A NEW BLIND ROBUST IMAGE WATERMARKING SCHEME IN SVD-DCT COMPOSITE DOMAIN

*Zhen Li, Kim-Hui Yap and Bai-Ying Lei**

School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore
{lizh0019,EKHYap,leib0001}@ntu.edu.sg

ABSTRACT

Digital watermarking has become an important technique for copyright protection, and various watermarking schemes have been proposed. Singular Value Decomposition (SVD) has been used as a valuable transform technique for robust digital watermarking due to some superior characteristics not obtained by DCT, DFT or DWT. In this paper, we present a new robust hybrid image watermarking scheme based on SVD and DCT. After applying SVD to the cover image blocks, we perform DCT on the macro block comprised of the first singular values (SVs) of each image block. We also developed a new method to embed the watermark in the high-frequency band of the SVD-DCT block by imposing a particular relationship between some pseudo-randomly selected pairs of the DCT coefficients. Experimental results show that the proposed watermarking method performs better than state-of-the-art SVD-based methods, and is comparable with the state-of-art wavelet-based robust image watermarking method.

Index Terms**—**Copyright Protection, Image Watermarking, SVD-DCT composite domain

1. INTRODUCTION

Digital multimedia is largely distributed today through Internet. As a result, the possibility of lossless and unlimited copies of digital contents is becoming more and more convenient. Over the last decade, digital watermarking has been proposed as a solution to the problem of copyright protection of multimedia documents in networked environments to complement cryptographic processes. Digital watermarking refers to the process of embedding digital information called watermark into a cover multimedia object such as audio, video, image and 3D models so that the watermark may be detected and extracted later to make an assertion about the object. In general, invisible watermarks can be broadly classified into two types, robust and fragile (or semi-fragile) watermarks. Robust watermarks [1-3] are generally used for copyright protection and ownership verification because they are robust to nearly all kinds of image processing operations. Fragile [4] watermarks are mainly used for content authentication and tempering location.

In recent years, some SVD-based digital image robust watermarking algorithms [1-3] have been proposed as powerful transform techniques for robust digital watermarking. This arises from the facts [2, 13] that: 1) SVs of an image are stable, i.e., when small disturbances are added to an image, the singular values still remain intact; 2) SVs represent intrinsic algebraic image properties which are intrinsic and not visual; and 3) SVD can perform decomposition on both square and rectangular matrices.

In this paper, a new watermarking method which combines the SVD and DCT is presented. As we know, the watermark should not be placed in perceptually insignificant regions of the image since many common signal and geometric processes affect these components. To address this problem, the watermark information is embedded only in the largest SVs which correspond to the energy of the most perceptually significant regions in the original image, in order to achieve high robustness against perceptivity preserving operations.

Unlike the traditional SVD-based watermarking schemes where the watermark bits are embedded directly on the SVs, the proposed scheme is based on bit embedding on the high-frequency DCT coefficients of the block of SVs obtained by SVD transformed image sub-blocks.

The rest of this paper is organized as follows. In Section 2, SVD principles are reviewed and then the proposed robust watermarking method is described in Section 3. The simulation results are shown in Sections 4. Finally, Section 5 concludes the paper.

2. REVIEW OF SINGULAR VALUE DECOMPOSITION

Singular Value Decomposition is a kind of orthogonal transforms used for matrix diagonalization. An image can be viewed as a non-negative real matrix. Let A be an image, and its size be $M \times N$. The SVD of A can be described as follows:

$$\begin{aligned}\mathbf{I} &= \mathbf{U}\mathbf{S}\mathbf{V}^T \\ &= [\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_N]\begin{bmatrix}\sigma_1 & & & \\ & \ddots & & \\ & & \sigma_R & \\ & & & \mathbf{0}\end{bmatrix}_{N\times N}\begin{bmatrix}\mathbf{v}_1 \\ \mathbf{v}_2 \\ \vdots \\ \mathbf{v}_N\end{bmatrix} \\ &= \sum_{i=1}^{R}\sigma_i \mathbf{u}_i \mathbf{v}_i^T\end{aligned} \tag{1}$$

where U and V are two $N\times N$ unitary orthogonal matrices that specify the geometry details of the cover image, and S is a $N\times N$ diagonal matrix. The elements of S are nonnegative values in a descending order.

From Eq. (1), we know that an image can be interpreted as a summation of N eigenimage. The singular value λ_i indicates the energy intensity in its corresponding eigenimage. Fig. 1 indicates the SVs obtained from the decomposition of the original Lena image, in monotonically decreasing order.

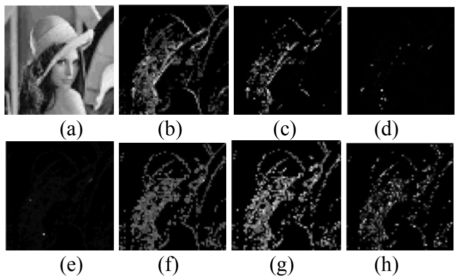

Fig. 1. Concatenated images consisting of SVs of 8×8 blocks from the cover Lena image. (a) ~ (h) the first to the eighth SVs

In SVD-based watermarking algorithms, U, S or V is modified so that the watermark information is embedded, resulting in U', S' or V', respectively and optionally. The watermarked image is constructed by

$$\mathbf{I}' = \mathbf{U}'\mathbf{S}'\mathbf{V}'^{T} = \sum_{i=1}^{R} \sigma_i' \mathbf{u}_i' \mathbf{v}_i'^{T} \quad (2)$$

3. PROPOSED SVD-DCT WATERMARKING METHOD

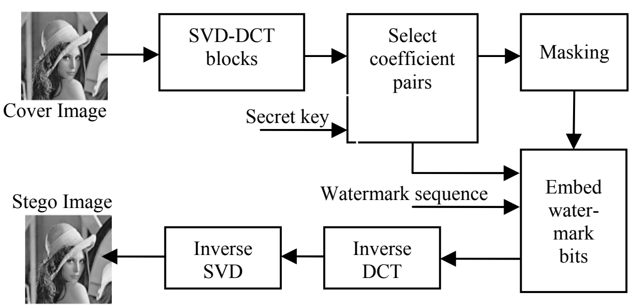

Fig. 3. Watermark embedding procedure

3.1. Watermark Embedding

The watermarking algorithm proposed here hides several bits of the watermark in every SVD-DCT block in the positions selected on a pseudo-random basis. The watermarking code is repeated over the whole image. The SVD-DCT block is acquired by the following steps:

1) Divide the cover image into non-overlapping 8×8 subblocks in the row-column order;

2) Perform SVD decomposition on each subblock and then the first singular value is obtained;

3) Concatenate the first singular values in adjacent 4×4 blocks consisting of 8×8 SVs and then a DCT block is formed.

After SVD-DCT transform, a 4×4 SVD-DCT coefficient block is acquired from a 32×32 macroblock in the cover image. A SVD-DCT block in the zigzag order is shown in Fig. 2, where the shaded positions are potential locations for watermark embedding.

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

Fig. 2. Sketch of the SVD-DCT macroblock

In Fig. 3, the sketch of the proposed watermark embedding scheme is illustrated. The watermark is embedded in the cover image through the following steps: 1) Select the coefficients pairs to be modified in the potential positions of the SVD-DCT block; 2) Compute the frequency mask; 3) Use the mask to weight the watermark amplitude; and 4) Modify the relationship between the selected coefficients pairs according to the watermark embedding rule.

To achieve an appropriate tradeoff between the robustness against filters such as JPEG compression and the imperceptibility after watermark embedding, the potential locations of macroblocks are in the high frequency band because in this work the DCT block is derived from the visual important components of the cover image (Fig. 1 (a)).

Motivated by previous works [8, 9], in this work the watermarking is achieved by changing the difference of the magnitudes of a selected pair to a predefined value. In this scheme, only 2 pairs of coefficients in the 8 potential positions in Fig. 2 are selected for embedding watermark bits. Since the attacker does not know which 2 pairs are embedded with watermark bits, attacking on all the 8 coefficients will cause intolerable distortions to the cover image.

In the embedding procedure, the difference between the magnitudes of two coefficients in a selected pairs is computed at first as follows:

$$D(x_1, y_1, x_2, y_2) = |F(x_1, y_1)| - |F(x_2, y_2)| \quad (3)$$

where F is the SVD-DCT block matrix and, (x_1, y_1) and (x_2, y_2) are the coordinates of the selected pair. Here we assume the high frequencies in the SVD-DCT block to be close enough so that $D(x_1, y_1, x_2, y_2)$ can be expected to be a zero-mean random process. Denote the modified pairs of coefficients with $F'(x_1, y_1)$ and $F'(x_2, y_2)$. The goal of the modification is that $D'(x_1, y_1, x_2, y_2)$ is positive if the watermark bit to be embedded is "1", and is negative otherwise.

The case of embedding a watermark bit "1" is as follows:

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

2) If $D(x_1, y_1, x_2, y_2) < mask$, perform the following operations if $F(x_1, y_1)$ and $F(x_2, y_2)$ are not both zero:

$$\begin{cases} F'(x_1, y_1) = sign(F(x_1, y_1)) * \\ \qquad \left[\left(|F(x_1, y_1)| + |F(x_2, y_2)| \right) / 2 + 0.5 \cdot mask \right] \\ F'(x_2, y_2) = sign(F(x_2, y_2)) * \\ \qquad \left[\left(|F(x_1, y_1)| + |F(x_2, y_2)| \right) / 2 - 0.5 \cdot mask \right] \end{cases} \quad (4)$$

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

$$\begin{cases} F'(x_1, y_1) = 0.5 \cdot mask \\ F'(x_2, y_2) = -0.5 \cdot mask \end{cases} \tag{5}$$

The parameter *mask* in Eq. (4) and (5) is the frequency mask for changing the watermarking strength according to the sharpness of the image macroblocks.

For embedding a bit of "0", the embedding mechanism is the same as embedding "1", but the positions of $F(x_1, y_1)$ and $F(x_2, y_2)$ in Eq. (4) and (5) are swapped, so that the newly computed difference $D'(x_1, y_1, x_2, y_2)$ will be negative. For each 32×32 macroblock, 2 watermark bits will be embedded since 2 pairs of embedding positions are selected.

After the watermark embedding, inverse DCT is performed on the modified SVD-DCT blocks, and then the blocks consisting of 4×4 SVs are reconstructed. Only the first SVs of the original 8×8 blocks contain watermark information, and other SVs are kept unchanged. The final stego image *I'* is the concatenation of the inverse SVD of the SVs blocks.

Since blocks with edge characteristics often have a lot of frequency components, the parameter *edge* is introduced to reduce artifacts: *edge* is the sum of the absolute values of the DCT-coefficients of indexes 9-16 that represent the higher DCT frequencies as marked in Fig. 2. High values in these components in blocks of the first SVs indicate that the macroblocks have edge characteristics. To determine the level of tolerance against distortions caused by the watermark embedding, a linear model is made as follows:

$$mask = \alpha \cdot edge + \beta \tag{6}$$

where the parameter α is for controlling the local embedding of the watermark, and β is needed for a base strength of the watermark in order to resist the effect of the rounding and truncation operations in the spatial domain. The parameter edge is formulated as follows:

$$edge = \sum_{i=9}^{16} |F(i)| \tag{7}$$

3.2 Optimization of the Watermarking Parameters

We use PSNR of 42dB as the balancing point for enough visual imperceptibility and high robustness against various attacks in the watermarking process. Through experiments, we observe that: 1) Assume we fix the PSNR value of stego image, if we increase α, then β must be decreased, and vice versa; 2) α is more efficient than β in terms of the robustness. So the optimal parameters α and β for an image can be formulated as follows:

$$\begin{cases} \alpha_{\max}(\mathbf{I}) = \arg\max_{\alpha} E(\alpha, \beta, \mathbf{I})\big|_{\beta=0} \\ \beta_{\max}(\mathbf{I}) = \arg\max_{\beta} E(\alpha, \beta, \mathbf{I})\big|_{\alpha=0.6\cdot\alpha_{\max}(\mathbf{I})} \end{cases} \tag{8}$$

where $E(\alpha, \beta, \mathbf{I}) = \{(\alpha, \beta) : \text{PSNR}(\alpha, \beta, \mathbf{I}) = 42\,\text{dB}\}$.

So the optimal parameters can be chosen by optimizing the following object function:

$$\left(\alpha^*(\mathbf{I}), \beta^*(\mathbf{I})\right) = \arg\min_{(\alpha,\beta)} \left\{ \|\boldsymbol{W} - \boldsymbol{W}'\|_2^2 + \lambda \left|\text{PSNR}(\alpha, \beta, \mathbf{I}) - 42\right| \right\} \tag{9}$$

where W' is the extracted watermark under the JPEG compression with quality 15, and the optimal parameters are chosen by the random gradient search method.

3.3. Watermark Extraction

The watermark extraction procedure is simple as follows:

1) Retrieval the positions of the coefficients pairs in each SVD-DCT block, according to the secret key, the image characteristics, and the positions of different SVD-DCT blocks, as in the watermark embedding procedure;

2) The difference between coefficients of each selected pair is computed:

$$D^*(x_1, y_1, x_2, y_2) = |F^*(x_1, y_1)| - |F^*(x_2, y_2)| \tag{10}$$

where $F^*(x_1, y_1)$ and $F^*(x_2, y_2)$ are the selected pairs of coefficients that might be watermarked;

3) Sum the values of different $D^*(x_1, y_1, x_2, y_2)$ corresponding to all pairs of coefficients where the same bit is repeatedly embedded:

$$B_i' = \sum_{\Phi_i} D^*(x_1, y_1, x_2, y_2) \tag{11}$$

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

4) The extracted bit is judged as follows:

$$W_i' = \begin{cases} 1 & if\ B_i' \ge 0 \\ 0 & if\ B_i' < 0 \end{cases} \tag{12}$$

4. EXPERIMENTAL RESULTS AND DISCUSSIONS

To check the robustness of the proposed algorithm, we perform various attacks on the watermarked image, including some typical content-preserving image processing and geometric attacks. Some comparisons with the watermarking schemes in MWT & EMD [3] (state-of-the-art wavelet-based method) and pure SVD [7] (state-of-the-art SVD-based method) [7] are also presented. In order to make fair comparisons, we embed the same random watermark with 64 bits repeatedly to fill up the capacity, which is also the case in [3]. All the experimental results are evaluated 10 times and the average result is reported. All the attacks used in the experiments are provided by StirMark Benchmark 4. The smaller area under the PSNR-BER curve is, the better the watermarking method is. Note that the BER values are not low since we use very heavy attacks in order to compare the robustness of the watermarking methods. In order to provide a statistical assessment, we use images in volume 3 of USC-SIPI Image Database [10]. The volume contains 44 miscellaneous images, including the popularly used Lena, Pepper, etc. All the images are preprocessed to be of size 512*512 and in gray format. The PSNR-BER curves reported in each subsection is the average of all the 44 curves. In terms of computational cost, the execution time for each of the test images by pure SVD and SVD & DCT is about 1s and 5s, respectively. In contrast, the execution time of MWT & EMD is about 5 minutes.

4.1 Robustness against JPEG Lossy Compression

As shown in Fig. 4 (a), compared with the pure SVD, the BER values dramatically increased under higher JPEG compression ratios and, compared with MWT & EMD, the performance is similar: although the BER values are a little bit higher than MWT & EMD within the range of 6 to 8 of JPEG quality.

4.2 Robustness against Gaussian Noise

As shown in Fig. 4 (b), under zero-mean Gaussian noises, the performances of SVD & DCT and MWT & EMD methods are comparable, and much better than the pure SVD method.

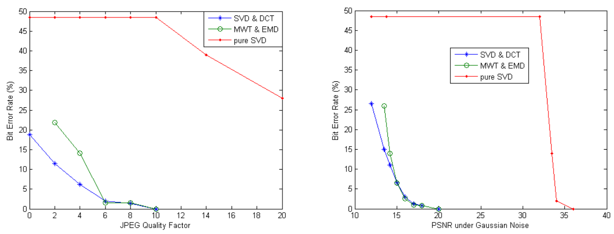

Fig. 4. Comparison of BERs. (a) under JPEG compression (b) under Gaussian noise attack.

4.3 Robustness against Median Filtering and Sharpening

From Table 1, we can see that the proposed method is obviously better than the pure SVD method, and is normally better than the MWT & EMD method in most cases. The BER of the extracted watermark under sharpening attacks for MWT & EMD, SVD and SVD & DCT are 0.19, 32.15, and 0.02, respectively.

TABLE 1. BERs under Median Filter Attacks

Median Filter Size	MWT & EMD	SVD	SVD & DCT
3×3	0	26.10	0
5×5	9.76	41.36	4.82
7×7	12.89	47.76	13.09
9×9	51.21	49.56	27.39

4. 4 Robustness against the Geometric Distortion Attack

From Table 2, it is obvious that the proposed method is more robust than the pure SVD method and the MWT & EMD method. The comparisons between the proposed method and the pure SVD method for cropping attacks and resizing attacks are shown in Table 3 and Table 4, respectively.

TABLE 2. BERs under Rotation Attacks

Rotation angles	-0.5°	-0.25°	0.25°	0.5°
MWT & EMD	45.36	7.03	7.19	44.95
SVD	37.65	25.74	23.53	39.26
SVD & DCT	23.12	4.09	4.92	22.84

TABLE 3. BERs under Cropping Attacks

Copping Percentage	50%	60%	80%	95%
MWT & EMD	0	13.17	42.74	48.44
SVD	0	19.26	49.53	50.24
SVD&DCT	0	8.58	15.12	32.19

TABLE 4. BERs under Resizing Attacks

Resizing	512-250-512	512-200-512	512-150-512	512-100-512
MWT & EMD	0	9.89	38.35	46.12
SVD	0	19.22	47.15	49.94
SVD & DCT	0	8.58	15.16	31.53

5. CONCLUSIONS

In this paper, a novel, yet simple, hybrid SVD-DCT domain watermarking scheme for image copyright protection is presented. The watermark detection is also efficient and blind. Our experiments show that, compared to state-of-the-arts methods, the proposed scheme is highly robust against some typical general content-preserving attacks and geometric distortion attacks. Future works may include incorporating wavelet analysis to further improve the PSNR-BER performance.

6. REFERENCES

[1] J. J. K. O'Ruanaidh, W. J. Dowling, and F. M. Boland, "Watermarking digital images for copyright protection," in Proc. *Inst. Elect. Eng.*, vol. 143, no. 4, pp. 250-256, 1996.

[2] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673-1687, 1997.

[3] Ning Bi, Qiyu Sun, Daren Huang, Zhihua Yang, Jiwu Huang, "Robust Image Watermarking Based on Multiband Wavelets and Empirical Mode Decomposition," *IEEE Transactions on Image Processing*, Vol. 16, no. 8, pp. 1956 -1966, 2007.

[4] C. C. Chang, C. C. Lin, Y. S. Hu, An SVD oriented watermark embedding scheme with high qualities for the resorted images, *International Journal of Innovative Computing, Information and Control*, Vol. 3, pp. 609-620, 2007.

[5] H.C. Andrews and C.L. Patterson, "Singular Value Decompositions and Digital Image Processing," *IEEE Trans. ASSP*, pp. 26-53, 1976.

[6] P. S. L. M. Barreto, H.Y. Kim, and V. Rijmen, "Toward secure public-key blockwise fragile authentication watermarking," in *Proc. Inst. Elect. Eng.*, vol. 149, no. 2, pp. 57-62, 2002.

[7] R. Liu, T. Tan, An SVD-based watermarking scheme for protecting rightful ownership, *IEEE Transactions on Multimedia,* Vol. 4, pp. 121-128, 2002.

[8] E. Koch and J. Zhao, "Toward robust and hidden image copyright labeling", *IEE Workshop Nonlinear Signal and Image Processing*, pp. 452-455, 1995.

[9] R. L. Lagendijk, Gerrit C. Langelaar and Reginald L. Lagendijk, "Optimal Differential Energy Watermarking of DCT Encoded Images and Video", *IEEE Transactions on Image Processing*, Vol. 10, pp. 148-158, 2001.

[10] The USC-SIPI Image Database Volume 3, http://sipi.usc.edu/database/database.php?volume=misc