

IMAGE WATERMARKING BASED ON GENETIC ALGORITHM

Zhicheng Wei^{1,2}, Hao Li¹, Jufeng Dai¹, Sashuang Wang¹

¹School of Electronic Information Engineering, Tianjin University, Tianjin 300072, China

²Department of Network Engineering, Hebei Normal University, Shijiazhuang 050016, China

ABSTRACT

In order to improve the robustness and imperceptibility of the image spread spectrum watermark algorithm, a new approach for optimization in 8×8 DCT domain using genetic algorithm (GA) was proposed. GA was used to choose the AC coefficients, which were modified to embed the spread spectrum watermark. The bands were varied to find the most suitable for image with different characteristics. Performance improvement with respect to existing algorithm is obtained by GA adaptive global search. The experimental results show that the proposed algorithm yields a watermark that is invisible to human eyes and robust to various image manipulation, and show that some special positions are the best choices for embedding the watermark. The authors also compare their experimental results with the results of the previous work of others.

1. INTRODUCTION

With the widespread use of the Internet, a lot of digital media, including audio, video and image, have been duplicated, modified by anyone easily and unlimitedly. The copyright protection of the intellectual property of the sensitive or critical digital information is an important legal issue globally. Recently, we have seen the trend of the studies in digital watermarking [1] since the techniques provide the essential mechanism for the ownership authentication.

Digital image watermarking provides copyright protection of image data by hiding appropriate information in the original image. There are a variety of schemes for embedding the watermark. Typical methods of watermarking were based on DCT[2], DWT[3], DFT[4], spatial-domain schemes[5], and vector quantization (VQ) domain methods[6]. One major disadvantage for these methods is if the attackers dissolve the relationships between the original image and the pre-determined set for watermark embedding, the watermarking capability for copyright protection no longer exists. Another disadvantage for typical schemes is how to decide and choose the pre-determined set. Therefore, genetic algorithm (GA) is

employed to solve the problems. In this paper, genetic algorithm is employed to choose the best suitable positions to embed the spread spectrum watermark [7][8].

This paper is organized as follows. Section 2 describes the genetic spread spectrum watermark algorithm. Section 3 illustrates the simulation results, and we also show the superiority of our scheme over the results proposed by other researcher in this section. And we conclude this paper in Section 4.

2. GENETIC WATERMARKING ALGORITHMS

We propose the algorithm whose block diagrams appear in Fig.1. The input image is I with size $M \times N$. We first perform the 8×8 block DCT on I and get the coefficients in the frequency bands, Y . The embedding and extraction method was proposed by Cox [7]. A watermark consists of a sequence of real numbers $X = x_1, \dots, x_n$. In practice, we create a watermark where each value x_i is chosen independently according to $N(0,1)$. The length of watermark, n , was decided by the number of bits of embedding in every 8×8 block.

Equations $Y_i' = Y_i(1 + \alpha x_i)$ and $Y_i' = Y_i(e^{\alpha x_i})$ in [7] were not suitable because the 8×8 DCT transform coefficients don't vary widely. So we insert the watermark into Y to obtain Y' according to (1).

$$Y_i' = Y_i + \alpha x_i \quad (1)$$

The gaussian random vector is imperceptibly inserted in a spread-spectrum-like fashion into the components of the data chosen by genetic algorithm, which are commonly used as adaptive approaches that provide a randomized, parallel, and global search method.

To evaluate the best coefficients for a cluster containing $M \times N/64$ DCT blocks, a sequence of numbers from 2 to 64 is used as the chromosome. Its magnitudes index AC coefficients following zigzag path in the DCT domain. In the beginning, all chromosomes are generated randomly. k bits of the watermark are embedded into distinct DCT blocks and the coefficients chosen for embedding watermark bits are indexed by the chromosome.

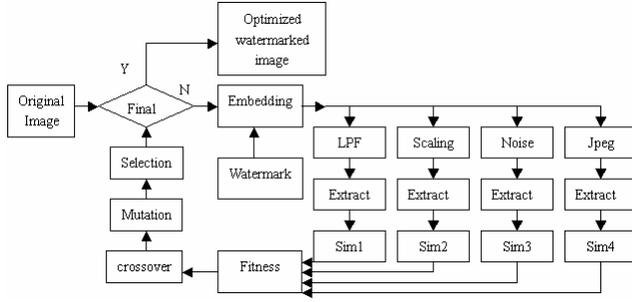


Fig.1. The block diagram of the present algorithm

Then, four attacks are chosen to evaluate the robustness of the embedded watermark. They are low pass filtering (LPF) with normalized radius 0.1, Image Scaling with factor 0.1, Gaussian Noise with strength 1, and JPEG coding distortion with parameter of 5% quality. The fitness of the chromosome is evaluated after attacking procedure.

The middle generation is then generated with crossover and mutation operators. The possibility of crossover and mutation, P_c , P_m are defined as (2) and (3) separately:

$$P_c = P_{cInitial} - \frac{P_{cInitial} - P_{cFinal}}{GenerationMax} \times g \quad (2)$$

$$P_m = P_{mInitial} + \frac{P_{mFinal} - P_{mInitial}}{GenerationMax} \times g \quad (3)$$

$P_{cInitial} = 0.9$, $P_{mInitial} = 0.05$, $P_{cFinal} = 0.3$, and $P_{mFinal} = 0.2$. The pre-specified number of generation, $GenerationMax$, is 100. g is the value of current iteration. The top 50% individuals are selected from the initial generation and the middle generation, then put them into the next generation.

Generally, the fitness of the chromosome can be calculated by evaluating the robustness and the image quality. But the fidelity is high when α is suitable. So the items about image quality such as PSNR or UQI are not included in the fitness. The watermark is extracted after an attack is applied on the watermarked simulated image. Then, the similarity (Sim) value between the original watermark X and extracted mark X^* is calculated as (4). The Sim values are taken into account to evaluate the fitness of a chromosome. The fitness function of GA is defined as (5).

$$Sim(X, X^*) = \frac{X^* \cdot X}{\sqrt{X^* \cdot X^*}} \quad (4)$$

$$Fitness = \sum_{i=1}^4 Sim_i \quad (5)$$

To decide whether the suspected image is a watermarked version of the original image, the similarity is compared with a fixed threshold δ . If the similarity is



Fig.2. Original "Goldhill" image



Fig.3. Watermarked version of present approach. PSNR=51, $\alpha=5$

greater than the fixed threshold, the watermark has been detected. It is proved as (6) that $Sim(X, X^*)$ follows the standard normal distribution.

$$\left. \begin{aligned} X &\sim N(0,1) \\ X^* \cdot X &= \sum_{i=1}^n x_i^* x_i \end{aligned} \right\} \Rightarrow X^* \cdot X \sim N(0, X^* X^{*T})$$

$$\Rightarrow X^* \cdot X \sim N(0, X^* \cdot X^*) \Rightarrow \frac{X^* \cdot X}{\sqrt{X^* \cdot X^*}} \sim N(0,1) \quad (6)$$

So set the threshold $\delta=6$ makes the probability of false watermark detection very small. It can be estimated as (7):

$$P_e = \int_{\delta}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx = \frac{1}{2} \int_{\frac{\delta}{\sqrt{2}}}^{\infty} \frac{2}{\sqrt{\pi}} e^{-t^2} dt$$

$$= \frac{1}{2} erfc\left(\frac{\delta}{\sqrt{2}}\right) = \frac{1}{2} erfc\left(\frac{6}{\sqrt{2}}\right)$$

$$= 9.8659 \times 10^{-10} \quad (7)$$

Table 1. PSNR and Similarity of test images

| Images | PSNR | Sim1 | Sim2 | Sim3 | Sim4 |
|----------|-------|-------|-------|-------|-------|
| Boat | 51.68 | 8.588 | 7.626 | 6.672 | 7.281 |
| Boy | 51.82 | 7.008 | 6.793 | 6.209 | 8.384 |
| Zelda | 51.93 | 6.546 | 7.174 | 8.017 | 7.813 |
| Baboon | 51.87 | 7.121 | 7.191 | 6.192 | 8.565 |
| Mary | 51.92 | 6.938 | 6.859 | 7.764 | 7.264 |
| Girl | 51.84 | 7.454 | 6.197 | 7.799 | 7.546 |
| Goldhill | 51.65 | 8.488 | 7.877 | 8.284 | 7.392 |
| Lena | 51.55 | 7.579 | 7.289 | 7.715 | 8.247 |
| Pepper | 51.86 | 7.936 | 7.158 | 7.726 | 7.403 |

3. EXPERIMENTAL RESULTS

In our simulation, we take nine well-known 256×256 test images with $\alpha = 5$. One of them is Goldhill, shown in figure 2. Two bits of watermark are embedded in every 8×8 DCT block. The size of corresponding watermark is 2048. The watermarked version of Goldhill generated with the present algorithm is shown in figure 3. Its PSNR 51 is much better than Cox’s PSNR 37.34. We can see although no evaluation about image quality is included in the fitness, the PSNR of watermark image is high.

The two watermarked versions of Goldhill, present approach and Cox’s approach, then go through four attacking methods separately. In figure 4, we can see how the average similarity measure is affected under these attacks. The plots of the present approach are all above the threshold $\delta = 6$ under the attacks of LPF and gaussian noise addition. So the spread spectrum watermark can be detected correctly in any strength of the two attacks. Meanwhile the false detector responses of Cox’s are down to 30% in the case of LPF, to 50% in the case of noise addition.

When the watermarked images are attacked by scaling, the plot of the present approach is under the threshold at few points, but it is found that the lowest similarity of the plot is equal to 5.77—a relatively high value. At the same time, about 20% plot of Cox is below the threshold. And we can see the responses to the JPEG of the two methods are similar except for the situation of 5% quality. Also, by increasing the parameter α , it is possible to maintain the same level of similarity measure while lowering the PSNR. In this way, robustness is improved for all possible attacks.

Other eight testing images have been processed. All PSNR and Sim values are shown in table 1. Also applying the algorithm on other testing images shows that the

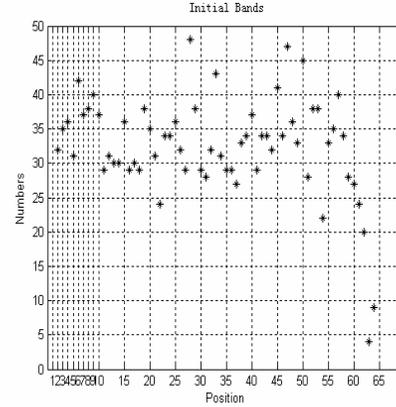


Fig.5. The histogram of bands at 0th iteration

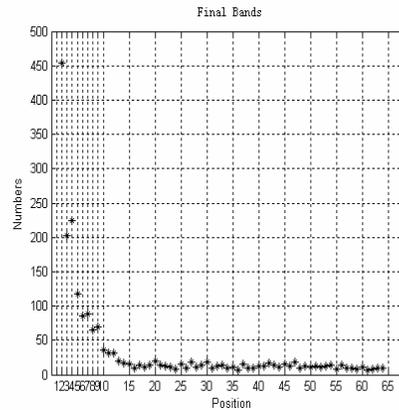


Fig.6. The histogram of bands at 100th iteration

watermarked images are perceptually equal to the originals, and that the watermarks are still detectable after attack, as indicated in above experimental results.

In our algorithm, the bands for the watermark to be embedded differ from one block to another. The selected bands also differ from one test image to another. Therefore, from a statistical point of view, we find that the low frequency domain is the bands needed to acquire the best fitness value. $Y(2)$ is always the maximum of them. Fig.5 and 6 compare the bands at the 0th and 100th iteration in GA of one test image.

4. CONCLUSIONS

A robust algorithm for DCT-based GA spread spectrum watermarking has been presented in this paper. We can extract the watermark correctly almost in all kinds of the four attacks. It is robust because we make use of GA to train the frequency set for embedding the watermark.

The motivation of proposing this method is to find the most suitable bands in the DCT coefficients. The best bands

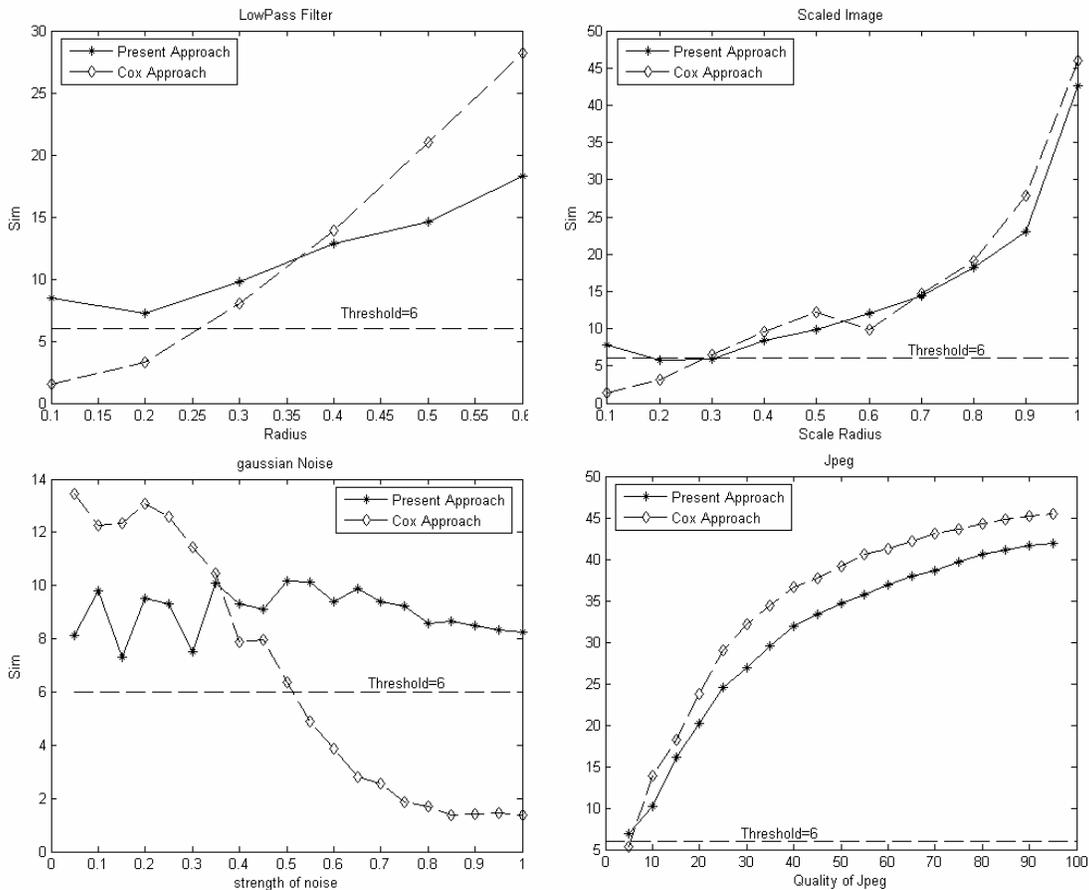


Fig.4. Performance comparison between the present approach and Cox's approach.(Top left) Similarity against lowpass filter, (top right) Image Scaling, (bottom left) gaussian noise and (bottom right) JPEG coding distortion. The $sim = 6$ threshold is included in all plots.

include not only the low frequency components but also high frequency coefficients. $Y(2)$ is found to be the most popular band for robust watermarking. In comparison with the Cox's method, watermark embedding with our scheme can get better-watermarked image qualities and more robust to the attacks.

REFERENCES

- [1] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, "Information hiding-a survey," *Proc. IEEE* 87(7) (1999) 1062--1078
- [2] W.C Chu, "DCT-based image watermarking using subsampling," *IEEE Trans. Multimedia* 5(1) (2003) 34-38
- [3] M. Barni, F. Bartolini, A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," *Image Process. IEEE Trans. Image Process.* 10(5) (2001) 783-791
- [4] J.J.K. O'Ruanaidh, W.J. Dowling, F.M. Boland, "Phase watermarking of digital image, Proceedings of the IEEE International Conference on Image," *Processing, Vol.3, Lausanne, Switzerland*, 1996, 239-242
- [5] N.Nikolaidis, I.Pitas, "Robust image watermarking in the spatial domain," *Signal Process.* 66(1998) 385-403
- [6] Jo.M.Kim.H "A digital image watermarking scheme based on vector quantisation," *IEICE Trans. Inf.&Syst.* Vol E85-D. (2002) 303-305
- [7] Ingemar J. Cox, Joe Kilian, F. Thomson Leighton, and Talal Sharnoon, "Secure Spread Spectrum Watermarking for Multimedia" *IEEE Trans. On Image Processing*, Vol.6, No.12, Dec.1997
- [8] Prayoth Kumsawat, Kitti Attakitmongcol, and Arthit Srikaew , "A new Approach for Optimization in Image Watermarking by using Genetic Algorithms" *IEEE Trans on Signal Processing*, Vol.53, No.12, Dec.2005
- [9] M.L.Miller and J.A.Bloom, "Computing the probability of false watermark detection," in *Proc. 3rd Int. Workshop on Information Hiding*, Oct.1999, pp.146-158