# AN EFFICIENT BLOCK-BY-BLOCK SVD-BASED IMAGE WATERMARKING SCHEME

**R. A. Ghazy [#], N. A. El-Fishawy[#], M. M. Hadhoud[$], M. I. Dessouky[#] and F. E. Abd El-Samie[#]**
# Dept. of Electronics and Elect. Communications., Fac. of Electronic Eng., Menoufia Univ., 32952, Menouf , EGYPT.
[$] Dept. of Inform. Tech., Faculty of Computers and Information , Menoufia Univ., 32511, Shebin Elkom , EGYPT.
E-mails:
eng_rasg@yahoo.com, nelfishawy@hotmail.com, mmhadhoud@yahoo.com and fathi_sayed@yahoo.com

**ABSTRACT**

This paper presents a block based digital image watermarking scheme 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. This segmentation and watermarking process makes the watermark much more robust to the attacks such as noise, compression, cropping. Watermark detection is implemented by extracting the watermark from the SVs of the watermarked blocks. Experiments show that extracting the watermark from one block at least is enough to ensure the existence of the watermark.

**Keywords**: Image Processing, Watermarking, Singular Value Decomposition.

## 1 INTRODUCTION

The spreading 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 correlation-based techniques, frequency domain techniques, DFT based techniques and DWT based techniques [2].

Watermarking means embedding a piece of information into multimedia content, such as video, audio or images in such a way that it is imperceptible to a human observer, but easily detected by a computer or detector [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.

Watermarking has 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-analog, analog-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. The existence of these properties depends on the application. The watermark can be embedded in the spatial domain or in the transform domain [2].

The SVD mathematical technique provides an elegant way for extracting algebraic features from an image. The main properties of the SVD matrix of an image can be exploited in image watermarking. The SVD matrix of an image has good stability. When a small perturbation is added to an image, large variation of its SVs does not occur [3], [4]. Using this property of the SVD matrix of an image, the watermark can be embedded to this matrix without 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 apart 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 in a modified manner. The SVs of the modified

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, Gaussian noise, resizing and rotation as the results will reveal. The watermark can either be 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 and section 5 gives the concluding remarks.

## 2 TRADITIONAL SVD-BASED IMAGE WATERMARKING

The SVD of an image is computed to obtain two orthogonal matrices U and V and a diagonal matrix S [7]. In the approach proposed by Liu et al., the watermark W is added into the matrix S then a new SVD process is performed on the new matrix S+kW to get $U_w$, $S_w$ and $V_w$ [3]. 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).

$$F=USV^T \quad (1)$$

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

$$D=S+kW \quad (2)$$

3. The SVD is performed on the new modified matrix (D matrix).

$$D=U_wS_wV_w^T \quad (3)$$

4. The watermarked image ($F_w$ matrix) is obtained by using the modified matrix ($S_w$ matrix).
5. 

$$F_w=US_wV^T \quad (4)$$

To extract the possibly corrupted watermark from the possibly distorted watermarked image, given $U_w$, 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).

$$F^*_w=U^*S^*_wV^{*T} \quad (5)$$

2. The matrix that includes the watermark is computed.

$$D^*=U_wS^*_wV_w^T \quad (6)$$

3. The possibly corrupted watermark is obtained.

$$W^*=(D^*-S)/k \quad (7)$$

The * refers to the corruption due to attacks.

## 3 THE PROPOSED WATERMARKING APPROACH

### 3.1 Watermark Embedding:

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

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

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

$$B_i=U_iS_iV_i^T \quad (8)$$

4. Add the watermark image (W matrix) to the S matrix of each block.

$$D_i=S_i+kW \quad (9)$$

5. Perform SVD on each $D_i$ matrix to obtain the SVs of each ($S_{wi}$ matrix).

$$D_i=U_{wi}S_{wi}V_{wi}^T \quad (10)$$

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

$$B_{wi}=U_i S_{wi} V_i^T \quad (11)$$

7. 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 $U_{wi}$, $V_{wi}$, $S_i$, matrices and possibly distorted image $F^*_w$, we can follow the steps mentioned below to get the possibly corrupted watermarks.

1. Divide the watermarked image ($F^*_w$ matrix) into blocks having the same size used in the embedding process.
2. Performs SVD on each watermarked block ($B^*_{wi}$ matrix) to obtain the SVs of each one ($S^*_{wi}$ matrix).

$$B^*_{wi}=U_i * S^*_{wi} V_i *^T \quad (12)$$

3. Obtains the matrices that contain the watermark using $U_{wi}$, $V_{wi}$, $S^*_{wi}$, matrices.

$$D^*_i= U_{wi} S^*_{wi} V_{wi}^T \quad (13)$$

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

$$(D^*_i - S_i)/k = W^*_i \quad (14)$$

## 4 EXPERIMENTAL RESULTS

In this section several experiments are carried out to compare between the methods of Liu et al. and the proposed approach. The 256x256 cameraman image is used to be watermarked. Figure 1 shows the original image, the watermark, the watermarked image, and the extracted watermark using Liu method. A single watermark is used. Figure 2 shows the original image, the block based watermark, the watermarked image and extracted watermark. The block of extracted watermarks which gives maximum correlation with the original watermark block is magnified in the figure. The correlation coefficients between the original transmitted watermark block and the watermark 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 but this size is moderate having small complexity. 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 difference between the original image and the watermarked image using the human eye, enforcing the fidelity of this method.

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

The first attack applied is Gaussian noise with zero mean and 0.01 variance. The second attack is blurring using a low pass filter of 3x3 window. The third attack is cropping half of the watermarked image. The fourth attack is JPEG compression. The fifth attack is rotation by 15 degree. The sixth attack is resizing from size 256×256 to 128×128 and then to 256×256. Figure (5) shows the extracted watermark and the correlation coefficient between each extracted watermark and the original watermark for the method of Liu. The results reveal that the value of the correlation coefficient is less than 50% for extracted watermarks under attacks except for the compression attack.

Figure (6) shows the extracted watermarks for the proposed algorithm after applying the same attacks we applied on Liu method. The extracted watermark giving the maximum correlation coefficient with the original watermark block is zoomed out in the figure, and the maximum correlation coefficient value is shown. In all cases, there is some blocks with correlation coefficient higher than 50% ensuring the existence of the watermark. Table (1) gives correlation coefficient results after applying Gaussian noise attacks with different values of noise variance. The table gives the highest correlation and number of extracted watermark blocks with correlation coefficients higher than the predetermined threshold for 0.5 and 0.4 thresholds. Similarly, Table (2) gives correlation coefficient results after applying lowpass filtering attacks with filters of different window sizes. Correlation (1) refers to the maximum correlation obtained by the proposed method and correlation (2) refers to the correlation obtained by Liu method. These results reveal the ability of the proposed algorithm to extract watermarks even in the presence of severe attacks.

Figure (7) shows the relation between different values of noise variance and the number of successfully extracted blocks using 0.5 and 0.4 thresholds, respectively. Notice that the number

of successive extracted blocks is inversely proportional to the value of the threshold.

## 5. CONCLUSION

This paper presents a visually undetectable, robust watermarking scheme. The proposed 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-Based method gives fidelity and robustness against Gaussian noise, cropping and JPEG compression. In the future work, the detection system will be extended to more transform domain watermarking approaches such as DWT- SVD and DCT-SVD.

## 6 REFERENCES

[1] M. L. Miller, 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] C. Shoemaker, Rudko, "Hidden Bits: A Survey of Techniques for Digital Watermarking" Independent StudyEER-290 Prof Rudko, Spring 2002.

[3] R. liu and T. tan, "An SVD-Based Watermarking Scheme for protecting rightful ownership", IEEE Trans. on multimedia, Vol. 4, no. 1 March 2002.

[4] Y. H. Wang, 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] E. Ganic and A. M. Eskicioglu, "A DFT-BASED Semi-Blind multiple watermarking scheme images", CUNY Brooklyn College, 2900 Bedford Avenue, Brooklyn, NY 11210, USA.

[6] A. H. Tewfik, "Watermarking digital image and video data ", IEEE Signal processing magazine, September 2000.

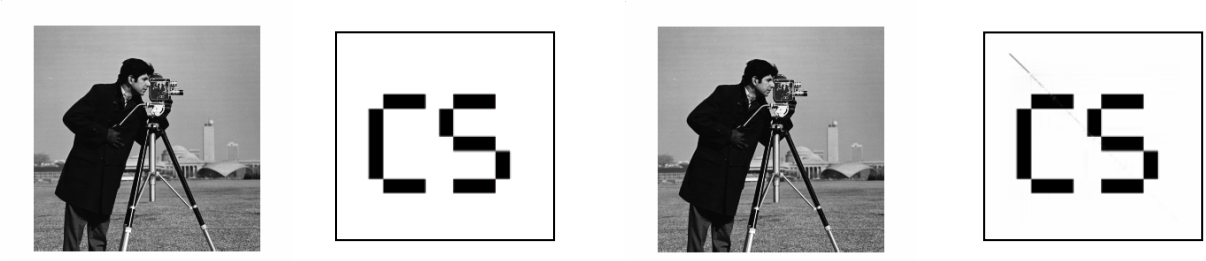
[7] A. Sverdlov, S. Dexter, A. M. Eskicioglu, "Robust DCT-SVD domain image watermarking for copyright protection: embedding data in all frequencies"

[8] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information hiding—A survey", Proceeding of the IEEE, Vol. 87, No. 7, July 1999.

[9] C. Y. Lin, 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] J. M. Shieh, D. C. Lou, and M. C. Chang, "A semi-blind watermarking scheme based on singular value decomposition", computer standards & interface 28 (2006) 428-440.

[11] W.Jinwel, L.Guanglle, D.Yuewel, W.Zhiquan, "Correlation detection system of watermarking based on HVS"



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

**Figure (1)** (a) Original image. (b) Watermark. (c) Watermarked image. (d) Extracted watermark given correlation coefficient=0.8308.

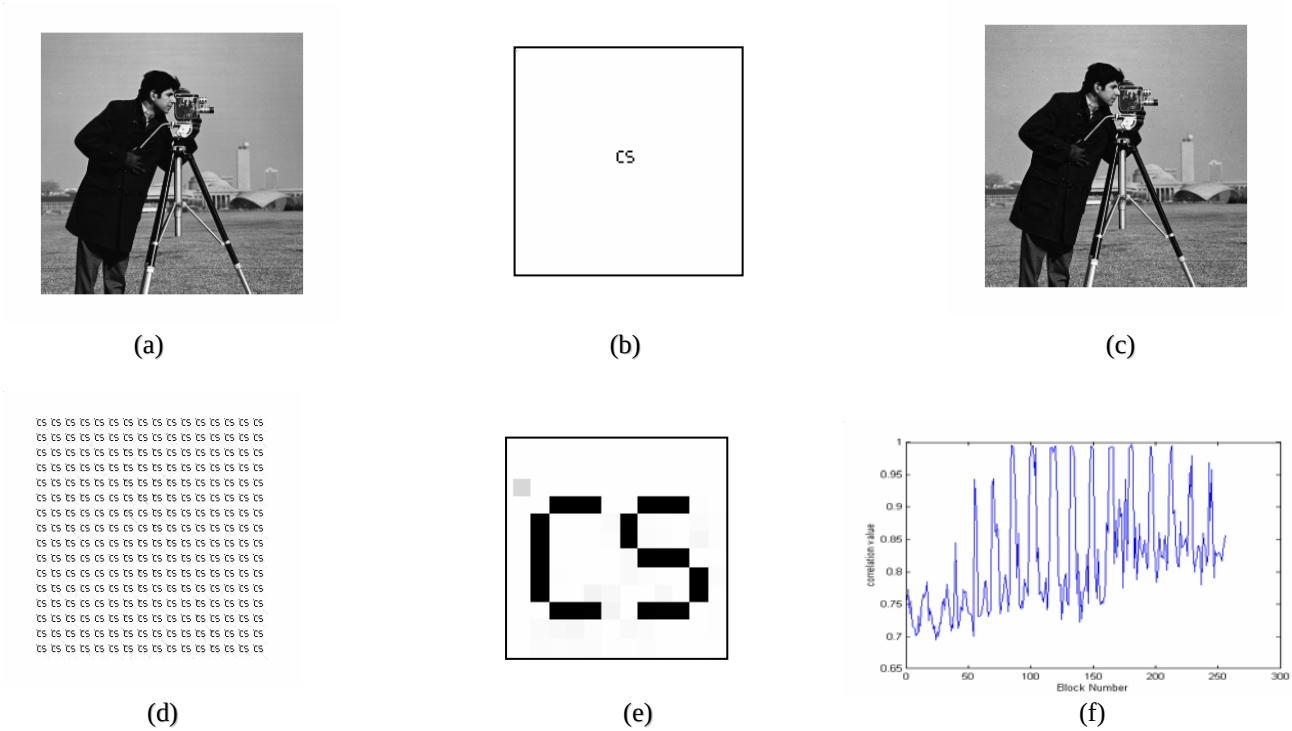



**Figure (2)** (a) Original image. (b) Watermark image. (c) Watermarked image. (d) Extracted watermark images. (e) The extracted watermark which give maximum correlation, after zooming it out. (f) Watermark correlation coefficients (max. correlation=0.9975).

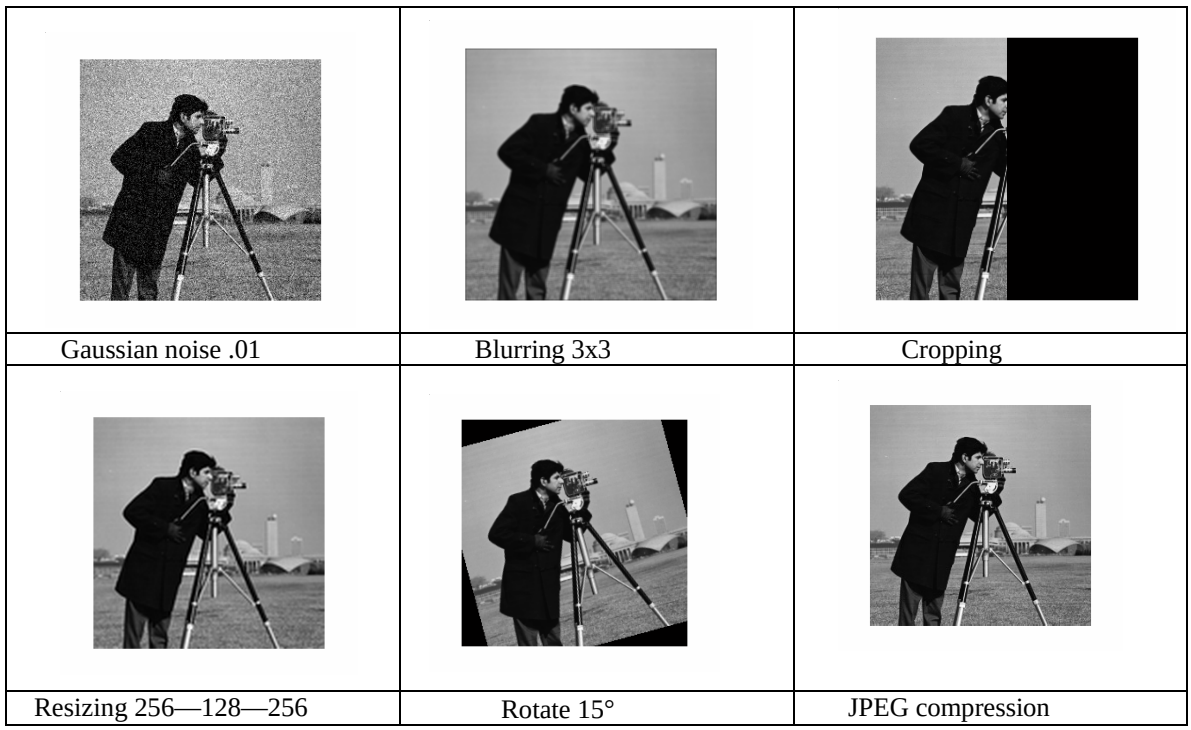



**Figure (3)** Attacked watermarked images for Liu method

| | | |
|---|---|---|
|  |  |  |
| Gaussian noise .01 | Blurring 3x3 | Cropping |
|  |  |  |
| Resizing 256—128—256 | Rotate 15° | JPEG compression |

**Figure (4)** Attacked watermarked images for the proposed method

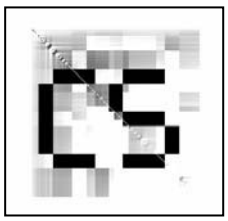
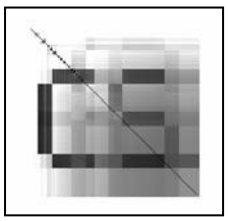
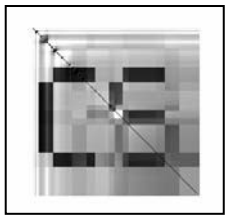
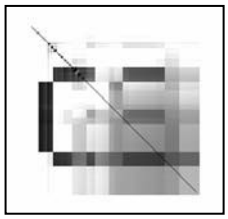
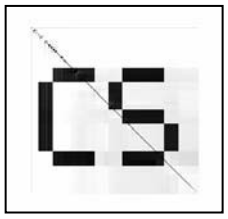
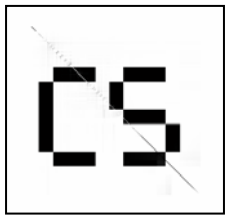
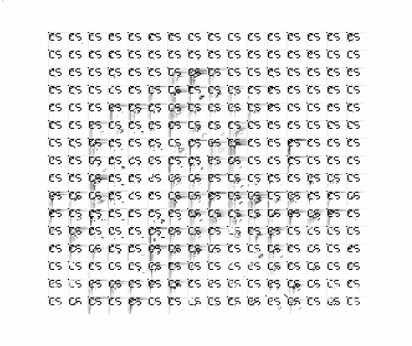
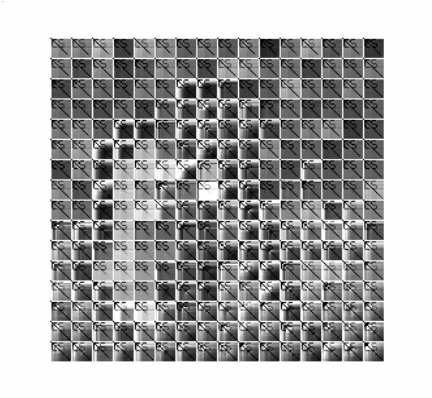
| | | |
|---|---|---|
|  |  |  |
| Gaussian noise .01<br>Correlation=0.1271 | Blurring 3x3<br>Correlation=0.0584 | Cropping<br>Correlation=0.0090 |
|  |  |  |
| Resizing 256—128—256<br>Correlation=0.0921 | Rotate 15°<br>Correlation=0.0510 | JPEG compression<br>Correlation=0.8202 |

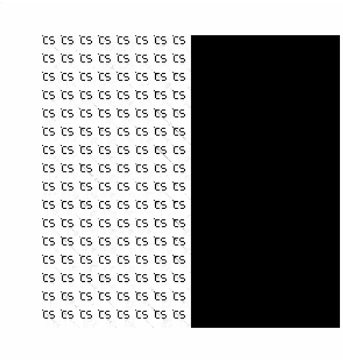
**Figure (5)** the extracted watermarks for Liu method after applying attacks

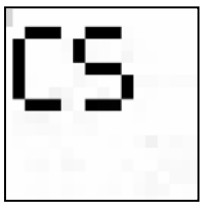


Gaussian noise variance = .01
Max. Correlation = 0.5408

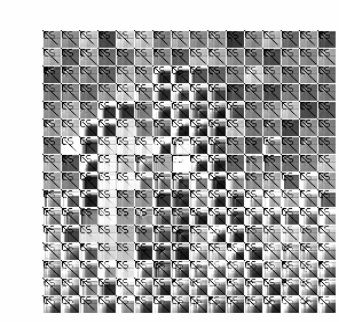


Blurring 3x3
Max. Correlation = 0.7072





Cropping
Max. Correlation = 0.9975



Resizing 256—128—256
Max. Correlation = 0.5435

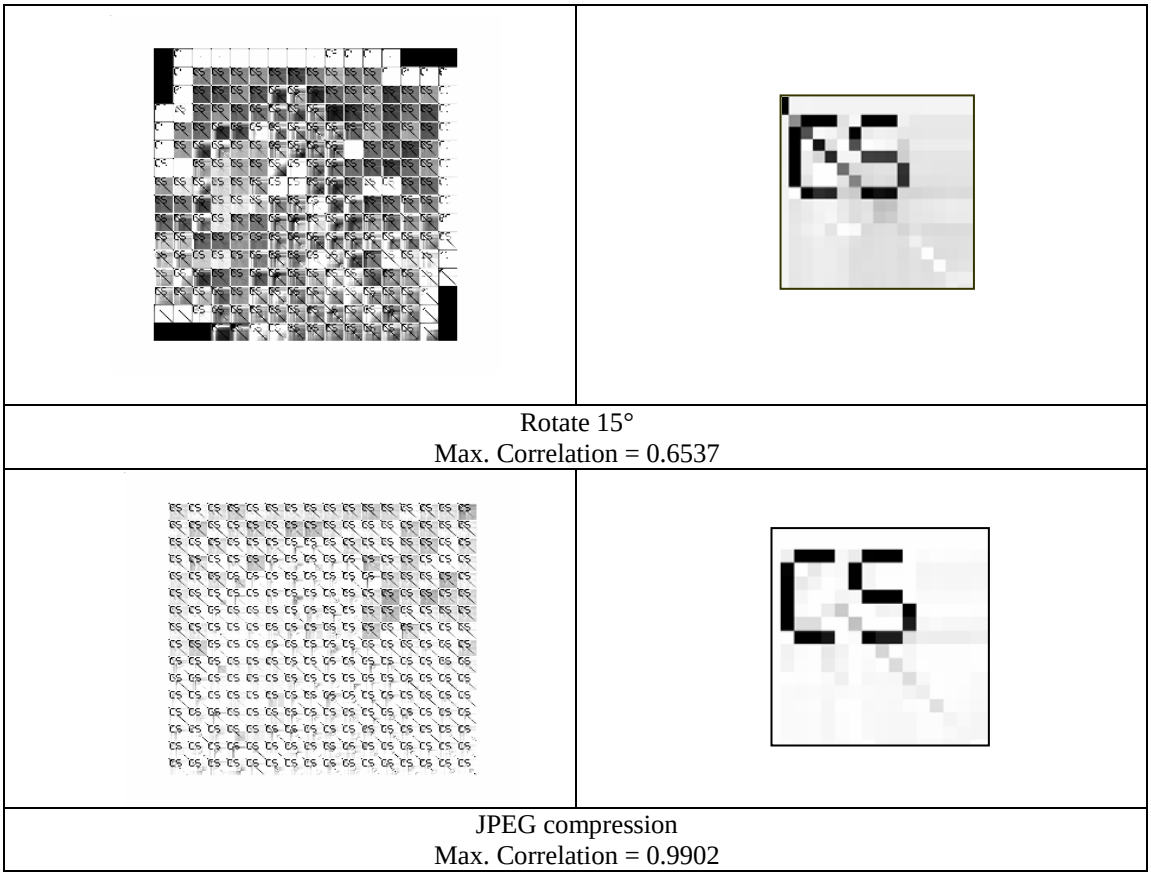



**Figure (6)** Extracted watermarks for different attacks.
Left: the extracted watermark from each block.
Right: magnification of the block that achieved maximum correlation with the original watermark.

**Table (1)** Correlation coefficients for noise attacks with different noise variances

| Variance | 0.001 | 0.005 | 0.01 | 0.05 | 0.1 | 0.5 | 1 |
|---|---|---|---|---|---|---|---|
| Correlation1 | 0.6100 | 0.5802 | 0.5667 | 0.5207 | 0.4661 | 0.4362 | 0.4377 |
| Corrlation2 | 0.3665 | 0.1641 | 0.1267 | 0.0854 | 0.0779 | 0.0700 | 0.0688 |
| No of blocks usingTH=0.5 | 13 | 8 | 4 | 1 | 0 | 0 | 0 |
| No of blocks usingTH=0.4 | 95 | 21 | 14 | 10 | 9 | 3 | 2 |

**Table (2)** Correlation coefficients lowpass filter attacks with different filter window sizes.

| Window size | 3 ×3 | 4 ×4 | 5 ×5 | 6 ×6 |
|---|---|---|---|---|
| Correlation1 | 0.7072 | 0.5430 | 0.6618 | 0.5736 |
| Corrlation2 | 0.0596 | 0.0372 | 0.0261 | 0.0191 |
| No of blocks using TH=0.5 | 13 | 2 | 1 | 2 |
| No of blocks using TH=0.4 | 16 | 8 | 3 | 2 |

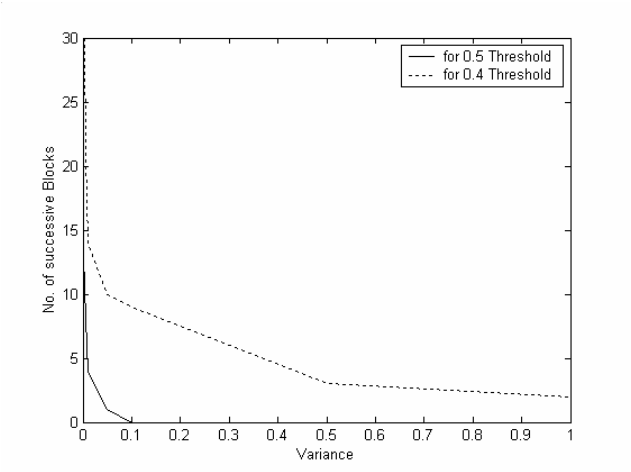



**Figure (7)** Noise variance vs. the number of successively extracted watermark Blocks using 0.4 and 0.5 thresholds.