Information Processing and Management 50 (2014) 909–923

Contents lists available at ScienceDirect

Information Processing and Management

journal homepage: www.elsevier.com/locate/infoproman

Homomorphic image watermarking with a singular value decomposition algorithm

Hanaa A. Abdallah [a], Rania A. Ghazy [b], Hany Kasban [c], Osama S. Faragallah [d], Abdalhameed A. Shaalan [a], Mohiy M. Hadhoud [e], Moawad I. Dessouky [b], Nawal A. El-Fishawy [d], Saleh A. Alshebeili [f], Fathi E. Abd El-samie [b,g,*]

[a] Faculty of Engineering, Zagazig University, Zagazig, Egypt
[b] Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[c] Engineering Department, Nuclear Research Center, Atomic Energy Authority, Egypt
[d] Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[e] Department of Information Technology, Faculty of Computers and Information, Menoufia University, 32511 Shebin Elkom, Egypt
[f] Electrical Engineering Department, KACST-TIC in Radio Frequency and Photonics for the e-Society (RFTONICS), King Saud University, Saudi Arabia
[g] KACST-TIC in Radio Frequency and Photonics for the e-Society (RFTONICS), King Saud University, Saudi Arabia

ARTICLE INFO

Article history:
Received 9 December 2010
Received in revised form 29 June 2014
Accepted 2 July 2014
Available online 24 August 2014

Keywords:
Image watermarking
Homomorphic transform
SVD
Wavelet transform

ABSTRACT

In this paper, a new homomorphic image watermarking method implementing the Singular Value Decomposition (SVD) algorithm is presented. The idea of the proposed method is based on embedding the watermark with the SVD algorithm in the reflectance component after applying the homomorphic transform. The reflectance component contains most of the image features but with low energy, and hence watermarks embedded in this component will be invisible. A block-by-block implementation of the proposed method is also introduced. The watermark embedding on a block-by-block basis makes the watermark more robust to attacks. A comparison study between the proposed method and the traditional SVD watermarking method is presented in the presence of attacks. The proposed method is more robust to various attacks. The embedding of chaotic encrypted watermarks is also investigated in this paper to increase the level of security.

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 security requirements, watermarking technology can be used. Watermarking means embedding a piece of information into a cover signal or image in such a way that it is imperceptible to a human observer, but is easily detectable by a computer or a detector (Cox, Miller, & Bloom, 2002). Several researchers have worked in the field of watermarking for its importance (Cox et al., 2002; Podilchuk & Delp, 2001). 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 (Shoemaker & Rudko, 2002).

* Corresponding author at: Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt.

E-mail addresses: dr.hanaaabdalaziz@gmail.com (H.A. Abdallah), eng_rasg@yahoo.com (R.A. Ghazy), Hany_kasban@yahoo.com (H. Kasban), osam_sal@yahoo.com (O.S. Faragallah), shaalan_zag2010@yahoo.com (A.A. Shaalan), mmhadhoud@yahoo.com (M.M. Hadhoud), dr_moawad@yahoo.com (M.I. Dessouky), nelfishawy@hotmail.com (N.A. El-Fishawy), dsaleh@ksu.edu.sa (S.A. Alshebeili), fathi_sayed@yahoo.com (F.E. Abd El-samie).

http://dx.doi.org/10.1016/j.ipm.2014.07.001
0306-4573/

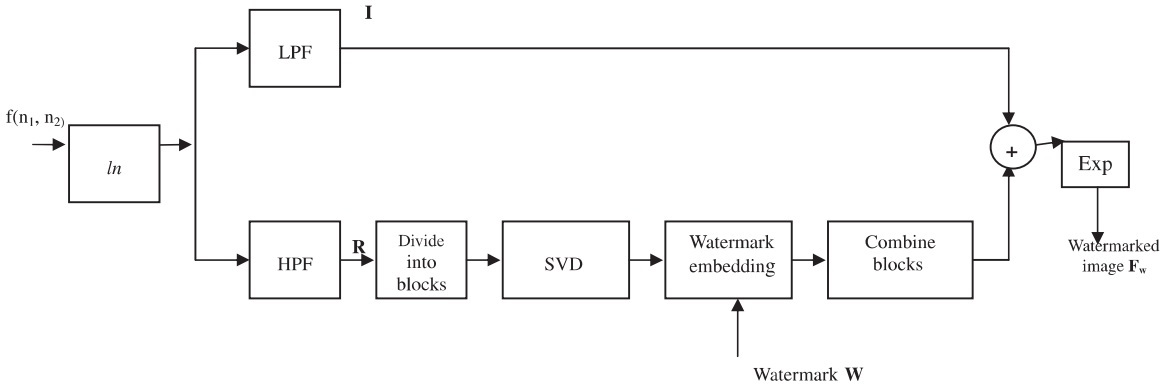


Fig. 1. Proposed homomorphic image watermark embedding.

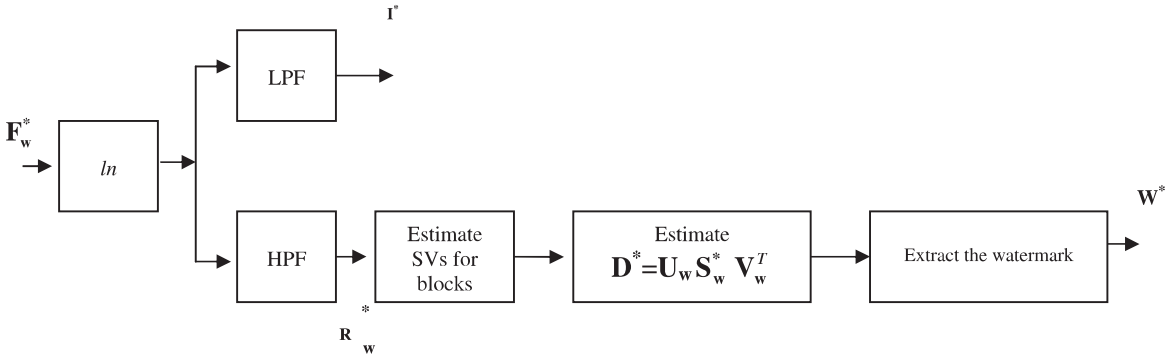


Fig. 2. Homomorphic watermark detection.

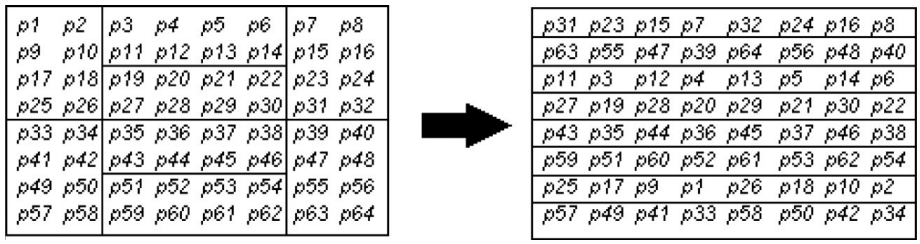


Fig. 3. Baker map randomization of an 8 × 8 matrix with a key of [2, 4, 2].

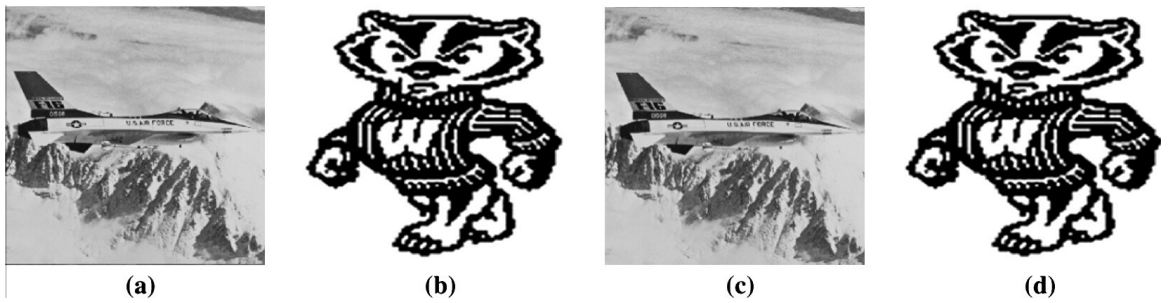


Fig. 4. Method of Liu. (a) Original image. (b) Watermark. (c) Watermarked image without attacks, PSNR = 62.65 dB. (d) Extracted watermark, $c_r = 0.9$.

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. Each watermarking technique consists of an embedding algorithm and a detection algorithm. An embedded watermark must achieve some requirements such as

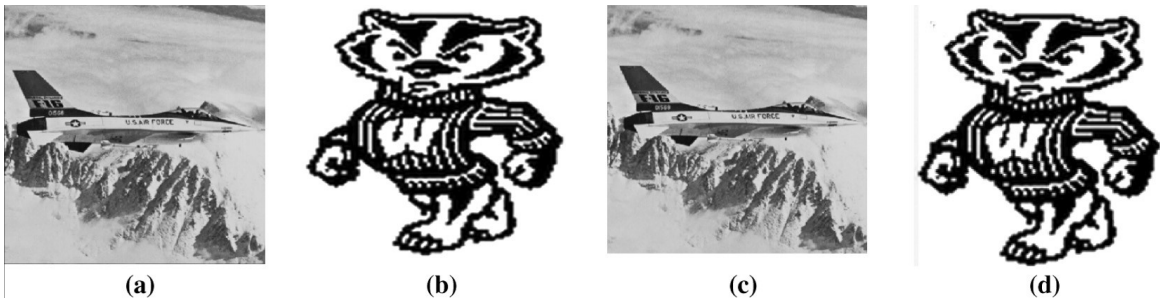


Fig. 5. SVD watermarking in the homomorphic domain. (a) Original image. (b) Watermark. (c) Watermarked image without attacks, PSNR = 65.7 dB. (d) Extracted watermark, $c_r = 0.9993$.

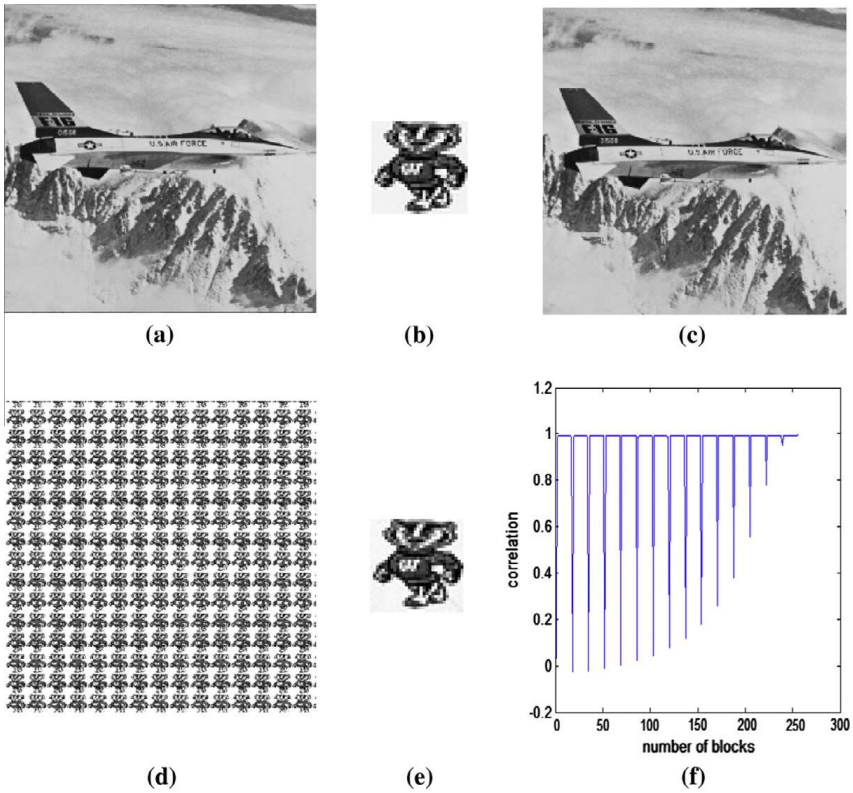


Fig. 6. Block-by-block SVD watermarking in the homomorphic domain. (a) Original image. (b) Watermark to be embedded in each block in the homomorphic domain. (c) Watermarked image without attacks, PSNR = 66.58 dB. (d) Extracted watermarks from each block. (e) Zooming of the extracted watermark, which has $c_{rmax} = 0.9997$. (f) Correlation coefficient values between each extracted watermark and the original one.

robustness, fidelity, and tamper resistance (Cox et al., 2002). Robustness means that the watermark must be robust to the transformations that include common signal distortions such as digital-to-analog conversion, analog-to-digital conversion, and lossy compression. Fidelity means that the watermark must 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 importance of these requirements depends on the application. The watermark can be embedded in the spatial domain or in a transform domain (Shoemaker & Rudko, 2002).

The SVD mathematical algorithm provides an elegant way for extracting algebraic features from an image. The main properties of the Singular Values (SVs) matrix of an image can be exploited in image watermarking. This matrix has a good stability. When a small perturbation affects the image, no large variations occur in its SVs (Chandra, 2002; Liu & Tan, 2002). Using this property, the watermark can be embedded to this matrix without large variations in the obtained image. Liu et al. have proposed an SVD image watermarking scheme, in which the watermark is added to the SVs of the whole image or to a apart of it (Liu & Tan, 2002). The watermark used in this scheme may be lost due to attacks.

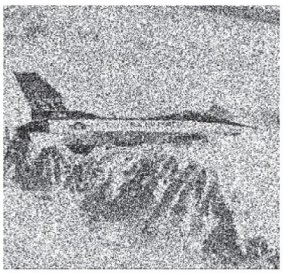
The main idea of homomorphic image processing is based on modeling the image as a product of a constant illumination and a varying reflectance (Chang, Tsai, & Lin, 2005; Srinivas Kumar, Chandra Mohan, & Chatterji, 2007). The product is dealt with as a summation using the logarithmic operation. The reflectance component can be separated using a High-Pass Filter

(a) JPEG Compression, Q=50%.

(b) Recovered watermark, c_r=0.75.

(c) Resizing, 512-256-512.

(d) Recovered watermark, c_r =0.5714.



(e) Gaussian noise, variance = 0.1.

(f) Recovered watermark, c_r =0.1438

(g) Cropping.

(h) Recovered watermark, c_r =0.0317

(i) Rotation.

(j) Recovered watermark, c_r = 0.1647

Fig. 7. Watermarked images and extracted watermarks for the method of Liu under attacks.

(a) JPEG Compression, Q=50%.

(b) Recovered watermark, c_r=0.98.

(c) Resizing, 512-256-512.

(d) Recovered watermark, c_r =0.91.

(e) Gaussian noise, variance = 0.1.

(f) Recovered watermark, c_r =0.79.

(g) Cropping.

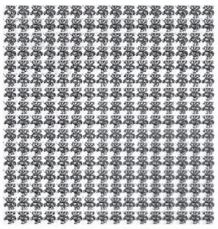
(h) Recovered watermark, c_r =0.94.

(i) Rotation.

(j) Recovered watermark, c_r =0.54.

Fig. 8. Watermarked images and extracted watermarks for SVD watermarking in the homomorphic domain under attacks.

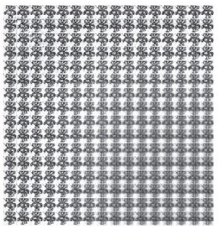
(a) JPEG Compression, Q=50%.



(b) Recovered watermarks.

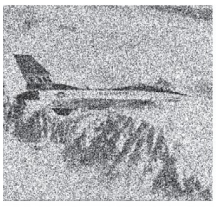
(c) Extracted watermark with c_{rmax}=0.993.

(d) Resizing, 512-256-512.

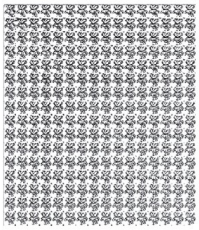


(e) Recovered watermarks.

(f) Extracted watermark with c_{rmax}=0.991



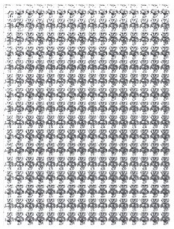
(g) Gaussian noise, variance = 0.1.



(h) Recovered watermarks.

(i) Extracted watermark with c_{rmax}=0.885.

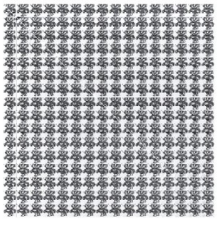
(j) Cropping.



(k) Recovered watermarks.

(l) Extracted watermark with c_{rmax}=0.98.

(m) Rotation.



(n) Recovered watermarks.

(o) Extracted watermark with c_{rmax}=0.993.

Fig. 9. Extracted watermarks for the block-by-block SVD watermarking in the homomorphic domain under attacks.

(HPF), while the illumination component can be separated using a Low-Pass Filter (LPF). Most of the image details lie in the reflectance component with low energy, while the illumination component is approximately constant with high energy. We can carry out the watermarking process in the homomorphic domain on the reflectance component. Our objective is to achieve invisibility of the watermark, robustness, fidelity and tamper resistance. Invisibility is achieved by watermark

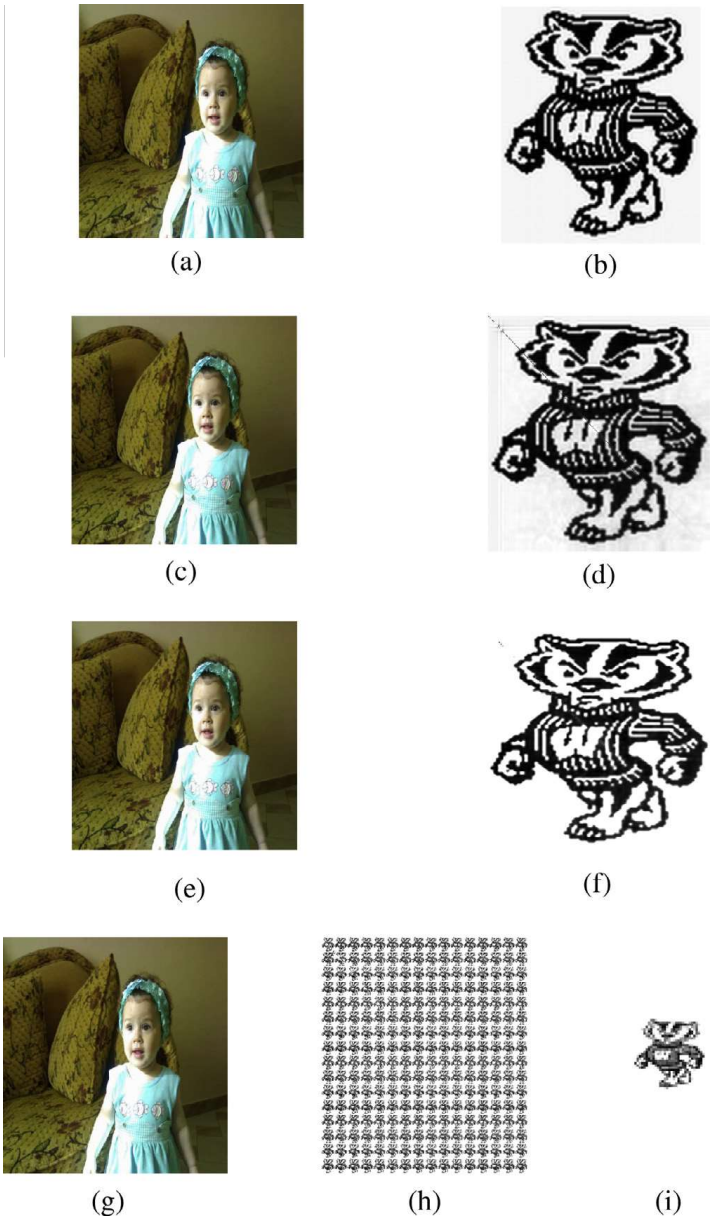


Fig. 10. (a) Original image. (b) Watermark. (c) Watermarked image without attacks using the method of Liu, PSNR = 48 dB. (d) Extracted watermark using the method of Liu, $c_r = 0.9$. (e) Watermarked image without attacks using SVD watermarking in the homomorphic domain, PSNR = 48.06 dB. (f) Recovered watermark using SVD watermarking in the homomorphic domain, $c_r = 0.995$. (g) Watermarked image using block-by-block SVD watermarking in the homomorphic domain, PSNR = 48.07 dB. (h) Recovered watermarks using block-by-block SVD watermarking in the homomorphic domain. (i) Magnification of the watermark with $c_{r\max} = 0.999$.

embedding in the low-energy reflectance component. Robustness, fidelity, and tamper resistance are guaranteed with the properties of the SVD algorithm.

The paper is organized as follows. Section 2 briefly explains the traditional SVD image watermarking scheme. Section 3 introduces the proposed SVD watermarking method in the homomorphic domain. Section 4 introduces a block-by-block implementation of SVD watermarking in the homomorphic domain. Section 5 discusses SVD watermarking in the homomorphic domain with encrypted watermarks. Section 6 gives the experimental results. Finally, Section 7 gives the concluding remarks.

2. SVD image watermarking

The SVD of an image is computed to obtain two orthogonal matrices **U** and **V**, and a diagonal matrix **S**. In the approach proposed by Liu et al., the watermark **W** is added to the matrix of SVs **S**, and then a new SVD process is performed on the resulting matrix $\mathbf{S} + k\mathbf{W}$ to get $\mathbf{U_w}$, $\mathbf{S_w}$, and $\mathbf{V_w}$ (Liu & Tan, 2002). k is a scale factor that controls the strength of the watermark embedded to the original image. The watermarked image $\mathbf{F_w}$ is obtained by multiplying the matrices **U**, $\mathbf{S_w}$, and $\mathbf{V}^T$. The steps of watermark embedding are summarized as follows:

(a) JPEG Compression, Q=50%.

(b) Recovered watermark, c_r= 0.63.

(c) Rotation.

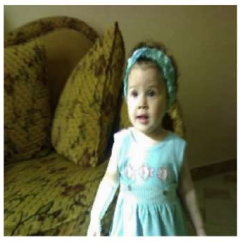
(d) Recovered watermark, c_r= 0.3396.

(e) Resizing, 512-256-512.

(f) Recovered watermark, c_r= 0.32.

(g) Salt and pepper (impulsive noise).

(h) Recovered watermark, c_r= 0.22.



(i) Blurring.

(j) Recovered watermark, c_r= 0.24.

Fig. 11. Watermarked color images and extracted watermarks for the method of Liu under attacks.

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

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

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

(a) Compression.

(b) Recovered watermark, c_r=0.993.

(c) Rotation.

(d) Recovered watermark, c_r=0.976.

(e) Resizing, 512-256-512.

(f) Recovered watermark, c_r=0.92.

(g) Salt and pepper (impulsive noise).

(h) Recovered watermark, c_r= 0.74.

(i) Blurring.

(j) Recovered watermark, c_r=0.94.

Fig. 12. Watermarked color images and extracted watermarks for SVD watermarking in the homomorphic domain.

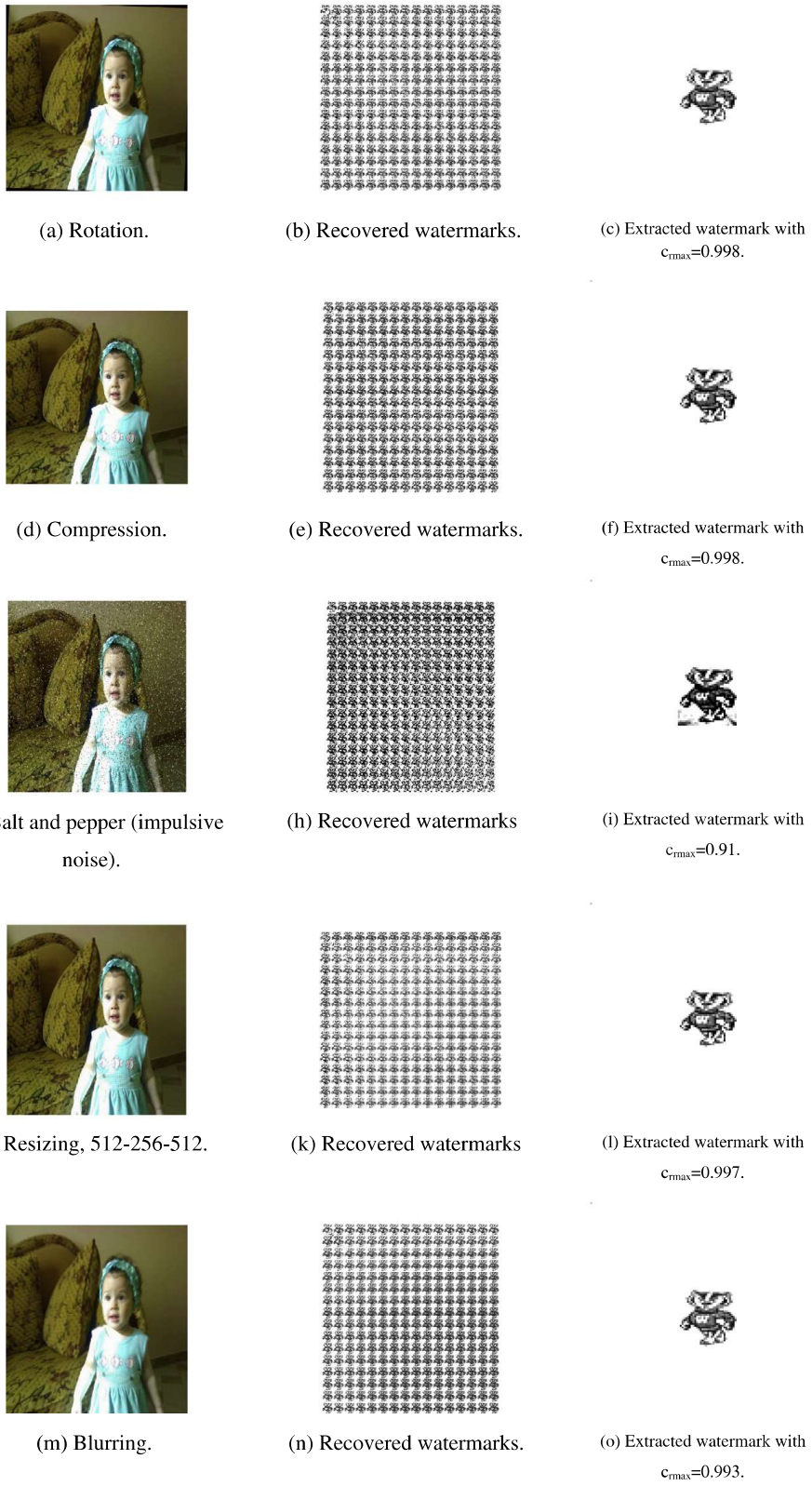
$$\mathbf{D} = \mathbf{S} + k\mathbf{W} \tag{2}$$

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

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

4. The watermarked image ($\mathbf{F_w}$ matrix) is obtained using the modified matrix ($\mathbf{S_w}$ matrix).

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



(a) Rotation. (b) Recovered watermarks. (c) Extracted watermark with c_{rmax}=0.998.

(d) Compression. (e) Recovered watermarks. (f) Extracted watermark with c_{rmax}=0.998.

(g) Salt and pepper (impulsive noise). (h) Recovered watermarks (i) Extracted watermark with c_{rmax}=0.91.

(j) Resizing, 512-256-512. (k) Recovered watermarks (l) Extracted watermark with c_{rmax}=0.997.

(m) Blurring. (n) Recovered watermarks. (o) Extracted watermark with c_{rmax}=0.993.

Fig. 13. Watermarked images and extracted watermarks for block-by-block SVD watermarking in the homomorphic domain.

To extract the possibly corrupted watermark from the possibly distorted watermarked image, given $\mathbf{U_w}$, $\mathbf{S}$, $\mathbf{V_w}$ matrices, and the possibly distorted image $\mathbf{F}^*_{\mathbf{w}}$, the above steps are reversed as follows:

1. The SVD is performed on the possibly distorted watermarked image ($\mathbf{F}_{\mathbf{w}}^{*}$ matrix).

$$\mathbf{F}_{\mathbf{w}}^{*} = \mathbf{U}^{*}\mathbf{S}_{\mathbf{w}}^{*}\mathbf{V}^{*T} \tag{5}$$

2. The matrix that includes the watermark is computed.

$$\mathbf{D}^{*} = \mathbf{U}_{\mathbf{w}}\mathbf{S}_{\mathbf{w}}^{*}\mathbf{V}_{\mathbf{w}}^{T} \tag{6}$$

3. The possibly corrupted watermark is obtained.

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

The * refers to the corruption due to attacks.

3. SVD image watermarking in the homomorphic domain

In general, an image can be regarded as a 2-D function of the form $f(n_1, n_2)$, whose values at the spatial coordinates (n_1, n_2) are positive scalar quantities (Li, Zheng, Mou, & Cai, 2002). Assuming that we are dealing with gray-scale images, we can say that when an image is generated from a physical process, its values are proportional to the energy radiated by a physical source. In other words, an image is an array of measured light intensities and is a function of the amount of light reflected from the objects in the scene. The intensities of pixels are the product of the incident illumination and objects reflectance. The illumination is approximately constant, while the reflectance holds most of the image details. The reflectance results from the way the objects in the image reflect light, and it is determined by the intrinsic properties of the objects. So, it is expected that a watermark embedded in the reflectance component can survive several attacks, because watermarks are generally required to be inserted in details or edges of the images (Chandra Mohan & Srinivas Kumar, 2008). In the following sub-sections, the steps of watermark embedding in the reflectance component of an image and watermark detection are presented.

3.1. Watermark embedding

1. The image intensities can be represented as follows (Ghazy, El-Feshawy, Hadhoud, Dessouky, & Abd El-Samie, 2007; Gonzalez & Woods, 2002):

$$f(n_1, n_2) = i(n_1, n_2)r(n_1, n_2) \tag{8}$$

where $i(n_1, n_2)$ is the light illumination and $r(n_1, n_2)$ is the reflectance of the object to be imaged.

2. The homomorphic transform is performed

$$\ln[f(n_1, n_2)] = \ln[i(n_1, n_2)] + \ln[r(n_1, n_2)] \tag{9}$$

3. An LPF and an HPF are applied to $\ln[f(n_1, n_2)]$ to separate the illumination component $\mathbf{I}$ from the reflectance component $\mathbf{R}$, in the form of matrices
4. The SVD is performed on the ($\mathbf{R}$ matrix)

$$\mathbf{R} = \mathbf{U}\mathbf{S}\mathbf{V}^{T} \tag{10}$$

5. The watermark ($\mathbf{W}$ matrix) is added to the SVs of the reflectance matrix.

$$\mathbf{D} = \mathbf{S} + k\mathbf{W} \tag{11}$$

6. The SVD is performed on the new modified matrix ($\mathbf{D}$ matrix).

$$\mathbf{D} = \mathbf{U}_{w}\mathbf{S}_{w}\mathbf{V}_{\mathbf{w}}^{T} \tag{12}$$

7. The watermarked reflectance matrix $\mathbf{R}_{\mathbf{w}}$ is obtained using the $\mathbf{S}_{\mathbf{w}}$ matrix.

$$\mathbf{R}_{\mathbf{w}} = \mathbf{U}\mathbf{S}_{\mathbf{w}}\mathbf{V}^{T} \tag{13}$$

8. An inverse homomorphic transform is performed on $\mathbf{I}$ and $\mathbf{R}_{\mathbf{w}}$ to obtain a matrix $\mathbf{X}_{\mathbf{w}}$.

$$\mathbf{X}_{\mathbf{w}} = \mathbf{R}_{\mathbf{w}} + \mathbf{I} \tag{14}$$

9. The watermarked image is obtained as follows:

$$\mathbf{F}_{\mathbf{w}} = \exp(\mathbf{X}_{\mathbf{w}}) \tag{15}$$

We can notice from Eqs. (13)–(15) that the watermark affects the watermarked image in a multiplicative manner, which is expected to make this watermarking scheme more resistant to traditional signal processing techniques. It is well-known in signal processing that multiplicative effects on signals are difficult to remove. So, traditional signal processing techniques

like filtering, JPEG, AWGN will have a smaller effect on the proposed technique that their effect on the SVD watermarking only.

3.2. Watermark detection

To extract the possibly corrupted watermark from the possibly distorted watermarked image, given $\mathbf{U_w}$, $\mathbf{S}$, $\mathbf{V_w}$ matrices, and the possibly distorted image $\mathbf{F}^*_\mathbf{w}$, the above steps are reversed as follows:

1. The homomorphic transform is performed on the possibly distorted watermarked image $\mathbf{F}^*_\mathbf{w}$.
2. An HPF similar to that used in the embedding process is used to get the possibly corrupted reflectance component $\mathbf{R}^*_\mathbf{w}$.
3. The SVD is performed on the $\mathbf{R}^*_\mathbf{w}$ matrix.

$$\mathbf{R}^*_\mathbf{w} = \mathbf{U}^*\mathbf{S}^*_\mathbf{w}\mathbf{V}^{*T} \tag{16}$$

4. The matrix that includes the watermark is computed.

$$\mathbf{D}^* = \mathbf{U_w}\mathbf{S}^*_\mathbf{w}\mathbf{V}^T_\mathbf{w} \tag{17}$$

5. The possibly corrupted watermark is obtained.

$$\mathbf{W}^* = (\mathbf{D}^* - \mathbf{S})/k \tag{18}$$

4. Block-by-block SVD watermarking in the homomorphic domain

Generally, watermark embedding on a block-by-block basis increases the ability of the watermark to survive attacks (Basso, Bergadano, Cavagnino, Pomponiu, & Vernone, 2009). The block-by-block SVD watermarking is employed by dividing the original image into blocks, and then the watermark is embedded in the SVs of the reflectance component of each block, separately. The steps of watermark embedding and detection on a block-by-block basis are presented in the following subsections.

4.1. Watermark embedding

The same steps from 1 to 4 in Section 3.1 are applied, and then:

5. The matrix $\mathbf{S}$ is divided into non-overlapping blocks $\mathbf{S_b}$.
6. The watermark matrix $\mathbf{W}$ is added to each block.

$$\mathbf{D} = \mathbf{S_b} + k\mathbf{W} \tag{19}$$

7. The watermarked blocks are combined back into a single matrix to build the $\mathbf{S_w}$ matrix.

The same steps from 8 to 10 in Section 3.1 are applied.

4.2. Watermark detection

The same steps from 1 to 4 in Section 3.2 are applied but on blocks and then:

5. The possibly corrupted watermark is obtained.

$$\mathbf{W}^* = (\mathbf{D}^* - \mathbf{S_b})/k \tag{20}$$

Watermark embedding and detection are shown in Figs. 1 and 2, respectively.

5. SVD watermarking in the homomorphic domain with encrypted watermarks

We study the process of embedding an encrypted watermark to an image to increase the level of security. The same steps of the method of Liu and the proposed SVD watermarking in the homomorphic domain are used with encrypted watermarks. The watermark is first encrypted with a 2-D chaotic Baker map and then embedded to the image and the extracted watermark is decrypted.

The discretized Baker map randomizes a square matrix by assigning each pixel another position in a bijective manner. The discretized Baker map will be denoted by $B_{(n_1,\ldots,n_l)}$, where the sequence of l integers, $n_1,n_2,\ldots,n_l$, is chosen such that each integer n_i divides N, and $N_i = n_1 + \cdots + n_i$. The pixel at (r,s), with $N_i \leqslant r < N_i + n_i$ and $0 \leqslant s < N$ is mapped to (Fridrich, 1998):

$$B_{(n_1,\ldots,n_k)}(r,s) = \left[\frac{N}{n_i}(r - N_i) + s \bmod \frac{N}{n_i}, \frac{n_i}{N}\left(s - s \bmod \frac{N}{n_i}\right) + N_i\right] \quad (21)$$

The steps of randomization can be summarized as follows:

1. An $N \times N$ square matrix is divided into l vertical rectangles of height N and width n_i with $n_1 + n_2 + \ldots n_l = N$).
2. Each vertical rectangle is divided into n_i blocks, and each block contains N points.
3. Each of these blocks is mapped to a row of pixels.

An example of the randomization of an 8×8 matrix is shown in Fig. 3. The secret key is [2, 4, 2], hence $N = 8$, $n_1 = 2$, $n_2 = 4$, and $n_3 = 2$.

6. Simulation results

Several experiments have been carried out to compare between the method of Liu, and the proposed SVD watermarking in the homomorphic domain for the whole image and on a block-by-block basis. The 512×512 Airplane and color Baby images have been used in the simulation experiments. The RGB color space is highly correlated, and hence it is not suitable for watermarking applications, except for the blue channel used by some researchers because of its low effect on human perception (Gilani, Kostopoulos, & Skodras, 2002). So, we have to transform the RGB color space to the Y C_b C_r color space. In this color space, most of the information is concentrated in the luminance (Y component) and little information is in the chrominance (C_b and C_r components). The experiments demonstrate that watermark embedding in the luminance component (Y) has a larger effect on the human vision than embedding in the C_b or C_r components, but due to the robustness to JPEG compression; we have performed watermark embedding in the Y channel.

Fig. 4 shows the original image, the watermark, the watermarked image, and the extracted watermark using the method of Liu. Fig. 5 shows the original image, the watermark, the watermarked image, and the extracted watermark using the proposed homomorphic method. It is clear that there is no visual difference between the original image and the watermarked image, ensuring the fidelity of the proposed homomorphic method. We can see that the Peak Signal-to-Noise Ratio (PSNR) of the watermarked image in the method of Liu is 62.65 dB, and in the proposed method, the PSNR is 65.7 dB. The correlation coefficient (c_r) values between the original watermark and the extracted watermarks for SVD watermarking and SVD watermarking in the homomorphic domain are 0.9 and 0.9993, respectively.

Fig. 6 shows the original image, the watermark, the watermarked image, and the extracted watermarks using the block-by-block SVD method in the homomorphic domain. It is clear that there is no visual difference between the original image and the watermarked image, ensuring the fidelity of the block-by-block SVD watermarking in the homomorphic domain. We find that the PSNR in this method is 66.58 dB. The maximum correlation coefficient between the original watermark and any of the extracted watermarks is $c_{r\max} = 0.9997$.

Table 1
Correlation coefficient values for the extracted watermarks with the different watermarking methods on the Airplane image with and without attacks.

Attack	Method		
	Method of Liu	SVD watermarking in the homomorphic domain	Block-by-block SVD watermarking in the homomorphic domain
No attack	0.9000	0.9993	0.9997
JPEG compression $Q = 50\%$	0.7500	0.98	0.9930
Resizing 512–256–512	0.5714	0.91	0.9910
Gaussian noise with variance = 0.1.	0.1438	0.79	0.8850
Cropping	0.0317	0.94	0.9930
Rotation	0.1647	0.54	0.9800

Table 2
Correlation coefficient values for the extracted watermarks with the different watermarking methods on the Airplane image with and without attacks.

Attack	Method		
	Method of Liu	SVD watermarking in the homomorphic domain	Block-by-block SVD watermarking in the homomorphic domain
No attack	0.9	0.995	0.999
Rotation	0.63	0.993	0.998
JPEG compression $Q = 50\%$	0.3396	0.976	0.998
Impulsive noise	0.32	0.92	0.91
Resizing 512–256–512	0.22	0.74	0.997
Blurring	0.24	0.94	0.993

Some attacks such as adding Gaussian noise, cropping, compression, rotation and resizing have been applied on the watermarked images. Figs. 7–9 show the watermarked images and the extracted watermarks under attacks for all watermarking methods. The first attack applied is the JPEG compression with quality factor 50%. The second attack is resizing from size 512×512 to 256×256 and back to 512×512. The third attack is addition of Gaussian noise with zero mean and 0.1 variance. The fourth attack is cropping. The fifth attack is rotation with $-3°$.

Fig. 7 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 lies between 0.1 and 0.8 for each attack except for the cropping attack, which gives $c_r = 0.0317$. Fig. 8 shows the extracted watermarks for the proposed SVD watermarking in the homomorphic domain after applying similar attacks. In all cases, the extracted watermarks have values of c_r higher than 0.5 and better than those of the method of Liu, which ensures the existence of the watermark and the superiority of the proposed SVD watermarking in the homomorphic domain.

Fig. 9 shows the extracted watermarks for the block-by-block SVD method in the homomorphic domain under similar attacks. In all cases, there are extracted watermarks with c_r higher than 0.8, which ensures the existence of the watermark. The results show that the detectability of the watermark has been greatly enhanced with the proposed block-by-block SVD

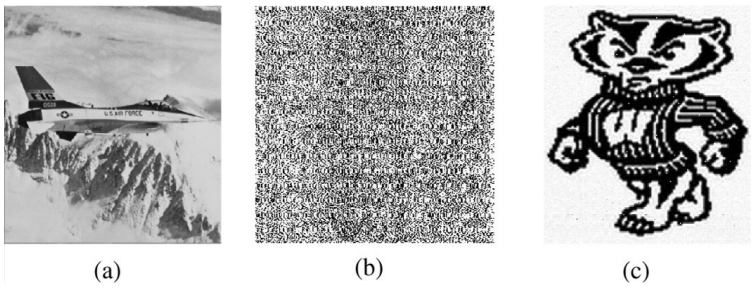


Fig. 14. Method of Liu with an encrypted watermark. (a) Watermarked image without attacks, PSNR = 61.29 dB. (b) Recovered encrypted watermark. (c) Decrypted watermark, $c_r = 0.9$.

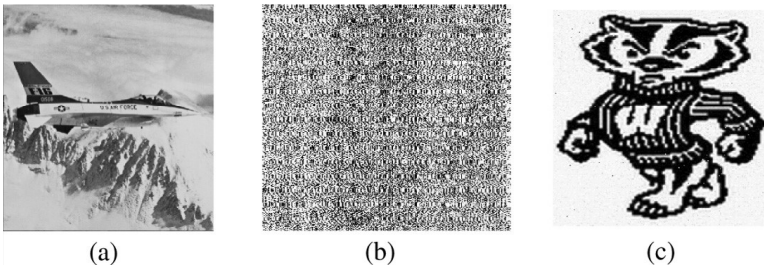


Fig. 15. SVD watermarking in the homomorphic domain with an encrypted watermark. (a) Watermarked image without attacks, PSNR = 62.8 dB. (b) Recovered encrypted watermark. (c) Decrypted watermark, $c_r = 0.92$.

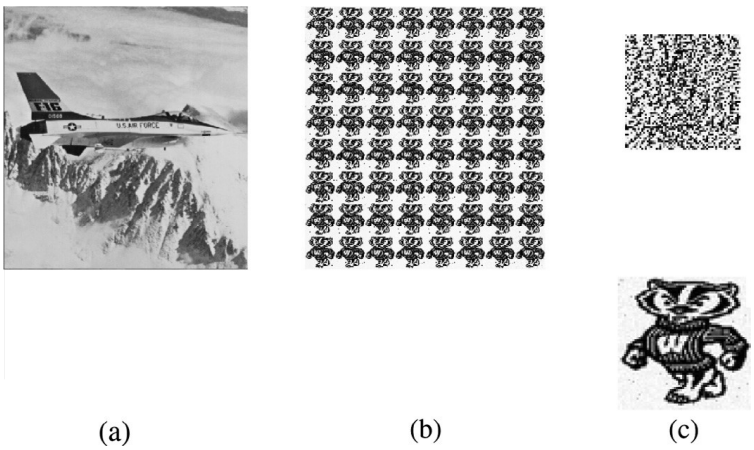


Fig. 16. Block-by-block SVD watermarking in the homomorphic domain with an encrypted watermark. (a) Watermarked image without attacks, PSNR = 64.47 dB. (b) Recovered encrypted watermarks. (c) The encrypted watermark and its decrypted version with $c_{r\max} = 0.99$.

Table 3
Correlation coefficient values for the extracted watermarks with the different watermarking methods on the Airplane image using an encrypted watermark with and without attacks.

Attack	Method		
	Method of Liu	SVD watermarking in the homomorphic domain	Block-by-block SVD watermarking in the homomorphic domain
No attack	0.9	0.92	0.99
Rotation	0.034	0.034	0.97
JPEG compression $Q = 50\%$	0.69	0.71	0.98
Cropping	0.032	0.24	0.98
Resizing 512–256–512	0.2	0.46	0.97
Blurring	0.13	0.23	0.96

watermarking method in the homomorphic domain. Watermark repetition has increased the probability that at least one watermark survives the attack.

The experimental results on the 512×512 color Baby image with the method of Liu, the SVD watermarking in the homomorphic domain, and the block-by-block SVD watermarking in the homomorphic domain are shown in Figs. 10–13. Tables 1 and 2 give correlation coefficient values for the Airplane and Baby images with all methods under different attacks. The obtained results reveal the superiority of watermarking in the homomorphic domain.

Some other experiments have been carried out to show the results of SVD watermarking and block-by-block SVD watermarking in the homomorphic domain with an encrypted watermark. The Baker map has been used for encryption. To measure the quality of encryption, we estimate the correlation coefficient between the encrypted watermark and the original watermark c_e. The lower the value of c_e, the better the degree of encryption. Also, to evaluate the quality of watermarking, we estimate the correlation coefficient between the extracted decrypted watermark and the original watermark c_r. The higher the value of the correlation coefficient, the better the quality of watermarking. The results of watermarking with encrypted watermarks are shown in Figs. 14–16 and Table 3. From these results, we notice that the watermarks can be decrypted and extracted successfully for both SVD and block-by-block SVD watermarking in the homomorphic domain. Thus, we can conclude that the proposed SVD watermarking and block-by-block SVD watermarking in the homomorphic domain can be used successfully with permutation-based encryption algorithms.

7. Conclusions

This paper presented a homomorphic image watermarking method using the SVD algorithm. By embedding a watermark with the SVD algorithm to the reflectance component of an image, we guarantee that the effect of the watermark on the image is multiplicative not additive. That is why watermarking in the homomorphic domain survive digital signal processing attacks. Simulation results have shown that the block-by-block SVD watermarking in the homomorphic domain has high fidelity, robustness, and detectability under attacks. Simulation results have also shown that the utilization of encrypted watermarks is possible with SVD and block-by-block SVD watermarking in the homomorphic domain. We have come to the conclusion that permutation-based algorithms can be used efficiently for this purpose to increase the level of security.

References

Basso, A., Bergadano, F., Cavagnino, D., Pomponiu, V., & Vernone, A. (2009). A novel block-based watermarking scheme using the SVD transform. *Algorithms, 2*(1), 46–75.

Chandra, D. V. S. (2002). Digital image watermarking using singular value decomposition, In *Proceedings of 45th IEEE midwest symposium on circuits and systems* (pp. 264–267).

Chandra Mohan, B., & Srinivas Kumar, S. (2008). A robust image watermarking scheme using singular value decomposition. *Journal of Multimedia, 3*(1).

Chang, C.-C., Tsai, P., & Lin, C.-C. (2005). SVD based digital image watermarking scheme. *Pattern Recognition Letters, 26*, 1577–1586.

Cox, I. J., Miller, M. L., & Bloom, J. A. (2002). *Digital watermarking*. San Francisco, CA: Morgan Kaufmann Publishers.

Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and Chaos, 8*(6), 1259–1284.

Ghazy, R. A., El-Feshawy, N. A., Hadhoud, M. M., Dessouky, M. I. & Abd El-Samie, F. S. (2007). An efficient block-by-block SVD-based image watermarking scheme. *Radio Science Conference, 2007* (pp. 1–9). NRSC 2007, National Volume, Issue, 13–15 March 2007.

Gilani, S. A. M., Kostopoulos, I. & Skodras, A. N. (2002). Color image-adaptive watermarking. In *Digital Signal Processing International Conference, DSP2002* (Vol. 2, pp. 721–724).

Gonzalez, R. C., & Woods, R. E. (2002). *Digital image processing*. Upper Saddle River, NJ: Prentice Hall.

Li, S., Zheng, X., Mou, X., & Cai, Y. (2002). Chaotic encryption scheme for real-time digital video. *Proceedings of SPIE, 4666*, 149–160.

Liu, R., & Tan, T. (2002). An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia, 4*(1), 121–128.

Podilchuk, C. I. & Delp, E. J. (2001). Digital watermarking: Algorithms and applications. *IEEE Signal Processing Magazine*, July 2001, pp. 33–46.

Shoemaker, C. & Rudko (2002). Hidden bits: A survey of techniques for digital watermarking. *Independent StudyEER-290 Prof Rudko*, spring 2002.

Srinivas Kumar, S., Chandra Mohan, B. & Chatterji, B. N. (2007). An oblivious image watermarking scheme using singular value decomposition. In *IASTED International Conference on Signal and Image Processing (ICSIP'07)*, Honolulu, Hawaii, USA, August 20–22, 2007.