A Novel Geometrically Invariant Blind Robust Watermarking Algorithm Based on SVD and DCT

Hu Guan[1,2] , Zhi Zeng[1] , Jie Liu[1] , Shuwu Zhang[1], Peiyu Guo[3]

[1]*High-Tech Innovation Center, Institute of Automation, Chinese Academy of Sciences, Beijing, China*

[2]*WaSu Media Group Co.Ltd, Hangzhou, China*

[3]*Academy of Broadcasting Science State Administration of Radio, Film & Television, Beijing, China*

E-mail:{ hu.guan, zhi.zeng, jie.liu, shuwu.zhang }@ia.ac.cn; guopeiyu@abs.ac.cn

***Abstract*—In this paper, we propose a novel blind image watermarking algorithm which is resistant to various attacks, including geometrical distortions. To embed the watermark, we first enlarge the image with a small scale to be fit for the next image blocking process. Secondly, the enlarged image is blocked into macroblocks and subblocks with adaptively determined sizes. Thirdly, we scramble the watermark and embed it repeatly into the coefficients which are obtained from the subblock-based SVD followed by macroblock-based DCT. Then, the watermarked image can be obtained by means of corresponding inverse transformations. The watermark extraction process is similar as the embedding one. Comparing with others' works, the small-scale image enlargement, the adaptive image blocking and the watermark scrambling we present in this SVD-DCT based method play an important role in increasing the robustness to resist geometrical distortions. Experimental results demonstrate that our method can not only resist common image processing attacks, but also has good performance when the image has been scaled or cropped.**

Keywords- image watermarking; geometrical distortion; Singular Value Decomposition (SVD); Discrete Cosine Transformation (DCT)

I. INTRODUCTION

In recent years, the rapid development of multimedia and internet techniques makes lots of digital contents transmitting and exchanging by means of internet. The protection of digital media copyrights has become more and more important. Against this background, many researchers doing their works on the topic of digital watermarking in order to protect the multimedia copyrights using technology means, especially for digital images, audios, videos, and so on.

With the development of digital image watermarking techniques, most researchers spend their time to embed the watermark into the transform domains of the images in order to get good invisibility and robustness, such as Discrete Fourier Transformation (DFT), Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT), and so on. In the last few years, Singular Value Decomposition (SVD) technique has been introduced in the watermark embedding process. The watermark can simply be embedded into the singular values which are obtained by the SVD of the original image [1]. The SVD can also be used with some other transformations together to improve the performances [2-5]. These schemes can get good performance on watermark invisibility and robustness. However, most of the previous algorithms in this area are non-blind, they can not detect or extract the watermark without the help of original images or some intermediate variables which are obtained in watermark embedding processes.

The scheme proposed in [5] is a kind of blind algorithm to embed and extract the image watermark. They used subblock-based SVD and macroblock-based DCT to embed the watermark in the transform coefficients. It can embed the watermark repeatly and get good performances when the watermarked image has undergone some kinds of common image processing, such as JPEG compression, Gaussian noise, median filtering, and so on. Meanwhile, this scheme also some disadvantages. Firstly, they used fixed sizes of macroblocks and subblocks when the image is blocked, due to which the algorithm can't resist image scaling distortion. Secondly, they embed the watermark in a fixed order according to the image blocks, because of which the algorithm can not resist image cropping distortion splendidly. Thirdly, they used random gradient search method to determine the embedding strength adaptively, which will seriously affect the watermark embedding efficiency.

To overcome the drawbacks of the algorithm in [5], we propose our novel geometrically invariant blind robust watermarking algorithm in this paper. We first enlarge the original image in a small scale to be fit for the following adaptively blocking process, and embed the scrambled watermark into the largest singular values of each subblock. We will discuss our algorithm in detail in section II.

The rest of this paper is organized as follows: section II presents our novel SVD-DCT based watermark embedding method and the corresponding watermark extraction method. Then, in section III, we concentrate on the experimental results of our algorithm. We illustrate the watermark robustness by comparing the results with some contrastive algorithms. We draw our conclusion in section IV and give some probable improvement measures.

II. SVD-DCT Based Watermarking Algorithm

In this section, we describe our watermark embedding and extraction schemes in detail and emphasize the novel ideas we propose. Because both SVD and DCT are common mathematical operations to the matrixes, we need not to show these in detail, we can find these in [4]. Be different from the image blocking scheme by fixing the macroblocks' and subblocks' sizes in [5], in our work, we fix the number of macroblocks in the whole image to be 16×16 and the number of subblocks in each macroblock to be 4×4. In order to increase the watermark extraction accuracy, we embed the scrambled watermark repeatly into the transform coefficients.

A. SVD-DCT Based Watermark Embedding Process

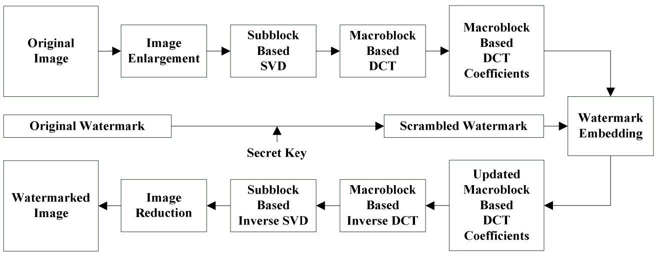


Figure 1. Watermark embedding process.

Fig. 1 illustrates the block diagram of the watermark embedding algorithm. We embed the watermark as follow:

- Enlarge the original image with a small scale. Both of the height and the width of the enlarged image are the minimal positive integrals which are not smaller than the original one's and both can be divided by 16 with no remainder;
- Divide the enlarged image into 16×16 non-overlapped macroblocks in the height-width order;
- Generate a random positive integer sequence whose length is equal to the length of the watermark using the secret key, and rearrange the watermark bits according to the random sequence to get a scrambled one.
- Doing the following operations based on each macroblock:

a) Divide the macroblock into 4×4 non-overlapped subblocks in the row-column order, enlarge the smaller subblocks to the same size as the largest one;

b) Perform SVD to each subblock and select their biggest singular values to make a 4×4 matrix;

c) Perform DCT to the 4×4 matrix above and select two pairs of medium-high frequency coefficients to embed two watermark bits. The nuclear watermark bits embedding scheme we use here is the same as in [5];

d) Perform inverse DCT to the updated 4×4 matrix and update the largest singular value of each subblock;

e) Update the subblocks' data using the inverse operation of SVD and obtain the watermarked macroblock.

- Reduce the watermarked enlarged image to the original size.

As mentioned in [5], for one bit embedding, we use two DCT coefficients. We first calculate the difference of the two coefficients' magnitudes as follow:

$$D(x_1,y_1,x_2,y_2)=|F(x_1,y_1)|-|F(x_2,y_2)| \cdot \tag{1}$$

And then we modify $F(x_1,y_1)$ and $F(x_2,y_2)$ in order to get a positive D if the watermark bit is "1" or a negative D if the watermark bit is "0".

We embed the watermark bit "1" as follows:

1) If $D(x_1,y_1,x_2,y_2)\geq mask$, no operations are needed;

2) If $D(x_1,y_1,x_2,y_2)< mask$, modify the coefficients as follows when both $F(x_1,y_1)$ and $F(x_2,y_2)$ are not zero:

$$\begin{cases} F'(x_1,y_1)=sign(F(x_1,y_1))\times \\ \qquad \left[(|F(x_1,y_1|+|F(x_2,y_2|)/2+0.5\cdot mask\right] \\ F'(x_2,y_2)=sign(F(x_2,y_2))\times \\ \qquad \left[(|F(x_1,y_1|+|F(x_2,y_2|)/2-0.5\cdot mask\right] \end{cases} \tag{2}$$

3) If $F(x_1,y_1)=F(x_2,y_2)=0$,

$$\begin{cases} F'(x_1,y_1)=0.5\cdot mask \\ F'(x_2,y_2)=-0.5\cdot mask \end{cases} \tag{3}$$

In the formulas above, *mask* is called embedding strength, we obtain this parameter as follow:

$$mask=\alpha\cdot edge+\beta \tag{4}$$

where *edge* is the sum of the absolute values of the 8 high frequency coefficients in 4×4 DCT for each macroblock. α and β are empirical values in our work instead of calculating them adaptively in [5].

If the watermark bit is "0", we use the similar rule as "1" but exchange the positions of $F(x_1,y_1)$ and $F(x_2,y_2)$ as same as $F'(x_1,y_1)$ and $F'(x_2,y_2)$ in (2) and (3).

In this part, we illustrate our novel watermark embedding scheme. Be different from others', we enlarge the original image in a small scale to be fit for the image blocking operation and fix the number of macroblocks and subblocks while image being blocked, in addition, we scramble the watermark before it being embedded. All these improvements above can make better performance for our algorithm than others'. We will discuss the advantages and disadvantages in section III.

B. SVD-DCT Based Watermark Extraction Process

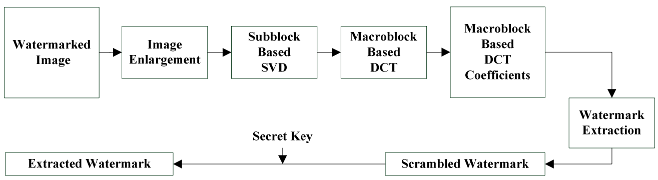


Figure 2. Watermark extraction process.

Fig. 2 illustrates the block diagram of our watermark extraction algorithm. Similar as watermark embedding process above, we also need to enlarge the detect image first and block it to perform the subblock-based SVD and macroblock-based DCT. Select the coefficient pairs in the same positions as watermark embedding and extract the bits one by one using the same nuclear watermark bits extraction scheme as in [5]:

Firstly, we calculate the difference of each coefficients pair.

$$D^*(x_1, y_1, x_2, y_2) = |F^*(x_1, y_1)| - |F^*(x_2, y_2)| . \tag{5}$$

Secondly, we sum the values of different D^* corresponding to all pairs of coefficients where the same bit is repeatedly embedded.

$$B'_i = \sum_{\Phi_i} D^*(x_1, y_1, x_2, y_2) . \tag{6}$$

where Φ_i is the set of selected coefficients pairs for the *i*-th bit.

And then, we extract the bits one by one as follow:

$$W'_i = \begin{cases} 1 & B'_i \geq 0 \\ 0 & B'_i < 0 \end{cases} . \tag{7}$$

After extract the bit sequence above, a more important step in our work is to perform the inverse scrambling process to get the correct order of the watermark using the same secret key as in watermark embedding process.

III. EXPERIMENTAL RESULTS

To measure the robustness of our algorithm, we perform the watermark embedding and extraction operations repeatly on several kinds of images with different sizes. We embed the watermark into the pixels of the gray scale images or the luminance components of the color images. We also perform many kinds of distortions to the watermarked images to check the resistance to the image processing and geometric distortions, including Median Filtering, JPEG Compression, Additive White Gaussian Noise (AWGN), Salt & Pepper Noise, Scaling and Cropping. We choose 45 images with the same size as 512 ×512 in [9] and 45 images with 7 kinds of different sizes in [8] to form the test image set. We use 64 bits 0-1 sequence as the watermark and embed it into the images.

Besides the algorithm we proposed, we also present some comparisons. One is the contrastive method which is similar as ours by fixing the numbers of blocks, but excluding the image enlargement and watermark scrambling processes when watermark being embedded and extracted. Another one is the SVD-DCT scheme in [5] by fixing the sizes of the blocks instead of fixing the numbers of them, but setting the embedding strength parameters to be empirical values instead of calculating them adaptively.

1	2	6	7
3	5	8	13
4	9	12	14
10	11	15	16

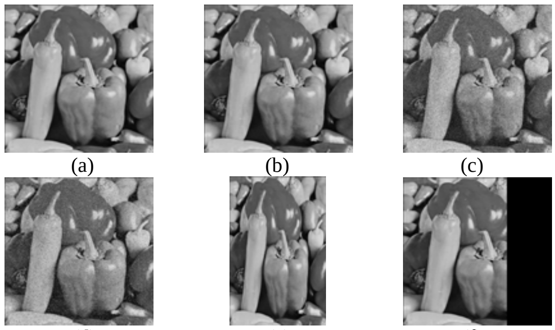
Figure 3. 4×4 DCT coefficients.

For each macroblock, empirically, we choose the DCT coefficients numbered 7 and 8 in Fig. 3 to embed the first bit, and choose the coefficients numbered 10 and 11 to embed the second one. We set the watermark embedding strength α to be 0.06 and set β to be 0.9 in all three methods. We get the average PSNRs of the 90 images in our proposed method, contrastive method and SVD-DCT scheme in [5] to be 36.74dB, 38.13dB, 38.25dB, respectively. Fig. 4 shows the original image and the watermarked one. Although the PSNR of our method is smaller than others' due to the image enlargement and reduction operations, we can see the watermark which is embedded using proposed method also has good invisibility. We can extract the watermarks from the watermarked images directly with the average bit error rate (BER) to be 0.00%.

(a) (b)

Figure 4. (a) original image (b) watermarked image.

Fig. 5 shows some distorted watermarked images with several attacks, including (a) Median Filtering with the window size to be 5×5; (b) JPEG Compression with the quality factor to be 30%; (c) AWGN with the variance to be 0.05; (d) Salt & Pepper Noise with the density to be 0.12; (e) Scaling with the width direction factor to be 65%; (f) Cropping with the ratio to be 30%. We measure the robustness according to the BER between the original watermark and the extracted one.



(a) (b) (c)

(d) (e) (f)

Figure 5. Distorted watermarked images.

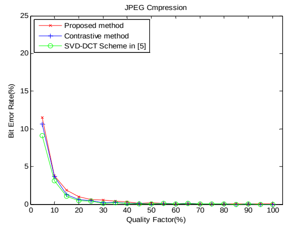
A. *Robustness against common image processing distortions*

Table I gives the different BERs of the three methods under median filtering attacks with multiple window sizes. Fig. 6 gives some results under JPEG compression and noise adding attacks. We can conclude that the three methods have similar resistance to the median filtering, JPEG compression, Additive White Gaussian Noise and Salt & Pepper Noise. All the methods can resist this kind of attacks well.

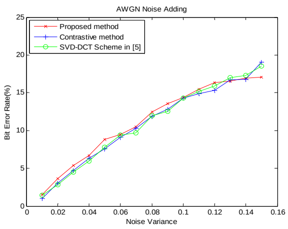
TABLE I. BERS UNDER MEDIAN FILTERING ATTACKS

Methods	**3×3**	**5×5**	**7×7**	**9×9**	**11×11**
Proposed	1.13%	6.15%	13.52%	20.64%	27.17%
Contrastive	0.99%	6.32%	12.99%	20.24%	26.88%
SVD-DCT in [5]	0.97%	6.60%	13.91%	21.28%	28.89%

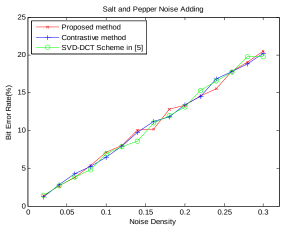
In our own method, we use image enlargement and image reduction in watermark embedding process, the quality of the image has been affected more or less, because of which the BER is a little bigger than others sometimes.



(a)



(b)

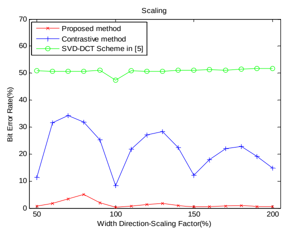


(c)

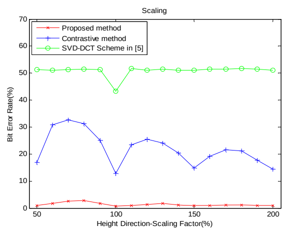
Figure 6. Comparison of BERs. (a) under JPEG compression (b) under Additive White Gaussian Noise (c) under Salt & Pepper Noise

B. Robustness against geometric distortions

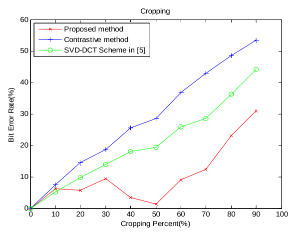
Fig. 7 (a) shows the resistance when images being scaled in the width direction while calculating each average BER with the height direction scale factor changed from 0.5 to 2.0, so do the results in Fig. 7 (b) in different directions. We can see our method has the best robustness to this kind of attack, and SVD-DCT scheme in [5] does not resist to this distortion substantially. Comparing proposed method and contrastive one, we can conclude that our method's superiority is embodied in the image enlargement process and image blocking process with the fixed number of blocks.



(a)



(b)



(c)

Figure 7. Comparison of BERs. (a) under width direction scaling (b) under height direction scaling (c) under cropping

Fig. 7 (c) shows resistance when images being cropped with different percents. We can see our method shows the best performance, but the method in [5] is worse, the main reason is the selection of the test images with size 512×512. Blocking the image by the way in [5] and embedding the watermark orderly lead to the result that the same bits will be embedded repeatly in the blocks which are in the same column, so this scheme does not resist to the cropping attacks by columns. Comparing the performances of the method in [5] and the contrastive method, we see the latter one shows the worst result. In our experiment, using the contrastive method, no matter how large the image is, we can embed only 8 times of the watermark repeatly. But using the method in [5] we can embed more bits in case of a larger image to get a better performance. According the results above, the watermark scrambling operation we proposed plays an important role in this algorithm.

IV. CONCLUSIONS

We present a novel algorithm for multi-bit watermark embedding and blind extraction. We use SVD-DCT based watermarking scheme to embed the watermark into the largest singular value of each macroblock by transforming the singular values matrixes to their DCT domains. We bring image enlargement and watermark scrambling schemes into the algorithm and block the image by fixing the number of macroblocks and subblocks. Results illustrate that our approach has pretty good resistance to many kinds of attacks, especially image scaling and cropping. The disadvantage of this method is that it doesn't resist to rotation and translation attacks, we can use this approach with template based [6] or feature points based [7] watermarking algorithm together to enhance its performance to such attacks.

ACKNOWLEDGMENT

This work has been supported by the National Sciences & Technology Supporting Program of China under Grant No.2011BAH16B01, No.2011BAH16B02, and No.2012BAH04F02; and the Cloud Computing Demonstration Project of National Development and Reform Commission.

REFERENCES

[1] Ruizhen Liu, Tieniu Tan. "A SVD-based watermarking scheme for protecting rightful ownership", IEEE Transactions on Multimedia, vol. 4, pp. 121-128, 2002.

[2] Quan Liu, Qingsong Ai. "A combination of DCT-based and SVD-based watermarking scheme", International Conference on Signal Processing, ICSP, vol. 1, pp. 873-876, 2004.

[3] Liang Liu, Qi Sun. "A new SVD-DWT composite watermarking", International Conference on Signal Processing, ICSP, vol. 4, pp. 16-20, 2006.

[4] Feng Liu, Yangguang Liu. "A watermarking algorithm for digital image based on DCT and SVD", Congress on Image and Signal Processing , CISP , vol. 1 , pp. 380-383 , 2008.

[5] Zhen Li, Kim-Hui Yap, Bai-Ying Lei. " A new blind robust image watermarking scheme in SVD-DCT composite domain", International Conference on Image Processing , ICIP , pp. 2757-2760 , 2011.

[6] Shelby Pereira, Thierry Pun. "Robust template matching for affine resistant image watermarks", IEEE Transactions on Image Processing, vol. 9, pp. 1123-1129, 2000.

[7] T. Jen-Sheng, H. Win-Bin, K. Yau-Hwang. "On the selection of optimal feature region set for robust digital image watermarking", IEEE Transactions on Image Processing, vol. 20, pp. 735-743, 2011.

[8] http://www.cs.washington.edu/research/imagedatabase/groundtruth/

[9] http://sipi.usc.edu/database/database.php?volume=misc