A Nonoblivious Image Watermarking System Based on Singular Value Decomposition and Texture Segmentation

Soroosh Rezazadeh, and Mehran Yazdi

Abstract**—**In this paper, a robust digital image watermarking scheme for copyright protection applications using the singular value decomposition (SVD) is proposed. In this scheme, an entropy masking model has been applied on the host image for the texture segmentation. Moreover, the local luminance and textures of the host image are considered for watermark embedding procedure to increase the robustness of the watermarking scheme. In contrast to all existing SVD-based watermarking systems that have been designed to embed visual watermarks, our system uses a pseudo-random sequence as a watermark. We have tested the performance of our method using a wide variety of image processing attacks on different test images. A comparison is made between the results of our proposed algorithm with those of a wavelet-based method to demonstrate the superior performance of our algorithm.

Keywords**—**Watermarking, copyright protection, singular value decomposition, entropy masking, texture segmentation.

I. Introduction

WATERMARKING is the process of embedding data into multimedia products such as images, audios and videos. This embedded data can later be detected or extracted from the multimedia for the proof of ownership or other purposes. There are three main issues in the design of a watermarking system: watermark structure, embedding algorithm, and extraction algorithm [1]. Most robust watermarks have been inserted in the pixel domain or in the transform domain. The SVD is one of the transforms that have been employed for the image watermarking. Some SVD-based watermarking systems are global schemes. Authors in [2] have proposed a global scheme that showed a good robustness and can embed visual watermarks or a pseudo-random sequence. However their method is completely inapplicable for copyright protection applications and cannot detect the true watermarks [3]. Another global scheme has been recently proposed by [4] and [5] which used a combination of other transforms such as DWT, DCT, and PCA. It seems that this scheme is inapplicable too due to the fact that embedding only the singular values of the watermark, that contain little information about the watermark, in the host image does not give a reliable clue to extract the true watermark. Moreover singular values of most images are highly correlated and consequently any watermark can be extracted from the watermarked image. Other strategies such as [6] and [7] applied the above schemes on blocks of the host and watermark images instead of whole images. It should be noted that there are schemes that did not use these concepts. For example, in [8] the host image is partitioned into non-overlapping blocks of size 4×4 and SVD of each block is computed and then the largest singular value of each block is quantized to embed one bit of the watermark image. However, using this approach, we are limited to use the watermarks with the certain size.

The above discussion reveals that using visual watermarks aren't appropriate for SVD-based watermarking systems. So we propose a new SVD-based watermarking system that uses pseudo-random Gaussian sequences as watermarks and prevents any false alarm on the watermark detection. Moreover, for having high transparency along with robustness, the local characteristics of the host image are employed during the watermarking procedure.

The rest of this paper is organized as follows. In section 2 SVD transform is briefly described. The proposed watermarking system is introduced in section 3. In section 4, the experimental results of the proposed method and comparison with a wavelet-based method are shown. The conclusions are brought in the last section.

II. SVD Preliminary

SVD is one of the numerical analysis tools used to analyze matrices. In SVD transform, a matrix can be decomposed into three matrices that have the same size as the original matrix. Let A be an image matrix of size $N{\times}N$ and with rank r, such that $r \leq N$. The matrix A can be decomposed as:

$$A = U \times S \times V^{\mathrm{T}} = [u_1, u_2, ..., u_N] \times \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_N \end{bmatrix} \times [v_1, v_2, ..., v_N]^{\mathrm{T}} = \sum_{i=1}^{r} \lambda_i u_i v_i^{\mathrm{T}} \tag{1}$$

Manuscript received April 30, 2006.

S. Rezazadeh is with the Department of Electrical and Electronic Engineering, School of Engineering, Shiraz University, Shiraz, Iran (e-mail: sorooshir1@yahoo.com).

M. Yazdi is with the Department of Electrical and Electronic Engineering, School of Engineering, Shiraz University, Shiraz, Iran (phone: 918-711-6239056; fax: 918-711-6287294; e-mail: yazdi@shirazu.ac.ir).

where U and V are called left and right singular vectors and are orthogonal matrices such that $U^TU=I$, $V^TV=I$. S is a $N\times N$ diagonal matrix whose elements (λ's) are singular values of A.

It is important to note that each singular value specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image layer [8]. We use this concept to develop our algorithm.

III. Proposed Watermarking Method

In the proposed scheme, the host image A is a grayscale image with size of $N\times N$ and the watermark X consists of a sequence of real numbers with Gaussian distribution such that:

$$X=\{x_1,x_2,\ldots,x_n\} \tag{2}$$

where each element x in X is drawn independently according to $N(0,1)$ (Normal distribution with mean=0 and variance=1). The steps of the algorithm are as follows.

A. Entropy Masking

In our proposed approach we take into consideration the local properties of the image and the features of the human visual system. Because the higher complexity and uncertainty can be found in high entropy regions of an image [9], an image containing a lot of redundancy in its pixel values has weak entropy and vice versa. This higher complexity leads the human eye to be less sensitive to the modifications in the areas with higher entropy. So, embedding watermarks in such regions allows for higher energy to get embedded. Authors in [10] and [11] have developed an entropy masking model in the DCT domain and proved that this concept can be efficiently used to increase the robustness of image and video watermarks. In fact, the entropy masking can be used to quantify texture contents of image regions [12] which completely match with previous definitions that state; human visual system is less sensitive to textured areas of an image (spatial masking). Consequently, we use this entropy masking model to segment the host image textures as follows.

First we compute the entropy image A_e. Each pixel of the entropy image A_e is obtained by calculating the entropy of an 9-by-9 neighborhood around the corresponding pixel in the host image A based on the following equation:

$$E = -\sum_{i=0}^{L-1} p(z_i)\log p(z_i) \tag{3}$$

where z denotes image gray levels and L is the number of gray levels. After computing the entropy image A_e we scale its pixel values between zero and one. In the next step we create a binary texture image (A_t) by thresholding the rescaled image to segment the texture areas (here we have used a threshold value of 0.8). By applying this procedure we can determine regions in the image that are less sensitive to human eye.

B. Embedding Scheme

For the digital watermark embedding process, we firstly divide the host image into a set of non-overlapping 8×8 sub-blocks A_k ($1 \le k \le N^2/64$). Then a pseudo-random number generator is used to select a certain number (n) of sub-blocks for the watermark embedding. The initial seed is saved in a key file for extraction process. This causes not only the watermark to be scattered over the image but also a secret key comes to hand. In the next step, we apply SVD on the selected sub-blocks and insert the watermark by the following embedding formula:

$$\lambda'_{\;,k} = \lambda_{\;,k} \times (1+\beta(k)x_k) \tag{4}$$
$$\beta(k) = \alpha T(k)$$

where $\lambda_{max,k}$ is the largest singular value of the block k and α is a scaling factor. For calculating $T(k)$ regarding the texture image A_t we count the number of texture points in each sub-block and then a certain distortion value between 6 and 14 is given to each block. These values are obtained based on our experiments on a trade off between the robustness and transparency. In this way, large values indicate that the corresponding block is highly textured and is also watermarked with higher strength. This embedding formula embeds the watermark with respect to singular values of blocks that also represent the luminance of the image. So luminance masking has been utilized automatically. After the watermark insertion we replace the selected sub-blocks in their original order to obtain watermarked image A'.

C. Extraction Process

In watermark detector, the host image is needed and the watermark is extracted by reversing the watermark embedding steps. To determine if the extracted watermark X' match with original watermark X we measure the similarity of X and X' by [13]:

$$sim(X, X') = X'\cdot X / \|X'\|_2 \tag{5}$$

and then compare it with a threshold T^*(=6). Setting the threshold T^*=6 makes the probability of detecting a wrong watermark very small.

IV. Experimental Results

In order to verify the validity of the proposed watermarking scheme we choose a watermark of length n=1000. A set of gray-level images of 512×512 pixels of "Lena", "Liftingbody", "Goldhill", and "Barbara" images (shown in Fig. 1a, 1b, 1c, and 1d) are used as the host images. For watermarking of host images we adjusted a scaling factor for each case in order to have approximately the same PSNR about 49.5 dB in all cases. The watermarked images are shown in Fig. 2e, 2f, 2g, 2h. As we can see, there are no blocking artifacts or visual degradations in the watermarked images. To specify the steps of our algorithm, the entropy image A_e, the texture image A_t, and an amplified version of the difference image between the watermarked and host images are shown in Fig. 2 for the "Lena" image. For the sake of space, we have not brought the results for other images. Next, in order to put the performance evaluation of our algorithm in a proper context, we compared our method with the wavelet-based method of [14]. This wavelet-based method performs two levels of decomposition on the host image by using "Haar" wavelet and then adds the watermark to the largest coefficients that are not located in the lowest resolution (excluding the LL_2 subband). The watermarked images with the wavelet method also have the same PSNR of 49.5 dB. We tested the robustness of our system under six common image processing attacks; 1) adding Gaussian noise with mean of zero and variance of 0.01, 2) 5×5 median filtering, 3) 16×16 Gaussian low-pass filtering with standard deviation of 0.5, 4) JPEG compression with quality factor of 15 (Compression Ratio≈26), 5) image scaling to its quarter size using "Bicubic" interpolation, and 6) 3×3 sharpening. The similarity comparison results are shown in Tables 1, 2, 3, and 4 for different test images. As we can see from these tables our method detects the watermark very well in all cases. Excluding the case of AWGN for the image "Barbara", our scheme performs much superior than the wavelet method.

Performance of wavelet method becomes very close to our scheme with the AWGN attack for textured images. However from the tables, it can be seen that in a high PSNR the wavelet method fails in most cases while our algorithm can detect the watermark well.

V. Conclusion

In this paper, we introduced a new approach for watermarking of still images based on SVD. The local characteristics of the image are considered for the watermark embedding. In contrast to all SVD-based methods we used a different type of watermarks in our system which prevents any false alarm on the watermark detection. Results showed that the proposed system is very robust against image processing attacks and it has a very high transparency.

References

[1] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," Proceedings of the IEEE, vol. 87, no. 7, pp. 1079-1107, 1999.

[2] R. Liu and T. Tan, "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership," *IEEE Transactions on Multimedia*, vol. 4, no. 1, pp. 121-128, Mar. 2002.

[3] X.P. Zhang and K. Li, "Comments on "An SVD-based watermarking scheme for protecting rightful Ownership"," *IEEE Transactions on Multimedia*, vol. 7, no. 2, pp. 593-594, April 2005.

[4] D.V.S. Chandra, "Digital Image Watermarking Using Singular Value Decomposition," *Proceedings of 45th IEEE Midwest Symposium on Circuits and Systems*, Tulsa, Oklahoma, USA, vol. 3, pp. 264-267, Aug. 2002.

[5] Y.D. Chung and C.H. Kim, "Robust Image Watermarking Against Filtering Attacks," SICE Annual Conference, Fukui, Japan, vol. 3, pp. 3017-3020, Aug. 2003.

[6] T. Xianghong, Y. Lianjie, and L. Lu, N. Yamei, "Study on a Multifunction Watermarking Algorithm," *Proceedings of IEEE 7th International Conference on Signal Precessing*, vol. 1, pp. 848-852, Sept. 2004.

[7] T. Xianghong, Y. Lianjie, Y. Hengli, and Y. Zhongke, "A Watermarking Algorithm Based on the SVD and Hadamard Transform," *Proceedings of IEEE International Conference on Communications, Circuits and Systems*, vol. 2, pp. 874-877, 2005.

[8] V.I. Gorodetski, L.J. Popyack, V. Samoilov, and V.A. Skormin, "SVD-Based Approach to Transparent Embedding Data into Digital Images," *International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security*, St. Petersburg, Russia, vol. 2052, pp. 263-274, May 2001.

[9] A. B. Watson, R. Borthwick, and M. Taylor, "Image Quality and Entropy Masking," *Proceedings of SPIE on Human Vision and Electronic Imaging*, Vol. 3016, pp. 2-12, 1997.

[10] S. Suthaharan, S. W. Kim, H. K. Lee, and S. Sathananthan, "Perceptually Tuned Robust Watermarking Scheme for Digital Images," *Pattern Recognition Letters*, vol. 21, no. 2, pp. 145-149, 2000.

[11] S. W. Kim, S. Suthaharan, "An Entropy Masking Model for Multimedia Content Watermarking," *IEEE International Conference on System Sciences*, 2004.

[12] R. C. Gonzalez, R. E. Woods, "Digital Image processing," Second Edition, Prentice Hall Inc, 2002.

[13] I. J.Cox, J. Killian, F. T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*,vol. 6, no. 12, pp. 1673-1687, 1997.

[14] X. G. Xia, C. G. Boncelet, and G. R. Arce, "Wavelet Transform Based Watermark for Digital Images," *Optics Express*, vol. 3, no. 12, pp. 497-511, Dec. 1998.

TABLE I
Similarity Measurement for Host Image of Lena

Attacks	Our method	Method in [14]
Median	15.6791	2.0401
Gaussian LPF	14.9507	5.1558
Scaling	28.1705	4.9587
JPEG	14.7919	8.3556
AWGN	9.8098	7.9903
Sharpening	9.7355	6.8856

TABLE II
Similarity Measurement for Host Image of Liftingbody

Attacks	Our method	Method in [14]
Median	22.1977	0.5026
Gaussian LPF	14.1440	1.2991
Scaling	29.9485	1.3317
JPEG	17.4451	4.7477
AWGN	12.7278	6.2398
Sharpening	11.3974	6.0549

TABLE III
Similarity Measurement for Host Image of Goldhill

Attacks	Our method	Method in [14]
Median	11.6842	0.0753
Gaussian LPF	12.1693	2.5375
Scaling	26.7145	2.5016
JPEG	11.2204	6.7440
AWGN	7.8860	7.8739
Sharpening	8.9214	8.4760

TABLE IV
Similarity Measurement for Host Image of Barbara

Attacks	Our method	Method in [14]
Median	10.2005	1.1449
Gaussian LPF	8.2720	2.3709
Scaling	21.8638	1.8719
JPEG	14.0905	8.0043
AWGN	7.0198	10.0095
Sharpening	8.5780	2.4072

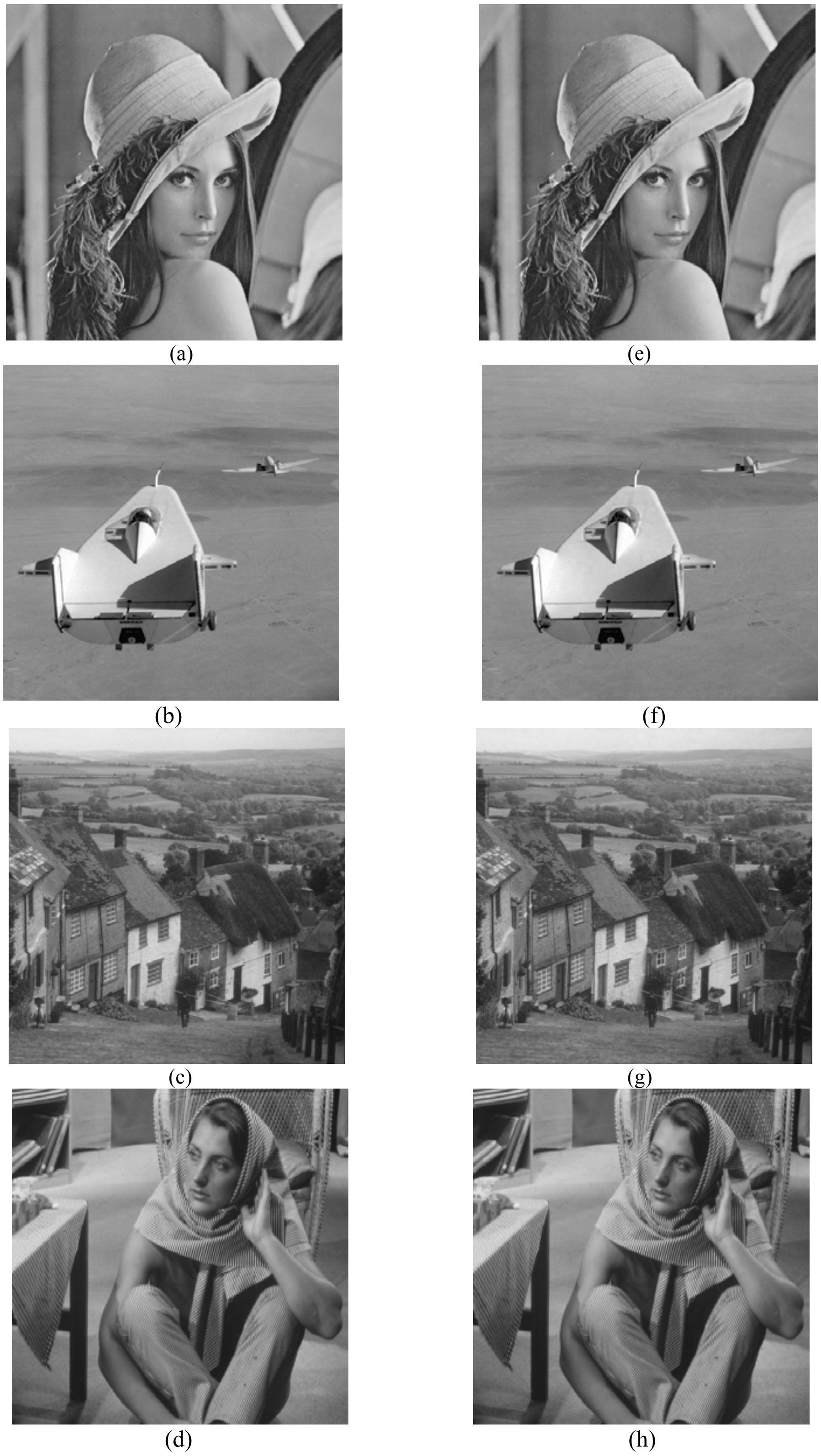
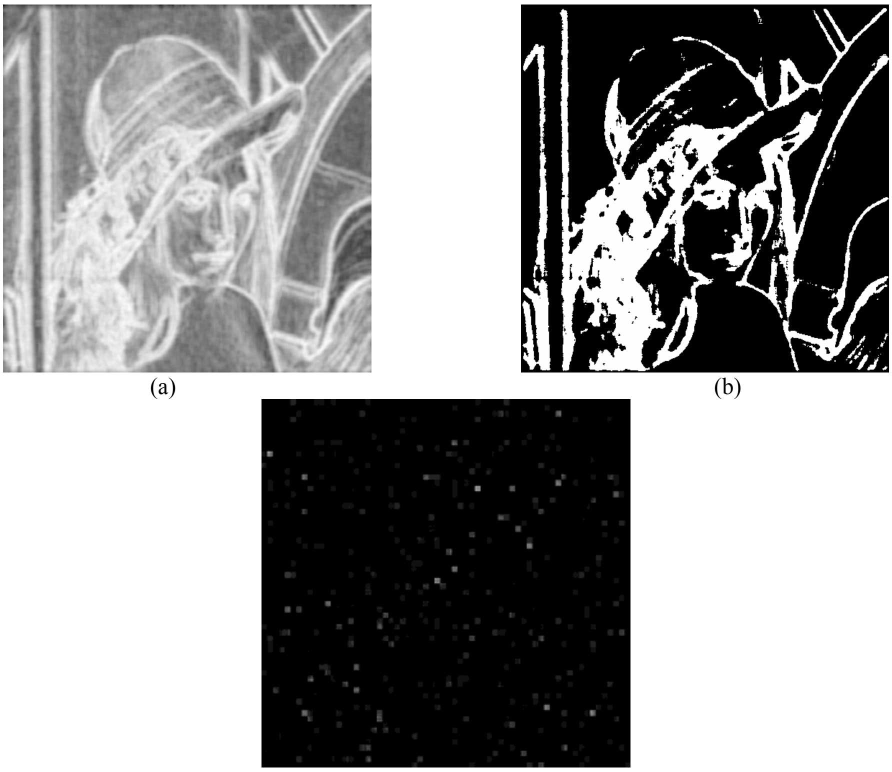


Fig. 1 host images; (a) Lena (b) Liftingbody (c) Goldhill (d) Barbara and watermarked images (PSNR=49.5 dB) for (e) Lena (f) Liftingbody (g) Goldhill (h) Barbara



(a)

(b)

(c)

Fig. 2 for Lena image; (a) entropy image A_e (b) texture image A_t (c) amplified difference image by factor 20.