Journal of Information Technology and Engineering
Vol. 1 No. 2 (December, 2016)

A Modified Video Watermarking Algorithm Based on SVD in the DCT Domain

Hao-Xian WANG[1,3], Zhe-Ming LU[2] and Sheng-He SUN[3]

[1]Department of Communication Engineering, School of Information Engineering, Harbin Institute of Technology at Weihai, 2# Wenhua Xi Road, Weihai, Shandong 264209 P. R. China. *E-mail:haoxianwang@yahoo.com.cn*

[2]School of Information Science and Technology, Sun Yat-Sen University, XinGangXi Road 135, Haizhu District Guangzhou 510275, P.R. China. *E-mail: luzhem@mail.sysu.edu.cn*

[3]Department of Automatic Test and Control, Harbin Institute of Technology, Harbin,Heilongjiang 150001, P. R. China *E-mail: sunshenghe@0451.com*

Received: 13th August 2016 Revised: 24th September 2016 Accepted: 10th December 2016

Abstract: *In this paper,a modified video watermarking based on SVD in the DCT domain is proposed.First,DCT is performed on the luminance component of each cover frame; besides,the DC and low frequency components are selected and permuted to compose a coefficient matrix;then, the coefficient matrix is divided into a number of non-overlapping blocks; what's more,SVD is applied to each coefficient block; last but not least, the obtained singular values are quantized and modified according to the corresponding watermark bit. Extensive experimental results demonstrate that the proposed watermarking scheme is effective and robust against not only attacks such as frame dropping, frame averaging, and H.263 coding, but also attacks such as random cropping, adding salt & pepper noise, adding Gaussian noise, sharpening, smoothing and low-pass filtering.*

Keywords: video watermarking***,*** *DCT, SVD.*

1. INTRODUCTION

Watermarking (data hiding) [1] is the process of embedding data into a multimedia element such as an image, audio or video file.This embedded data can later be extracted from, or detected in the multimedia for security purposes. A watermarking algorithm consists of the watermark structure, an embedding algorithm, an extraction, or a detection algorithm. Watermarks can be embedded in the pixel domain or a transform domain. In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity. In all frequency domain watermarking schemes [2], there is a conflict between robustness and transparency. If the watermark is embedded in perceptually most significant components, the scheme would be robust to attacks but the watermark may be difficult to hide. On the other hand, if the watermark is embedded in perceptually insignificant components, it would be easier to hide the watermark but the scheme may be less resilient to attacks. However, transform methods including DCT and DWT attempt to decompose images in terms of a standard basis set.This is not necessarily the optimal representation for a given image, so a few years ago a third transform called singular value decomposition (SVD) was explored for watermarking [3]. SVD is an optimal matrix decomposition technique in a least square sense. It packs maximum energy into as few coefficients as possible. SVD has the ability of adapting to variations in local statistics of an image, so watermarking schemes using SVD are typically of large capacity. Reference [2] apply the DCT to the cover image, then map the DCT coefficients in a zig-zag order into four quadrants, and apply the SVD to each quadrant. The singular values in each quadrant are modified by the singular values of the DCT-transformed visual watermark. The watermark embedded in lowest frequencies is resilient to one set of attacks while embedded in highest frequencies is resilient to another set of attacks.The algorithm is non-blind.In reference [4], a semi-fragile blind watermarking method is proposed, which extracts image features from the U component of the SVD domain to generate watermarks. The watermark generation and embedding are disposed in the image itself, and the authentication for the received image needs no information about the original image or watermark. Reference [3] proposed a hybrid DWT-SVD domain watermarking scheme considering human visual properties.The host image is first decomposed into four subbands, and then the singular values of the watermark are embedded into the singular values of each subband.The embedding strength is determined by a human visual model. Reference [5] presents a block based digital image watermarking scheme that is dependent on the mathematical technique of SVD. The original image is divided into blocks, and then the watermark is embedded in

the singular values (SVs) of each block separately. This segmentation and watermarking process makes the watermark much more robust to the attacks such as noise, compression and cropping. Watermark detection is implemented by extracting the watermark from the SVs of the watermarked blocks. The algorithm in this reference [3,5] has one flaw,by comparing the experiment,we find that the watermark can be restored even if the extracted singular values of watermark is wrong. In Reference [6], the SVD is applied to the DC and low frequency DCT coefficients matrix of the randomly selected block,which belong to the luminance component of each frame,then the obtained singular values are Quantized and Modified according to the corresponding watermark bit. The algorithm in this paper is a modified one based on reference [6].

2. ALGORITHM AND IMPLEMENTATION

2.1 Watermark Embedding

Our digital watermark embedding process is divided into 9 steps and is briefly described below.

Step 1: Permute the binary watermark image by a random seed key1, supposing the watermark image size is of $k \times k$.

Step 2: Apply the DCT to the luminance component of every cover frame of the video.

Step 3: Select the DC and low frequency components of the DCT coefficients to compose a $n \times n$ matrix A,disturb the element in matrix A by a seed key 2.

Step 4: Divide the disturbed matrix A into $k \times k$ non-overlapping blocks, each including 8×8 elements.

Step 5: Apply SVD to each block, the obtained singular values are denoted as σ_i, $1 \le i \le 8$.

Step 6: Quantize σ_1 with a quantization step size Δ, and then round data to nearest integer multiples of a quantum value smoothly, i.e., $Q_\sigma = \text{round}(\sigma_1 / \Delta)$. A large quantization step size can increase the robustness of watermarking method but produce unacceptably large frame distortion.

Step 7: Modify Q_σ according to the corresponding watermark bit. If the watermark bit is 1 and $\text{mod}(Q_\sigma, 2) = 1$, then $Q_\sigma = Q_\sigma + 1$. Similarly, if the watermark bit is 0 and $\text{mod}(Q_\sigma, 2) = 0$, then $Q_\sigma = Q_\sigma + 1$. keeps unchanged for other cases.

Step 8: Obtain the modified elements of each block by the inverse SVD. Map the block back to their original positions in matrix A, map the modified coefficients back to their original positions by seed key 2.

Step 9: Apply the inverse DCT to produce the watermarked luminance component of the cover frame.Thus, we get the watermarked frame.

Repeated above steps for every frame, we can get the watermarked video.

2.2 Watermark Extraction

The watermark extraction process is as follows:

Step 1: Apply the DCT to the luminance component of the cover frame.

Step 2: Select the DC and low frequency components of the DCT coefficients to compose a $n \times n$ matrix A_w, disturb the element in matrix A_w by a seed key 2.

Step 3: Divide the disturbed matrix A_w into $k \times k$ non-overlapping blocks, each including 8 × 8 elements.

Step 4: Apply SVD to each block, the obtained singular values are denoted as, σ_{Wi} $1 \le i \le 8$.

Step 5: Use a quantization step size Δ to quantize and round σ_{W1}, if mod ($Q_{w\sigma}$, 2) = 1, then the extracted watermark bit is 0, otherwise the watermark bit is 1.

Step 6: Piece all extracted watermark bits together, and use seed key1 to retrieve the watermark image for each frame.

3. EXPERIMENTAL RESULTS

The watermark embedded is a 32×32 binary image, it is 1024 bits in length. The videos, "Waterfall", "bus", "Coastguard", in our experiment are with Common Image Format. And there are 100 frames in each video sequence. The quantization step size Δ in our tests is 120. Figures 1(a) (b) (c) (d) (e) (f) show the original and watermarked first frames

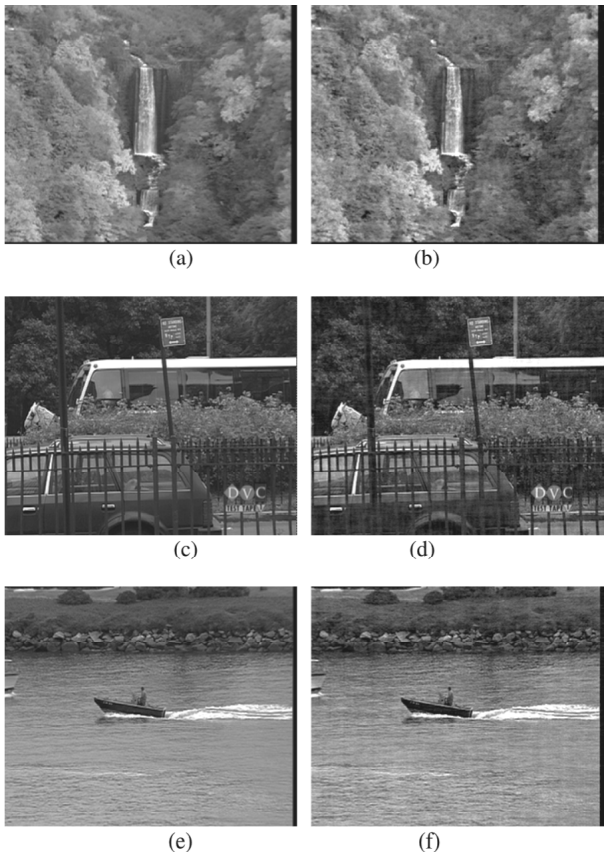
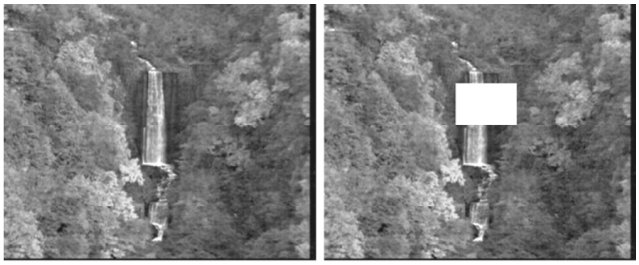


Figure 1: (a) Original first frame of "Waterfall", (b) Watermarked first frame of "Waterfall", (c) Original first frame of "Bus", (d) Watermarked first frame of "Bus", (e) Original first frame of "Coastguard", (f) Watermarked first frame of "Coastguard".

of "Waterfall", "Bus" and "Coastguard", respectively. Suppose B represents the frame averaging process between the watermarked first "Waterfall" frame and the watermarked second "Waterfall" frame, the BER of B is 0.0215, the illustrative effect of B is shown in Figure 2 (a). Suppose C represents the frame random cropping process of the watermarked first "Waterfall" frame, the BER of C is 0.1445, the illustrative effects of C is shown in Figure 2(b). Figures 3(a) (b) (c) show the original and the extracted watermarks from B and C, respectively. Table 1 shows the PSNR (Peak Signal Noise Ratio) of the first 25 watermarked frames of Video "Waterfall". Table 2 shows the maximum, minimum, and average PSNRs of 100 watermarked frames of "Waterfall", "Bus" and "Coastguard", respectively. Table 3 and table 4 shows the watermark extraction performance against the H. 263 compression attack. The results of the watermarking algorithm involving resisting the rotation, adding salt & pepper noise, adding Gaussian noise attacks, sharpening,smoothing and low-pass filtering are shown in Table 5.



(a) (b)

Figure 2: (a) The Illustrative Effect of B (b) The Illustrative Effects of C

Figure 3: (a) Original Watermark (b) Extracted Watermark under the Attack B (c) Extracted Watermark under the Attack C.

Table 1
PSNRs of the First 25 Watermarked Frames of "Waterfall"

Frame	*PSNR(dB)*				
1∼5	32.324	32.767	32.787	32.755	32.675
6∼10	32.627	32.650	32.689	32.675	32.628
11∼15	32.690	32.589	32.576	32.590	32.567
16∼20	32.650	32.706	32.657	32.681	32.695
21∼25	32.648	32.587	32.602	32.683	32.639

Table 2
Maximum, Minimum, Average PSNRs of 100 Watermarked Frames of "Waterfall", "Bus" and "Coastguard"

	Waterfall	*Bus*	*Coastguard*
Maximum	32.7870	33.2252	33.2958
Minimum	32.2017	32.4557	32.3161
Average	32.5516	32.7928	32.7389

Table 3
Average BERs of 100 Watermarked Frames of "Waterfall", "Bus" and "Coastguard"

Compression attack	*Waterfall*	*Bus*	*Coastguard*
H.263(6Mbits/s)	0.0412	0.0574	0.0497
H.263(4Mbits/s)	0.0415	0.0792	0.0500

Table 4
Performance of the 100th Watermarked Frames of "Waterfall", "Bus" and "Coastguard" Against Compression

Compression attack H.263 (4Mbits/s)	*Waterfall*	*Bus*	*Coastguard*
Extracted watermark			
BER	0.0615	0.0811	0.0645

Table 5
Performance of the Extracted Watermark from the Watermarked First "Waterfall" Frame

	Constructed watermark	*BER*
Adding Salt & pepper noise (0.05)		0.0537
Adding Gaussian noise(0.005)		0.0488
Sharpening attack		0.1650
Rotation attack(counter-clockwise 0.3°)		0.2539
Low-pass filtering (3×3)		0.2363
Smoothing attack		0.2451

4. CONCLUSIONS

According to the results in our experiment, we can see that, our algorithm is robust to attacks such as frame dropping, frame averaging, and H.263 coding. Besides, it is also robust to rotation,random cropping, adding salt & pepper noise, adding Gaussian noise, sharpening, smoothing and low-pass filtering. In addition, because the watermark is embedded into every frame of the video sequence, so it has a good performance to resist frame dropping attack.

REFERENCES

[1] I. J. Cox, M. L. Miller, and J. A. Bloom, "Digital Watermarking", Morgan Kaufmann Publishers, 2002.

[2] Alexander Sverdlov, Scott Dexter, Ahmet M. Eskicioglu, "Robust DCT-SVD Domain Image Watermarking for Copyright Protection: Embedding Data in All Frequencies", EUSIPCO2005, Antalya, Turkey, September 2005.

[3] Q. Li, C. Yuan and Y. Z. Zhong, "Adaptive DWT-SVD Domain Image Watermarking Using Human Visual Model," in ICACT2007, Feb. 12-14, 2007, pp. 1947-1951.

[4] Y. P. Hu and Z. G. Chen, "An SVD-Based Watermarking Method for Image Authentication," in Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007, pp. 1723-1728.

[5] R. Ghazy, N. El-fishawy, M. Hadhoud, M. Dessouky and F. A. El-Samie, "An Efficient Block-by-Block SVD-Based Image Watermarking Scheme," *Ubiquitous Computing and Communication Journal*, 2, 1-9 (2007).

[6] Hao-Xian Wang, Zhe-Ming Lu and Sheng-He Sun, A Blind Video Watermarking Algorithm Based on SVD in the DCT Domain, International e-Conference on Computer Science 2007.