ATLANTIS PRESS

Advances in Computer Science Research, volume 62

2nd Joint International Information Technology, Mechanical and Electronic Engineering Conference (JIMEC 2017)

A Robust Watermarking Algorithm For JPEG Images

Baosheng Sun, Daofu Gong*, Fenlin Liu

**Foundation of Science and Technology on Information Assurance Laboratory(Zhengzhou Science and Technology Institute), Zhengzhou 450001, China, sunbaosheng@aliyun.com*

Keywords: JPEG image; singular value decomposition perturbation theory; quantized DCT coefficient; dither modulation

Abstract

This paper proposes a robust and blind watermarking algorithm based on matrix Singular Value Decomposition (SVD) perturbation theory for JPEG image copyright protection. First, the quantized DCT coefficient blocks are extracted from the JPEG image, then SVD is performed on each block, and finally the watermark is embedded into a set of selected maximum singular values of the quantized Discrete Cosine Transform (DCT) coefficients using dither modulation. From the embedding principle of the watermarking algorithm, we can see that the watermark information can be completely extracted correctly when the watermarked image under certain attack. A large number of experiments show that the algorithm has a higher degree of robustness against attacks such as Gaussian noise and JPEG compression, etc.

1 Introduction

In recent years, with the rapid development of Internet and intelligent mobile devices, the transmission of digital image information becomes more and more frequent. According to the statistics of Facebook, more than 350 million images are uploaded to the Internet every day [9]. JPEG compression is the image standard compression which is popularly used in Internet [3]. The widespread use of digital images has also promoted the development and application of digital image editing software such as Adobe Photoshop, CorelDRAW, etc. These tools may make the images easily illegally edited and transmitted, so it is significant to carry on the research of image copyright protection technologies, one of which is digital watermarking [5].

Watermarking algorithms for JPEG images can be classified into two categories: Embedding watermarks in non-JPEG domains, and directly embedding watermarks into the JPEG domain. Wherein a non-JPEG domain watermarking algorithm, such as paper [1] according to the JPEG compression standard, the watermark embedding is realized by adjusting the difference of the DCT coefficients at the same position of the adjacent image block, so it is compatible with JPEG compression and has better robustness to JPEG compression attack. DCT transform has good robustness and high energy compression capability. Discrete Wavelet Transform (DWT) is compatible with JPEG compression standard [4]. Therefore, paper [4] presents a hybrid image watermarking algorithm based on DCT and DWT. In order to ensure the correct extraction of the watermark, it needs to calculate the means of the vertical (LH) sub band in the DWT domain as the secret key. The algorithm is robust to JPEG compression attacks, but requires a large amount of storage space to store the secret keys. If the watermark is embedded in the non-JPEG domain, it would be distort easily when the watermarked image is compressed. However, it is more convenient to embed the watermark directly in JPEG domain [2].

After embedding the watermark in the JPEG domain, all the DCT coefficients need to be re-quantized with the same quantization table. This means that small-magnitude watermark can be completely removed in the re-quantization [8]. Therefore, the watermark embedding process should be compatible with the JPEG compression standard, which is one of the key problems in JPEG watermark embedding. In [2], the embedding of secret information is realized by modifying all quantized DCT coefficients whose absolute value is L. The algorithm improves the embedding capacity and restores the original image. But the embedding capacity is different for different images, and has a poor ability resist attack. In [7] the watermark information is embedded into the quantized DCT coefficients based on the fact that the relationship between DCT coefficients at the same position in different blocks remains unchanged. But the robustness is affected by the quality factor of the original image.

In order to improve the watermarking robustness of JPEG images, this paper combines the perturbation theory of singular value decomposition and embeds watermarking information into the maximum singular value of DCT coefficients. Extensive experiments show that this algorithm can efficiently resist the JPEG compression, Gaussian noise, salt and pepper noise, median filtering, and scaling attack.

2 Proposed algorithm

Perturbation theory of matrix singular value decomposition [6]: When the matrix A superposes a perturbation matrix B, the change of the singular values of A does not exceed the maximum singular value of the matrix B.

Copyright © 2017, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

The principle of watermarking algorithm based on SVD is shown in Figure 1. The maximum singular value s of each quantized DCT coefficient block is extracted. When the embedding watermark information is 1, modulate the remainder $\mathrm{mod}(s,\delta)$ of s with the quantization factor δ to $\delta/2$; when the embedding watermark is 0, $\mathrm{mod}(s,\delta)$ is modulated to 0. Attacks on the watermarked image are equivalent of adding a perturbation matrix on it. From the perturbation theory of SVD, we can know that if the maximum singular value of the perturbation matrix does not exceed $\delta/4$, the change of the maximum singular value of the watermarked block does not exceed $\delta/4$ and the watermark information can be completely extracted correctly, namely, when $\mathrm{mod}(s,\delta)\in[\delta/4,3\delta/4]$ the extracted watermark information is 1, when $\mathrm{mod}(s,\delta)\in[0,\delta/4)\cup(3\delta/4,\delta)$ the extracted watermark information is 0.

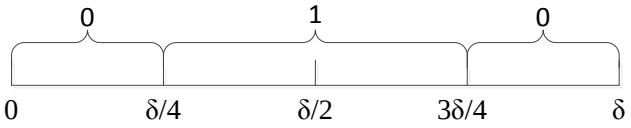


Figure 1: Schematic watermarking algorithm

Watermark embedding and extraction flow chart shown in Figure 2:

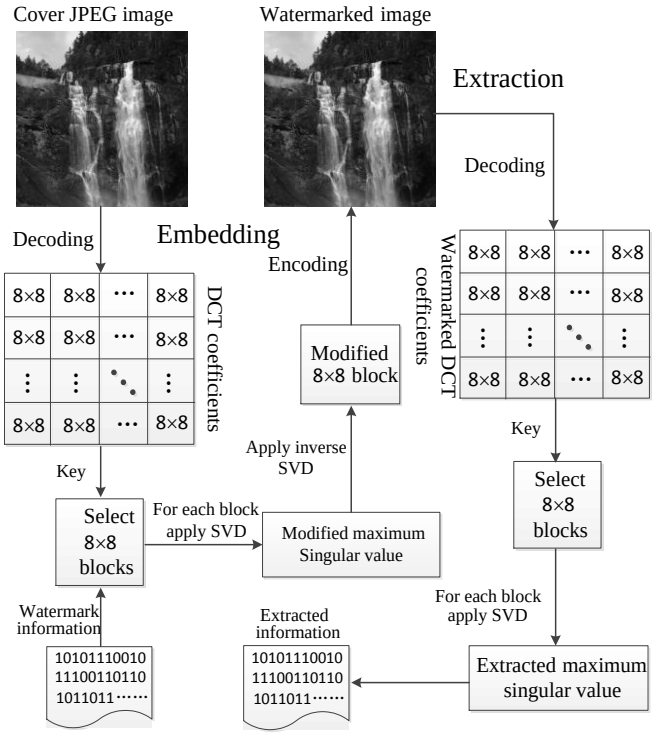


Figure 2: Watermark embedding and extraction

2.1 Watermark embedding procedure

The original image I is a JPEG image of size $M\times N$. The embedding watermark information is 0, 1 bit sequence $W=\{w_1,w_2,\cdots,w_i,\cdots,w_L\}$ where $w_i\in\{0,1\}$, L is the watermark length. Watermark embedding algorithm specific steps are as follows:

Step1: Read in the original image I and perform entropy decoding to obtain a series of quantized DCT coefficient blocks $\mathbf{X}=\{X_k\}$, where $k=0,\cdots,B-1$ and B is the total number of blocks.

Step2: Select L blocks from the set $\mathbf{X}$ by the secret key K and recorded as $\{X_{k1},X_{k2},\cdots,X_{ki},\cdots,X_{kL}\}$, where $ki\in[0,B-1]$ and $i=1,2,\cdots,L$, the selected block is used as the watermark embedding block.

Step3: Apply SVD to matrix X_{ki}

$$X_{ki}=U_{ki}\times S_{ki}\times V_{ki}^T \tag{1}$$

where U_{ki}、V_{ki} are the left and right singular matrix of X_{ki} respectively. V_{ki}^T is the transpose of matrix V_{ki}, S_{ki} is the singular value matrix of X_{ki} and s_{ki1} is the maximum singular value.

Step4: Modify s_{ki1} to achieve watermark embedding. The embedding rules are as follows:
If $w=1$,

$$s_{ki1}^w=s_{ki1}-\mathrm{mod}(s_{ki1},\delta)+\delta/2 \tag{2}$$

If $w=0$,

$$s_{ki1}^w=\begin{cases}s_{ki1}-\mathrm{mod}(s_{ki1},\delta), & if\ \mathrm{mod}(s_{ki1},\delta)<\delta/2\\ s_{ki1}-\mathrm{mod}(s_{ki1},\delta)+\delta, & if\ \mathrm{mod}(s_{ki1},\delta)\ge\delta/2\end{cases} \tag{3}$$

where s_{ki1}^w is the watermarked maximum singular value, $\mathrm{mod}(s_{ki1},\delta)$ stands for s_{ki1} take the remainder to δ, δ is quantization factor.

Step5: Apply inverse SVD to get the watermarked quantized DCT coefficient block X_{ki}^w

$$X_{ki}^w=U_{ki}\times S_{ki}^w\times V_{ki}^T \tag{4}$$

Step6: Round each element of X_{ki}^w obtain the watermarked quantized DCT coefficient X_{ki}^{wz}. Replace X_{ki}^{wz} with X_{ki} and combined with the remaining part, and eventually encode to get the watermarked image I_w.

2.2 Watermark extraction procedure

The watermark extraction process only needs the secret key K and the quantization factor δ. Therefore, it's a blind watermarking. The concrete steps of watermark extraction are as follows:

Step1: Step1, Step2, Step3 in the process of embedding watermark are used to get the watermarked maximum singular value s_{ki1}^{w} .

Step2: Extract the watermark information w_i' according to the formula (5):

$$w_i' = \begin{cases} 1, & \frac{1}{4}\delta \le \mathrm{mod}(s_{ki1}^{w}, \delta) \le \frac{3}{4}\delta \\ 0, & 0 \le \mathrm{mod}(s_{ki1}^{w}, \delta) < \frac{1}{4}\delta \ or \ \frac{3}{4}\delta < \mathrm{mod}(s_{ki1}^{w}, \delta) < \delta \end{cases} \quad (5)$$

The extracted watermarking $W' = \{w_1', w_2', \cdots, w_i', \cdots, w_L'\}, w_i' \in \{0,1\}$.

Note: It is worth noting that the change of the maximum singular value of the watermarked DCT block is not greater than $\delta / 2$ according to the formula (2) and (3). To ensure the sequence of the maximum singular value in the DCT block after embedding watermark, let $s_{ki1} = s_{ki2} + \delta/2$ when $s_{ki1} - s_{ki2} < \delta/2$, where s_{ki2} is the second largest singular value.

3 Experimental results

To verify the performance of the proposed algorithm, the invisibility and robustness are tested in Matlab R2009a. Experimental images are selected from the BossBase [1] image library and compressed into JPEG images with the quality factor of 85. The content of the image covers a wide range, including: natural scenery, man-made facilities and human portraits, etc. Part of the carrier image shown in Figure 3:

Figure 3: Carrier image: Building, Water, Giraffe, Car, Flower, Human

The peak signal to noise rate (PSNR) is used in this paper to evaluate the image quality. It is defined as follows:

$$PSNR = 10 \times log_{10}\left(\frac{M \times N \times 255^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}\left[I(\mathrm{m},\mathrm{n}) - I^{W}(\mathrm{m},\mathrm{n}) \right]^2} \right) \quad (6)$$

Where $M \times N$ is the size of the image, $I(\mathrm{m},\mathrm{n})$ and $I_w(\mathrm{m},\mathrm{n})$ are the pixel values of the original image and the watermarked image at position (m,n) respectively. PSNR unit is dB, and the greater the PSNR the better the watermark invisibility.

According to the algorithm proposed in Section 2, different watermarks are embedded into the above-mentioned carrier images. The PSNR of the watermarked images at different embedding rates is shown in Table 1, where L indicates the watermark length.

L (bit)	Building	Water	Giraffe	Car	Flower	Human
1024	40.69	40.70	42.14	41.81	41.01	42.06
2048	40.42	40.51	41.92	41.57	40.85	41.64
3072	40.31	40.27	41.77	41.24	40.70	41.40
4096	40.21	40.14	41.50	41.17	40.54	41.29

Table 1: The PSNR of watermarked images with different embedding ratio

The bit error rate (BER) is used to evaluate the watermark robustness. Calculated as follows:

$$\mathrm{BER}(\%) = \frac{\sum_{i=1}^{L_w} w_i \oplus w_i'}{L} \times 100 \quad (7)$$

where $\oplus$ denotes the XOR operation. w_i 、 $w_i' \in \{0,1\}$ are the original watermark and extracted watermark respectively. L is the length of the watermark. The smaller the BER value is, the higher the similarity between the extracted watermark and the original watermark, the better the robustness of the watermarking algorithm.

In order to verify the rationality of the principle of the watermarking algorithm, we embed the watermark into the images in Fig. 3. The quantification factor $\delta = 20$, the watermark length is 4096 bits. Then, the watermarked image is compressed with different quality factors. The BER (%) values against JPEG compression of watermarked images is reported in the columns 3, 5 and 6 of Table 2 and table 3. Q is the quality factor. β is the range of the maximum singular value of the perturbation matrix produced by JPEG compression. From table 2 and table 3, it can be seen that when the max value of β less than $5(\delta/4 = 20/4 = 5)$ the BER is 0. The result is identical with the principle of the watermarking algorithm.

[1] BossBase image Library Download URL:http://agents.fel.cvut.cz/stegodata/;

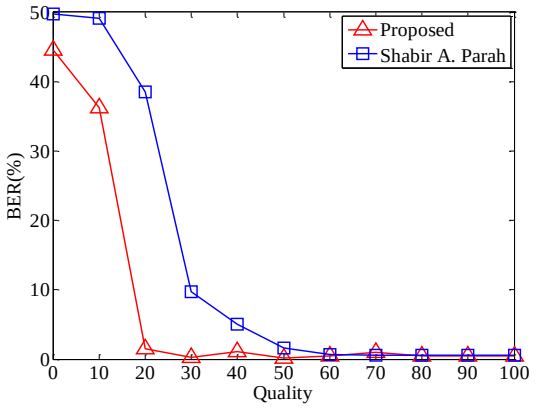
Q	Building	β	Water	β	Giraffe	β
10	35.9	[1,20]	36.9	[0,18]	33.1	[1,19]
20	1.87	[1,11]	0.56	[0,10]	0.73	[1,11]
30	0.12	[0,7.5]	0.00	[0,7.4]	0.04	[0,7.1]
40	0.02	[0,8.8]	0.00	[0,5.8]	0.00	[1,6.5]
50	0.07	[0,6.9]	**0.00**	**[0,4.8]**	0.00	[0,5.1]
60	0.02	[0,9.4]	**0.00**	**[0,3.7]**	**0.00**	**[0,3.7]**
70	0.02	[0,8.5]	**0.00**	**[0,3.4]**	**0.00**	**[0,3.7]**
80	0.02	[0,7.7]	**0.00**	**[0,2.8]**	**0.00**	**[0,3.6]**
90	0.02	[0,8.8]	**0.00**	**[0,1.6]**	**0.00**	**[0,3.8]**
100	0.02	[0,8.1]	**0.00**	**[0,1.6]**	**0.00**	**[0,3.3]**

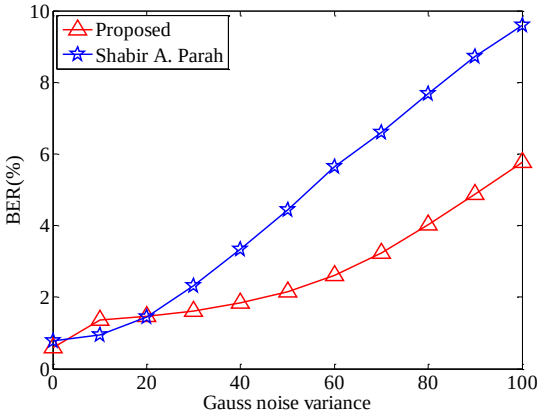
Table 2: The BER of the images in figure 3 which attacked by JPEG compression with different quality factors and the range of the maximum singular value of the perturbation matrix

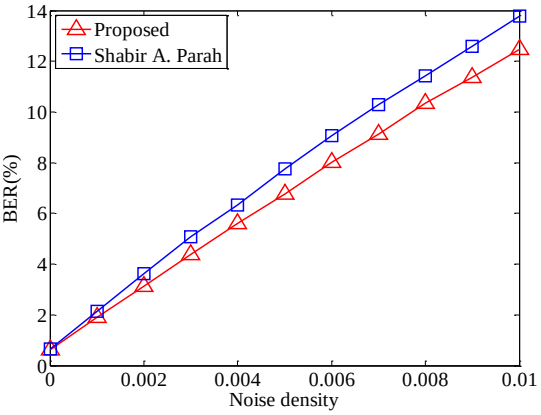
Q	Car	β	Flower	β	Human	β
10	36.2	[1,20]	34.7	[1,21]	32.8	[1,21]
20	1.85	[0,12]	1.36	[0,10]	0.97	[1,11]
30	0.21	[0,12]	0.00	[0,7.5]	0.07	[0,7.9]
40	0.34	[0,7.8]	0.00	[0,5.9]	0.00	[1,6.6]
50	0.12	[0,9.2]	**0.00**	**[0,4.9]**	0.02	[0,6.4]
60	0.34	[0,8.5]	**0.00**	**[0,4.2]**	0.02	[0,6.1]
70	0.34	[0,9.1]	**0.00**	**[0,3.4]**	**0.00**	**[0,4.6]**
80	0.36	[0,8.0]	**0.00**	**[0,2.7]**	**0.00**	**[0,4.8]**
90	0.36	[0,8.4]	**0.00**	**[0,1.4]**	**0.00**	**[0,4.5]**
100	0.36	[0,8.7]	**0.00**	**[0,1.0]**	**0.00**	**[0,4.3]**

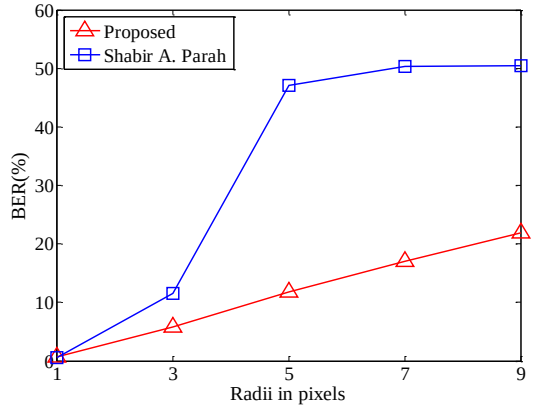
Table 3: The BER of the images in figure 3 which attacked by JPEG compression with different quality factors and the range of the maximum singular value of the perturbation matrix

By comparing with the algorithm proposed by Shabir A. Parah [4], the robustness of the proposed algorithm to the JPEG compression, Gaussian noise, salt and pepper noise, median filtering attack is verified. In the experiments, the embedding watermark information is 0, 1 bit; the watermark length is 4096 bits. 100 images were randomly selected from the BossBase image library as the carrier image. BER is the mean of 100 images. In Shabir A. Parah [4], embedding factor is 20, extraction factor is 5, scaling factor $V = 0.5$, and threshold $T = 80$. In this paper, the quantification factor $\delta = 20$ .The experimental results are shown in Figure 4. It can be seen from Fig.4 that the proposed algorithm has better robust to JPEG compression, Gaussian noise, salt and pepper noise, median filter and scaling attack compared with the algorithm proposed by Shabir A. Parah [4].









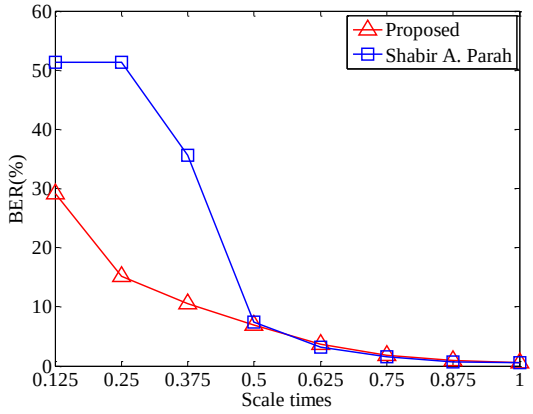


Figure 4: The mean value of the BER of the 100 images is extracted after the attack. JPEG compression attack; Gauss noise attack; Salt and pepper noise attack; Median filtering attack; Scaling attack;

4 Conclusions

In this paper, a robust and blind watermarking algorithm is proposed based on the perturbation theory of SVD. According to the principle of the algorithm, the embedded watermark can be completely correct extraction when the maximum singular value of perturbation matrix does not exceed a quarter of the quantification factor. Meanwhile experimental results show that the proposed algorithm is robust to JPEG compression, Gaussian noise, salt and pepper noise, median filtering, and scaling attack. In the future, we will focus on the impact of various attacks on the image singular value, analyze and improve the robustness of the algorithm.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (No. 61401512, 61379151, 61272489and 61302159), the Excellent Youth Foundation of Henan Province of China (No. 144100510001).

References

[1] Parah S A, Sheikh J A, Loan N A, et al. “Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing”, Digital Signal Processing, **53**, pp. 11-24, (2016).

[2] Nikolaidis A. “Low overhead reversible data hiding for color JPEG images”, Multimedia Tools And Applications, **75**, pp. 1869-1881, (2016).

[3] Chang C C, Chen T S, Chung L Z. “A steganographic method based upon JPEG and quantization table modification”, Information Sciences, **141**, pp. 123-138, (2002).

[4] El Gamal A F, Mosa N A, El Said W K. “Block-based Watermarking for Color Images using DCT and DWT”, International Journal of Computer Applications, **66**, pp. 0975-8887, (2013).

[5] Tiwari G. “A Review on Robust Watermarking with its Applications and Comparative Analysis”, International Journal of Signal Processing, Image Processing and Pattern Recognition, **8**, pp. 85-90, (2015).

[6] Hong Z Q. “Algebraic feature extraction of image for recognition”, Pattern recognition, **24**, pp. 211-219, (1991).

[7] Luo W, Heileman G L, Pizano C E. “Fast and robust watermarking of JPEG files”, Image Analysis and Interpretation (2002).

[8] Wong P H W, Au O C. “A blind watermarking technique in JPEG compressed domain”, Image Processing, **3**, pp. 497-500, (2002).

[9] Ong S Y, Wong K S, Qi X, et al. “Beyond format-compliant encryption for JPEG image”, Signal Processing: Image Communication, **31**, pp. 47-60, (2015).