Progress In Electromagnetics Research B, Vol. 8, 147–159, 2008

PERFORMANCE EVALUATION OF BLOCK BASED SVD IMAGE WATERMARKING

R. A. Ghazy

Department of Electronics and Electrical Communications
Faculty of Electronic Engineering
Menoufia University
32952, Menouf, Egypt

M. M. Hadhoud

Department of Information Technology
Faculty of Computers and Information
Menoufia University
32511, Shebin Elkom, Egypt

M. I. Dessouky

Department of Electronics and Electrical Communications
Faculty of Electronic Engineering
Menoufia University
32952, Menouf, Egypt

N. A. El-Fishawy

Department of Computers Engineering
Faculty of Electronic Engineering
Menoufia University
32952, Menouf, Egypt

F. E. Abd El-Samie

Department of Electronics and Electrical Communications
Faculty of Electronic Engineering
Menoufia University
32952, Menouf, Egypt

Abstract—This paper presents a block based digital image watermarking algorithm that is dependent on the mathematical technique of singular value decomposition (SVD). Traditional SVD watermarking already exists for watermark embedding on the image as a whole. In the proposed approach, the original image is divided into blocks, and then the watermark is embedded in the singular values (SVs) of each block, separately. The watermark embedding on a block-by-block basis makes the watermark more robust to the attacks such as noise, compression, cropping and lowpass filtering as the results reveal. The watermark detection is implemented by extracting the watermark from the SVs of the watermarked blocks. Extracting the watermark from one block at least is enough to ensure the existence of the watermark.

1. INTRODUCTION

The spreading use of digital multimedia nowadays has made copyright protection a necessity. Authentication and information hiding have also become important issues. To achieve these issues, watermarking technology is used. Several researchers have worked in the field of watermarking for its importance [1–11]. The work in this field has led to several watermarking techniques such as the correlation-based techniques, the frequency domain techniques and the wavelet domain techniques [2].

Watermarking means embedding a piece of information into a multimedia content, such as a video, an audio or an image in such a way that it is imperceptible to a human observer, but easily detectable by a computer [1]. Before the emergence of digital image watermarking, it was difficult to achieve copyright protection, authentication and data hiding, but now it is easy to achieve these goals using watermarking techniques. Every watermarking algorithm consists of an embedding algorithm and a detection algorithm.

Embedded watermarks may have several properties such as robustness, fidelity, and tamper-resistance [1]. The robustness means that the watermark must be robust to transformations that include common signal distortions such as digital-to-analogue conversion, analogue-to-digital conversion, and lossy compression. Fidelity means that the watermark should be neither noticeable to the viewer nor degrading for the quality of the content. Tamper-resistance means that the watermark is often required to be resistant to signal processing algorithms. These properties depend on the application. The watermark can be embedded in the spatial domain or in a transform

domain [2].

The SVD mathematical technique provides an elegant way for extracting algebraic features from an image. The main properties of the SVs matrix of an image can be exploited in image watermarking. This matrix has a good stability. When a small perturbation occurs in an image, the variation of its SVs can be neglected [3, 4]. Using this property of the SVs matrix of an image, the watermark can be embedded to this matrix without a large variation in the obtained image.

Liu et al. have proposed an SVD based watermarking scheme, in which, the watermark is added to the SVs of the whole image or a part of it [3]. A single watermark is used in this scheme which may be lost due to attacks. To avoid this disadvantage, we propose an approach, in which, the original image is segmented into blocks and the watermark is added to the SVs of each block. The SVs of the watermarked blocks are used to extract the watermark after the attacks. As a result of using several watermarked blocks, several watermarks can be recovered. So, if any attack affects the watermarked image, some of the watermarks will survive. This block-by-block method gives robustness against JPEG compression, cropping, blurring by a lowpass filter, Gaussian noise, resizing and rotation as the results will reveal. The watermark can be either a pseudo-random number, or an image. In this paper, the watermark used is an image.

This paper is organized as follows. Section 2 briefly explains the SVD-based watermarking scheme. Section 3 introduces the proposed scheme. Section 4 introduces the experimental results. Section 5 gives the conclusion.

2. THE THRADITIONAL SVD WATERMARKING ALGORITHM

The SVD of an image is computed to obtain two orthogonal matrices U, V and a diagonal matrix S [7]. In the approach proposed by Liu et al. [3], the watermark W is added to the matrix S. Then, a new SVD process is performed on the new matrix $S + kW$ to get U_w, S_w and V_w, where k is the scale factor that controls the strength of the watermark embedded to the original image. Then, the watermarked image F_w is obtained by multiplying the matrices U, S_w, and V^T. The steps of watermark embedding are summarized as follows:

1. The SVD is performed on the original image (F matrix).

$$F = USV^T \tag{1}$$

2. The watermark (W matrix) is added to the SVs of the original

image (S matrix).

$$D = S + kW \tag{2}$$

3. The SVD is performed on the D matrix.

$$D = U_w S_w V_w^T \tag{3}$$

4. The watermarked image (F_w matrix) is obtained using the modified SVs (S_w matrix).

$$F_w = U S_w V^T \tag{4}$$

To extract the possibly corrupted watermark from the possibly distorted watermarked image, given the U_w, S, V_w matrices and the possibly distorted image F_w^*, the above steps are reversed as follows:

1. The SVD is performed on the possibly distorted watermarked image (F_w^* matrix).

$$F_w^* = U^* S_w^* V^{*T} \tag{5}$$

2. The matrix that contains the watermark is computed.

$$D^* = U_w S_w^* V_w^T \tag{6}$$

3. The possibly corrupted watermark is obtained.

$$W^* = (D^* - S)/k \tag{7}$$

The * means corruption due to attacks.

3. THE PROPOSED BLOCK-BASED SVD WATERMARKING ALGORITHM

3.1. Watermark Embedding

In this algorithm, the original image (F matrix) is divided into nonoverlapping blocks. The watermark is embedded to the SVs (S matrix) of each block giving new SVs matrices. An SVD is performed on each of these new SVs matrices to get the SVs matrices of the watermarked blocks. Then, these SVs matrices are used to build the watermarked blocks. By rearranging these blocks again into one matrix of the same dimensions as the original image, the watermarked image F_w is built in the spatial domain. The steps of the embedding process can be summarized as follows:

1. Divide the original image (F matrix) into non-overlapping blocks.

2. Perform the SVD on each block (B_i matrix) to obtain the SVs (S_i matrix), where $i = 1, 2, 3, \ldots, N$, and N is number of blocks.

$$B_i = U_i S_i V_i^T \tag{8}$$

3. Add the watermark (W matrix) to the S_i matrix of each block. The watermark W is of the same size as that of each block.

$$D_i = S_i + kW \tag{9}$$

4. Perform the SVD on each D_i matrix to obtain the SVs of each watermarked block (S_{wi} matrix).

$$D_i = U_{wi} S_{wi} V_{wi}^T \tag{10}$$

5. Use the SVs of each block (S_{wi} matrix) to build the watermarked blocks in the spatial domain.

$$B_{wi} = U_i S_{wi} V_i^T \tag{11}$$

6. Rearrange the watermarked blocks back into one matrix to build the watermarked image in the spatial domain (F_w matrix).

3.2. Watermark Detection

Having the U_{wi}, V_{wi}, S_i matrices and the possibly distorted image F_w^*, we can follow the steps mentioned below to get the possibly corrupted watermark.

1. Divide the possibly corrupted watermarked image (F_w^* matrix) into blocks having the same size used in the embedding process.

2. Performs the SVD on each possibly corrupted watermarked block (B_{wi}^* matrix) to obtain the SVs of each one (S_{wi}^* matrix).

$$B_{wi}^* = U_i^* S_{wi}^* V_i^{*T} \tag{12}$$

3. Obtain the matrices that contain the watermark using the U_{wi}, V_{wi} and S_{wi}^* matrices.

$$D_i^* = U_{wi} S_{wi}^* V_{wi}^T \tag{13}$$

4. Extract the possibly corrupted watermark (W^* matrix) from the D_i^* matrices.

$$W_i^* = (D_i^* - S_i)/k \tag{14}$$

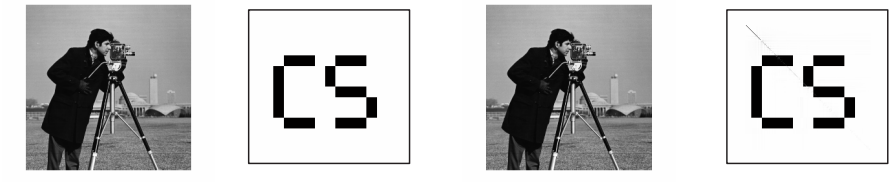
The detection of the watermark in a single block is enough to ensure the existence of this watermark in the image. This increases the detection probability of the watermark in the presence of attacks.

4. EXPERIMENTAL RESULTS

In this section, several experiments are carried out to compare between the method of Liu and the proposed method for image watermarking. The 256×256 cameraman image is used as the original image. Figure 1 shows the original image, the watermark of the same size as the original image, the watermarked image, and the extracted watermark without any attacks using the method of Liu. A single watermark is used and the correlation coefficient c_r between the extracted watermark and the original one is 0.8308. Figure 2 shows the original image, the watermark added to each block, the watermarked image, the extracted watermarks and the extracted watermark with the maximum correlation coefficient with the original watermark in the absence of any attacks. The extracted watermark which gives the $c_{rmax} = 0.9975$ is magnified in the figure. The correlation coefficients between the original watermark and the watermarks extracted from each block in the image using the proposed method are indicated in Fig. 2(f). The size of each block used in our experiments is 16×16. Different block sizes can be used. Figure 2(f) indicates that the correlation coefficient is higher than 0.5 for all extracted watermarks. This ensures the ability of the proposed algorithm to extract the watermarks perfectly in the absence of any attacks. Notice also that there is no visual difference between the original image and the watermarked image and this ensures the fidelity of the proposed method.

Other experiments are carried out on the watermarked images with some attacks such as Gaussian noise, blurring, cropping, JPEG compression, rotation and resizing. Figures 3 and 4 show the watermarked images with some attacks for both the method of Liu and the proposed method, respectively. The major problem encountered with the attacks is the process of watermark extraction which is studied in Figs. 5 and 6.

The first attack applied is the addition of Gaussian noise with zero mean and 0.01 variance. The second attack is blurring of the image



(a) (b) (c) (d)

Figure 1. (a) Original image. (b) Watermark. (c) Watermarked image without attacks. (d) Extracted watermark with $c_r = 0.8308$.

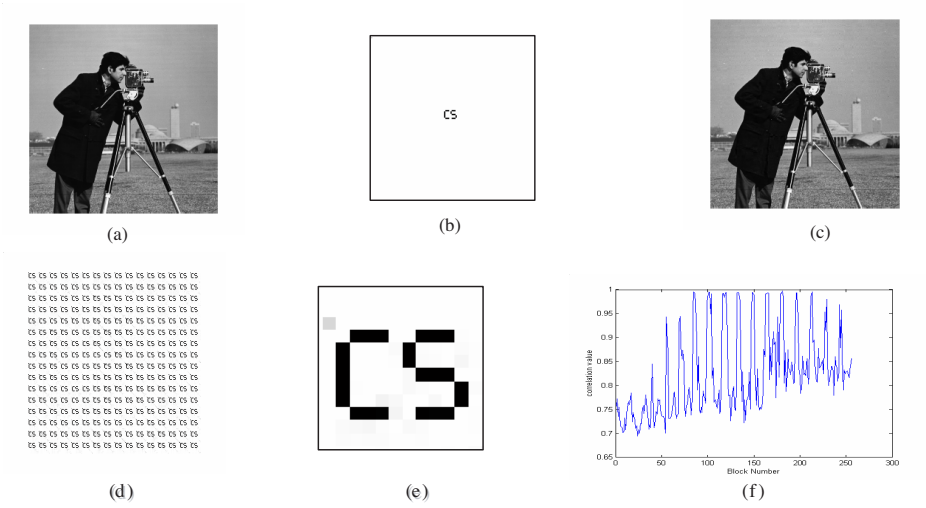


Figure 2. (a) Original image. (b) Watermark embedded in each block. (c) Watermarked image without attacks. (d) Extracted watermarks from each block. (e) Zooming of the extracted watermark which has $c_{rmax} = 0.9975$ (f) Correlation coefficient between each extracted watermark and the original one.

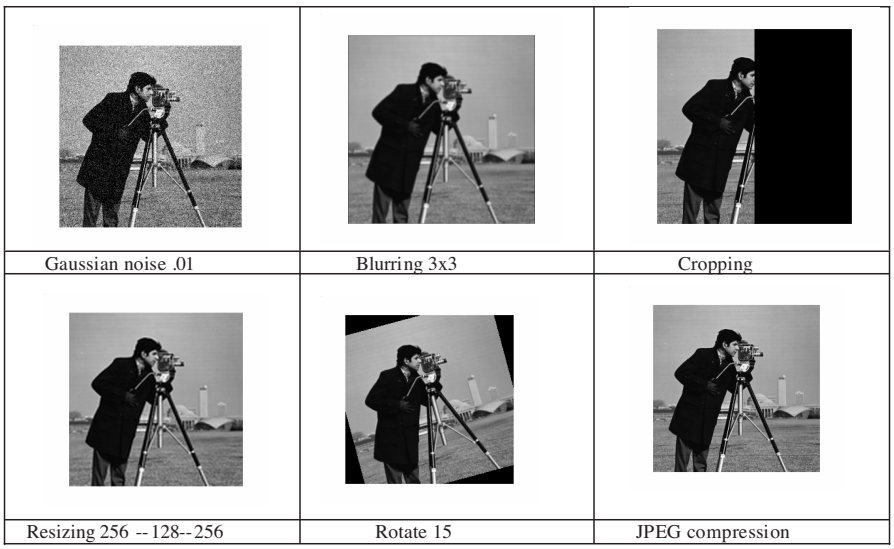


Figure 3. Attacks on the image watermarked by the method of Liu.

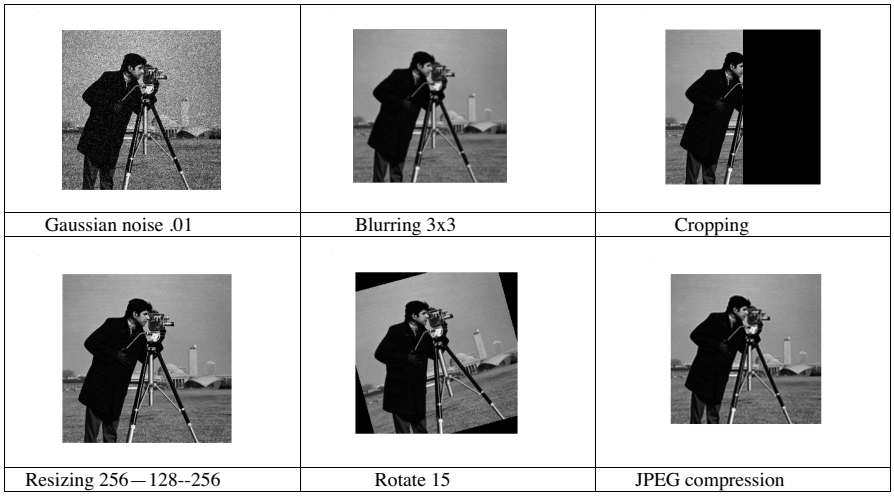


Figure 4. Attacks on the image watermarked by the proposed method.

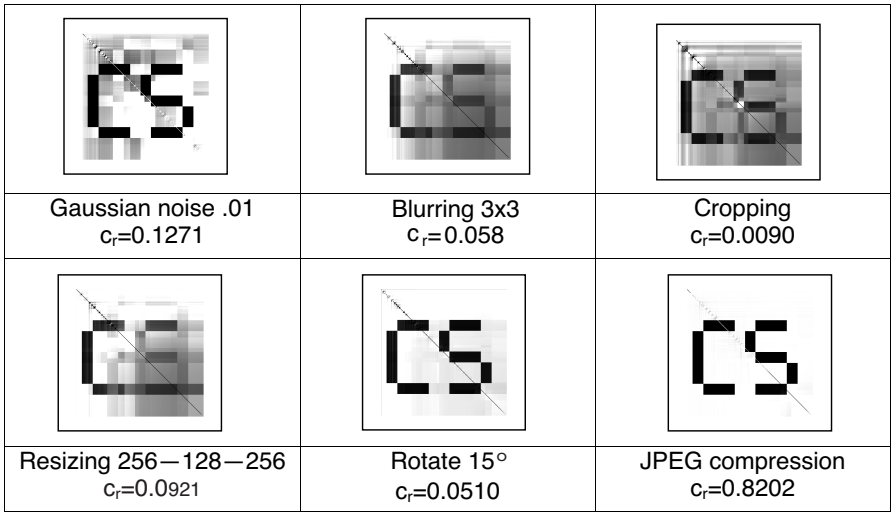
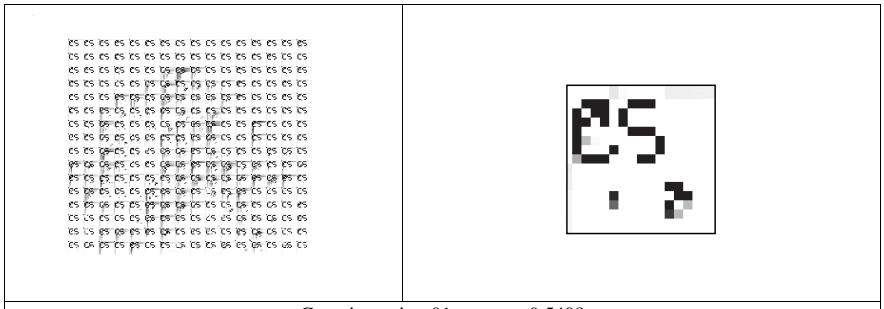
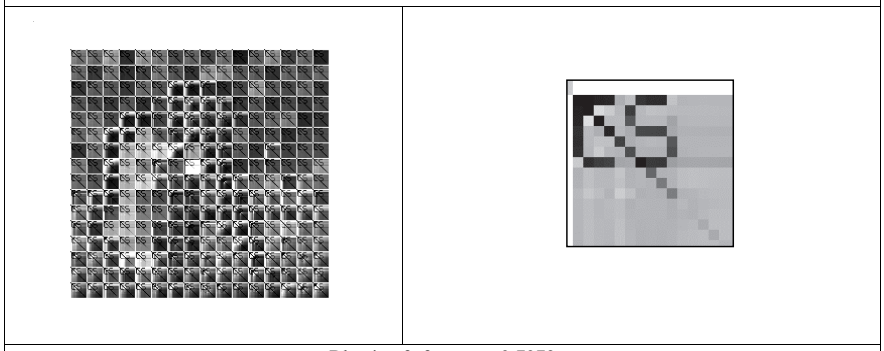


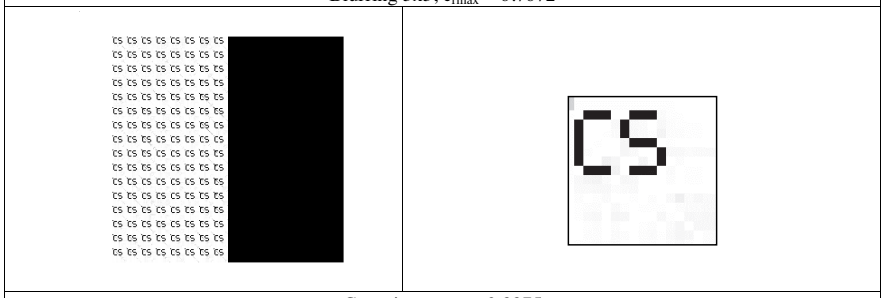
Figure 5. Extracted watermarks for the method of Liu in the presence of attacks



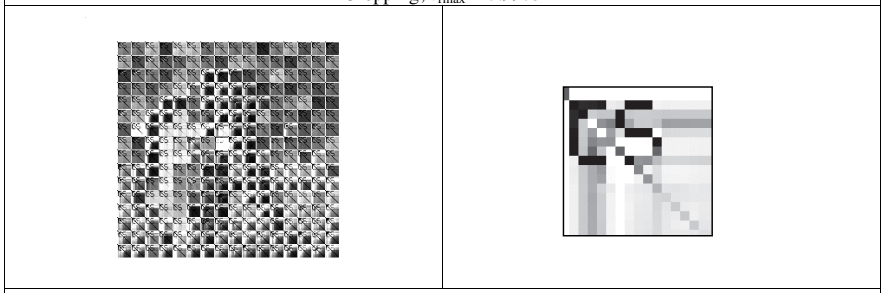
Gaussian noise .01, $c_{rmax} = 0.5408$



Blurring 3x3, $c_{rmax} = 0.7072$



Cropping, $c_{rmax} = 0.9975$



Resizing 256—128—256, $c_{rmax} = 0.5435$

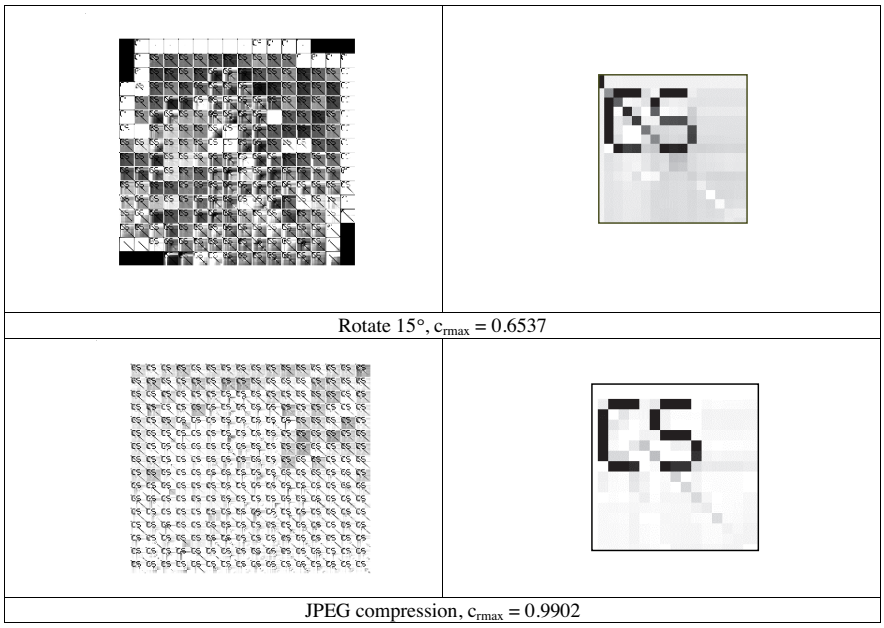


Figure 6. Extracted watermarks for the proposed method in the presence of different attacks. Left: the extracted watermark from each block. Right: magnification of the block that achieves maximum correlation with the original watermark.

by a lowpass filter of 3×3 window. The third attack is cropping half of the watermarked image. The fourth attack is JPEG compression. The fifth attack is rotation by 15°. The sixth attack is resizing. Figure 5 shows the extracted watermarks for the different attacks and the correlation coefficient between each extracted watermark and the original watermark for the method of Liu. The results reveal that the value of c_r is less than 0.5 for each attack except for the compression attack.

Figure 6 shows the extracted watermarks for the proposed algorithm after applying the same attacks. The extracted watermark which gives c_{rmax} with the original watermark is magnified in the figure. In all cases, there are some extracted watermarks with c_r higher than 0.5 which ensures the existence of the watermark. Tables 1 and 2 show the superiority of the proposed method to the method of Liu in the presence of a Gaussian noise attack and a lowpass filtering attack, respectively.

Figure 7 shows the relation between the noise variance and

Table 1. Correlation coefficients between the detected watermarks and the original one for both the proposed method and the method of Liu in the presence of a Gaussian noise attack.

Noise Variance	0.001	0.005	0.01	0.05	0.1	0.5	1
c_{r1max} (proposed)	0.6100	0.5802	0.5667	0.5207	0.4661	0.4362	0.4377
c_{r2} (Liu method)	0.3665	0.1641	0.1267	0.0854	0.0779	0.0700	0.0688
No of blocks with $c_r \geq 0.5$ (proposed)	13	8	4	1	0	0	0
No of blocks with $c_r \geq 0.4$ (proposed)	95	21	14	10	9	3	2

Table 2. Correlation coefficients between the detected watermarks and the original one for both the proposed method and the method of Liu in the presence of a lowpass filtering attack.

Lowpass filter Window size	3	4	5	6
c_{r1max} (proposed)	00.7072	0.5430	0.6618	0.5736
c_{r2} (Liu method)	0.0596	0.0372	0.0261	0.0191
No of blocks $c_r \geq 0.5$	13	2	1	2
No of blocks with $c_r \geq 0.4$	16	8	3	2

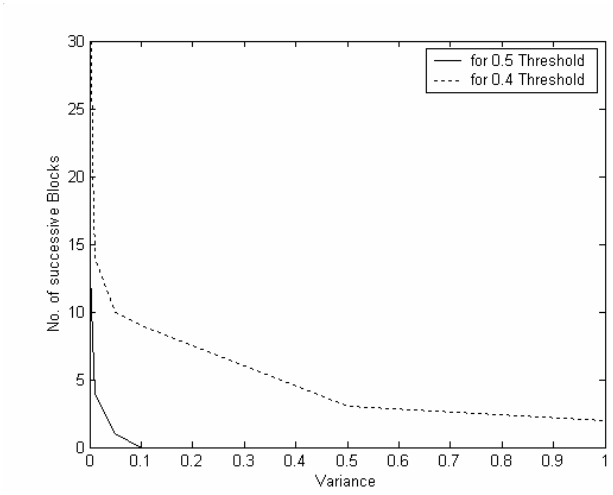


Figure 7. Relation between the noise variance and the number of blocks that have extracted watermarks with a correlation coefficient higher than the threshold value.

the number of successfully extracted watermarks for the proposed method in the presence of a Gaussian noise attack using 0.5 and 0.4 thresholds, respectively. Notice that the number of successfully extracted watermarks is inversely proportional to the value of the threshold.

5. CONCLUSION

This paper presents a visually undetectable, robust watermarking algorithm. This algorithm depends on embedding the watermark into the SVs of the original image after dividing it into blocks. The experimental results show that the proposed Block-by-Block SVD-watermarking algorithm has a high fidelity and robustness in the presence of different types of attacks. The results reveal also the superiority of the proposed algorithm to the traditional SVD watermarking algorithm.

REFERENCES

1. Miller, M. L., I. J. Cox, J. M. G. Linnartz, and T. Kalker, "A review of watermarking principles and practices," *IEEE International Conference on Image Processing*, 1997.
2. Shoemaker, C. and Rudko, "Hidden bits: A survey of techniques for digital watermarking," Independent Study EER-290 Prof. Rudko, Spring 2002.
3. Liu, R. and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. on Multimedia*, Vol. 4, No. 1 March 2002.
4. Wang, Y. H., T. N. Tan, and Y. Zhu, "Face verification based on singular value decomposition and radial basis function neural network," National Laboratory of Pattern Recognition (NLPR), Institute of Automation, Chinese Academy of Sciences.
5. Ganic, E. and A. M. Eskicioglu, "A DFT-BASED semi-blind multiple watermarking scheme images," CUNY Brooklyn College, 2900 Bedford Avenue, Brooklyn, NY 11210, USA.
6. Tewfik, A. H., "Watermarking digital image and video data," *IEEE Signal Processing Magazine*, September 2000.
7. Sverdlov, A., S. Dexter, and A. M. Eskicioglu, "Robust DCT-SVD domain image watermarking for copyright protection: Embedding data in all frequencies," *Proceedings of the 13th European Signal Processing Conference*, 2005.

8. Petitcolas, F. A. P., R. J. Anderson, and M. G. Kuhn, "Information hiding — A survey," *Proceeding of the IEEE*, Vol. 87, No. 7, July 1999.
9. Lin, C. Y., M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, scaling, and translation resilient watermarking for images," *IEEE Transactions on Image Processing*, Vol. 10, No. 5, May 2001.
10. Shieh, J. M., D. C. Lou, and M. C. Chang, "A semi-blind watermarking scheme based on singular value decomposition," *Computer Standards & Interface*, Vol. 28, 428–440, 2006.
11. Xiao, L., Z. H. Wei, and H. Z. Wu, "Ridgelet-based robust and perceptual watermarking for images," *IJCSNS International Journal of Computer Science and Network Security*, Vol. 6, No. 2B, February 2006.