents a blind digital watermarking method for digital image based on bilinear interpolation. The algorithm has the following characteristics: (1) it generate adaptive watermark based on the size of digital image，so as to improve the robustness of binary watermark; (2) the watermark is embedded in the DCT coefficient of intermediate frequency, which can effectively resist common attacks, such as Gaussian-noise adding, salt pepper noise adding, cropping, JPEG compression;(3) the watermarking detection is simple and fast, and does not require host image. Experimental results show that the algorithm also has good invisibility. The algorithm gives a better fit to the high quality of watermarking visibility in video transmission and it can be applied to video watermarking.

V. ACKNOWLEDGMENT

Key Laboratory of forensic evidence in Shandong Province University (Shandong University of Political Science and Law)

This paper is sponsored by Natural Science Foundation of China(NO.61174018); Natural Science Foundation of Shandong Province, China.(NO.ZR2010FM042); Natural Science Foundation of Shandong Province, China.(NO.ZR2012F014).

VI. REFERENCES

[1] Cox IJ, Killian J, Leighton T, et al., Secure spread spectrum watermarking for multimedia, IEEE Trans. on Image Processing, 1997, 6(12): 1673-1687.

[2] Joumaa H., Davoine F.. An ICA based algorithm for video watermarking. Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005, vol.2, pp.805-808.

[3] Z.F.Yang, P.C.Lee, W.H.Chen, and J.G.Leu, Extension of Structural Watermarks Based on Balanced Incomplete Block Designs, Journal of Information Hiding and Multimedia Signal Processing, October 2011,vol.2, no.4, pp.354-365.

[4] HUANG Jiwu. Embedding image watermarks in DC components[J]. IEEE Transaction on Circuits and System for Video Technology, 2000, 10 (6):974 - 979.

[5] Noorkami. M, Mersereau. R. M. A Framework for Robust Watermarking of H.264 Encoded Video With Controllable Detection Performance. IEEE Transactions on Information Forensics and Security, March 2007, vol.2, pp. 14 - 23.

[6] Na Li, Xiaoshi Zheng, Yanling Zhao, Guangqi Liu,Qingxi Wang. A Strongly Crop-resistant Robust Watermarking Scheme. The Sixth World Congress on Intelligent Control and Automation, WCICA2006.06: 9627-9630.

[7] Lian-Shan Liu, Ren-Hou Li, Qi Gao. A robust video watermarking scheme based on DCT. Proceedings of International Conference on Machine Learning and Cybernetics, 2005, Vol. 8, pp.5176-5180.

[8] Jui-Cheng Yen. Watermark embedded in permuted domain[J]. Electronics Letters,2001, vol.37(2):80-81.

TABLE I. THE FACTOR α CHANGES WITHIN A REASONABLE RANGE OF *PSNR* AND *NC*.

α	0.0005	0.0008	0.001	0.005 (best)	0.01	0.06	0.1	0.125	0.15
PSNR (dB)	40.8514	40.8509	40.8509	40.8181	40.7219	37.5551	34.6562	33.1069	31.7508
NC	0.8401	0.9477	0.9709	1	1	1	1	1	1
Detected watermark