A ROBUST BLIND AND SECURE WATERMARKING SCHEME USING POSITIVE SEMI DEFINITE MATRICES

Noui Oussama[1] and Noui Lemnouar[2]

[1]Department of Computer Science, UHL University, Batna, Algeria
[2]Department of Mathematics, UHL University, Batna, Algeria

ABSTRACT

In the last decade the need for new and robust watermarking schemes has been increased because of the large illegal possession by not respecting the intellectual property rights in the multimedia in the internet. In this paper we introduce a novel blind robust watermarking scheme which exploits the positive circulant matrices in frequency domain which is the SVD, Different applications such as copyright protection, control and illicit distributions have been given. Simulation results indicate that the proposed method is robust against attacks as common digital processing: compression, blurring, dithering, printing and scanning, etc. and subterfuge attacks (collusion and forgery) also geometric distortions and transformations. Furthermore, good results of NC (normalized correlation) and PSNR (Peak signal-to-noise ratio) have been achieved while comparing with recent state of the art watermarking algorithms.

KEYWORDS

Circulant matrix, Digital image watermarking, Singular value decomposition, Positive semi-definite matrix.

1. INTRODUCTION

Recently, multimedia technology and the internet have seen a wide availability and accessibility, and the need for storage and transmitting digital images have enhanced, in the other hand the issue of not respecting the intellectual property rights is increased as well, by submitting artificial documents, in this case to ensure the security for content owners and service provider using cryptosystem encryption for data become not useful because it can only achieve confidentiality of data which means only the owner can see the content, where in most cases the submission and transmitting of content has done in a plain form, to overcome this problem digital watermarking techniques are used.

Watermarking is the procedure of embedding a watermark which can be an image or binary sequence or a multimedia object into a multimedia data. The result will be a watermarked data with invisible watermark. The extraction procedure will grab the watermark which will contains the information about the rightful owner and about the copyrighted object.

There are two types of watermarking schemes, watermarking in spatial domain and in frequently domain, the first the embedding of the watermark is done into the pixel values directly without any transformation, usually it is simple to be implemented but it suffer from weakness against many attacks, that’s why the second type is more interesting in research, in frequently domain we first apply a transformation on the host image as DCT, DWT, DFT or SVD. Also watermarking

DOI:10.5121/ijcsit.2014.6508

can be categorized from another point of view into three groups fragile, semi fragile and robust, where fragile means the watermark can be lost or corrupted after applying any type of image processing attacks, semi fragile the watermark resist only light attacks such as compression, and robust watermarking is when the watermark resist all common processing attacks and the last factor that watermarking schemes can be categorized about is blindness, a non blind watermarking schemes is when the original image is required for the extraction of the watermark, semi blind is when a part of an image is required and a blind scheme is when we don't need the original image or a part of it to recover the watermark only a key can be required in some cases.
The watermarking schemes in [1-4] are in spatial domain they are robust against geometrical attacks but they suffer from the poor capacity of data embedding, this drawback led other researchers to propose watermarking schemes in frequency domain [5-24], most of those methods are semi or non blind like [5, 6, 7, 8, 9, 13, 14, 19] which means the host image is required in the extraction procedure, also some methods has a good robustness but they don't offer a good transparency like [13, 14, 16, 19]. In most applications of watermarking the main concern has been the robustness against common digital attacks but usually resolving rightful ownership deadlock is ignored, the deadlock problem occurs where multiple ownership claims are made and the rightful ownership of digital content cannot be resolved.

For example a pirate simply adds his watermark to the watermarked data. This second mark allows the pirate to claim copyright ownership. Now the data has two marks, most watermarking schemes are unable to establish who watermarked the data first.

In this paper we propose a novel blind robust digital image watermarking scheme based on positive semi definite matrices and singular values decomposition. The proposed scheme has a variable watermark size, this flexibility may be operated following the desired data hiding capacity.

the rest of the paper is organized as follows: Section two is a related knowledge that we based on in the proposed method, the section describe the concept of the singular values decomposition, positive semi definite matrices and circulant matrices then Section three explains the proposed digital watermarking method. The simulation and the experimental results are discussed in section four also a performance comparison was given, Section five present applications of the scheme in copyright protection, illicit distribution and copy control, finally, conclusions are drawn in section six.

2. PRELIMINARY KNOWLEDGE

2.1. Singular values decomposition SVD

It is well known that:

Theorem (SVD) [17]:

For every real $n \times n$ matrix A of rank r, there are two orthogonal matrices U and V such that $U \times U^t = I$ and $V \times V^t = I$ where I is the Identity matrix and a diagonal matrix
$S = diag\ (\partial_1, \partial_2, \ldots, \partial_n)$ with $\partial_1 \geq \partial_2 \geq \cdot\cdot \geq 0$
such that

$$A = U \times S \times V^t \tag{1}$$

The entries $\partial_1, \partial_2, \ldots, \partial_r$ are the non zero singular values of A , i.e, the positive square roots of the non zero eigenvalues of $A^t A$ and $A\ A^t$ and $\partial_{r+1} = \ldots = \partial_n = 0$.

The columns of U are eigenvectors of $A\,A^t$ and the columns of V are eigenvectors of A^tA.
This theorem can be extended to rectangular $m \times n$ matrices.

2.2. Positive semi definite matrix

A symmetric $n \times n$ real matrix A is called positive semi definite if $x^t Ax \geq 0$ for all $x \in R^n$, where x^t denotes the transpose of x, and A is called positive definite if $x^t Ax > 0$ for all non-zero $x \in R^n$. It is easy to verify that the following statements are equivalent [18]:

a) The symmetric matrix A is positive semi definite.
b) All eigen values of A are non-negative.

Example

Given a set E of m vectors $v_1, .., v_m$ in R^n, the $m \times m$ gram matrix $G = (a)_{ij}$ is defined by

$a_{ij} = v_i\, v_j^t$

G can be also defined by $V^t\, V$ where V is a matrix whose columns are the vectors $v_1, .., v_m$. The matrix of gram is positive semi definite, it is positive definite if and only the vectors $v_1, .., v_m$ are linearly independent.

2.3. Circulant matrices

A $n \times n$ circulant matrix is formed from any n vector $c = (c_1, .., c_n)$ by cyclically permuting the entries, for example if $c = (c_1, c_2, c_3, c_4)$, the 4×4 circulant matrix $C = cir(c)$ is given by

$$\begin{pmatrix} c_1 & c_2 & c_3 & c_4 \\ c_4 & c_1 & c_2 & c_3 \\ c_3 & c_4 & c_1 & c_2 \\ c_2 & c_3 & c_4 & c_1 \end{pmatrix} \tag{2}$$

As the matrix $CC^t = C^tC$ is positive semi- definite its spectral decomposition coincides with its SVD decomposition, it is easy to verify that

$$CC^t = U_0 diag(\delta_1, \delta_2, \delta_3, \delta_4) U_0{}^t \tag{3}$$

with

$$\begin{aligned} \delta_1 &= (c_1 + c_2 + c_3 + c_4)^2 \\ \delta_2 &= (c_1 - c_2 + c_3 - c_4)^2 \\ \delta_3 = \delta_4 &= (c_1 - c_3)^2 + (c_2 - c_4)^2 \end{aligned} \tag{4}$$

are the singular values and U_0 is the constant matrix :

$$U_0 = \begin{pmatrix} 1/2 & -1/2 & 0 & -\sqrt{2}/2 \\ 1/2 & 1/2 & -\sqrt{2}/2 & 0 \\ 1/2 & -1/2 & 0 & \sqrt{2}/2 \\ 1/2 & 1/2 & \sqrt{2}/2 & 0 \end{pmatrix} \tag{5}$$

3. Proposed method

In the beginning of this section, we note that the main idea of our scheme is presenting a watermarking method using positive semi-definite matrices for which the spectral decomposition coincides with the singular value decomposition [18]. The watermark W is generated as positive semi definite matrix and its singular value decomposition is $U_W \times S_W \times {V_W}^t$ with $U_W = V_W$.
Now we will present more details on the proposed scheme.

3.1. Construction of watermark

Before considering the proposed method, we consider a circulant matrix $C_1 = cir(c_1^1, c_2^1, c_3^1, c_4^1)$ and we are going to discuss the choice of $c_1^1, c_2^1, c_3^1, c_4^1$ so that the singular values of the positive definite circulant matrix $C_1C_1^t = C_1^tC_1$ verify:

$$\delta_1^1 \geq \delta_2^1 \geq \delta_3^1 \geq \delta_4^1 \tag{6}$$

To this end, we put $S_1^1 = c_1^1 + c_3^1$, $S_2^1 = c_2^1 + c_4^1$, $D_1^1 = c_1^1 - c_3^1$, $D_2^1 = c_2^1 - c_4^1$
Then, according to (4), to obtain the decreasing sequence (6) it is enough to take

$$c_1^1 = \frac{S_1^1 + D_1^1}{2},\ c_2^1 = \frac{S_2^1 + D_2^1}{2},\ c_3^1 = \frac{S_1^1 - D_1^1}{2},\ c_4^1 = \frac{S_2^1 - D_2^1}{2}$$

Where $D_1^1 > 0$, $D_2^1 > 0$, $S_2^1 > 0$, $h^1 > 0$, are four arbitrary positive numbers and $S_1^1 = r_1 + S_2^1 + h^1$ with $r_1 = \sqrt{(D_1^1)^2 + (D_2^1)^2}$.

Hence $U_0 diag(\delta_1^1, \delta_2^1, \delta_3^1, \delta_4^1){U_0}^t$ is the SVD decomposition of $C_1C_1^t$.

If A is an image of size $4m \times 4m$, to every arbitrary vector (D_1^1, D_2^1, S_2^1, h^1) is associated a vector $c_1 = (c_1^1, c_2^1, c_3^1, c_4^1)$, as mentioned above, a 4×4 circulant matrix $C_1 = cir(c_1)$ and a watermark as $4m \times 4m$ matrix with one block

$$W_1 = \begin{pmatrix} C_1C_1^t & 0 & . & 0 \\ 0 & 0 & & . \\ . & & . & . \\ 0 & . & . & 0 \end{pmatrix} \tag{7}$$

To obtain a watermark W_k with k blocks

$$W_k = \begin{pmatrix} C_1C_1^t & 0 & . & . & . & 0 \\ 0 & C_2C_2^t & & & & . \\ . & & . & & & . \\ . & & & C_kC_k^t & & . \\ & & & & 0 & \\ . & & & & . & . \\ 0 & . & . & . & . & 0 \end{pmatrix} \tag{8}$$

We construct iteratively the nth block $C_nC_n^t$, $n \geq 2$ as follows:
Let $0 < D_1^n < D_1^{n-1} < .. < D_1^1$, $0 < D_2^n < D_2^{n-1} < .. < D_2^1$

And

$r_n = \sqrt{(D_1^n)^2 + (D_2^n)^2}$, $S_1^n = \frac{r_{n-1} + r_n}{2}$, $S_2^n = \frac{r_{n-1} + r_n}{4}$

Put $c_1^n = \frac{S_1^n + D_1^n}{2}$, $c_2^n = \frac{S_2^n + D_2^n}{2}$, $c_3^n = \frac{S_1^n - D_1^n}{2}$, $c_4^n = \frac{S_2^n - D_2^n}{2}$

Then

$$c_n = (c_1^n, c_2^n, c_3^n, c_4^n)$$
$$C_n = cir(c_n)$$

and the watermark with k blocks is

$$W_k = \begin{pmatrix} U_0 & 0 & . & 0 \\ 0 & . & & . \\ . & & U_0 & 0 \\ 0 & . & 0 & I \end{pmatrix} \times diag(\delta_1^1,..,\delta_4^1,\delta_1^2,..,\delta_4^2 ... \delta_1^k,..,\delta_4^k,0,..,0) \times \begin{pmatrix} U_0^t & 0 & . & 0 \\ 0 & . & & . \\ . & & U_0^t & 0 \\ 0 & . & 0 & I \end{pmatrix} \qquad (9)$$

with $\delta_1^1 \geq \delta_2^1 \geq \delta_3^1 \geq \delta_4^1 \geq \delta_1^2 \geq \cdots \geq \delta_4^k \geq 0$ and I is $4(m-k) \times 4(m-k)$ identity matrix. Hence to generate a watermark W_k with k blocks we need four arbitrary positive numbers $D_1^1 > 0$, $D_2^1 > 0$, $S_2^1 > 0$, $h^1 > 0$ for the first block and two random sequences

$$0 < D_1^k < D_1^{k-1} < .. < D_1^1$$
$$0 < D_2^k < D_2^{k-1} < .. < D_2^1$$

for other blocks; that is, the insertion key K_1 is of length 2k+2.

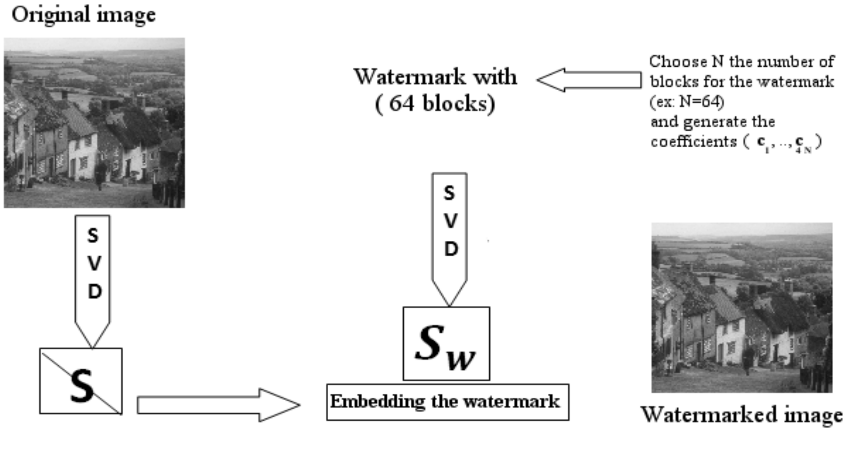

Original image
S V D
S
Watermark with (64 blocks)
Choose N the number of blocks for the watermark (ex: N=64) and generate the coefficients (c_1, .., c_{4N})
S V D
S_w
Embedding the watermark
Watermarked image

Figure 1. The proposed watermarking embedding procedure

3.2. Watermark insertion procedure

To watermark a given original image A of size $4m \times 4m$, we will use a watermark with one block as following:

1) We define the insertion key $K_1 = (D_1^1,\ D_2^1,\ S_2^1,\ h^1)$ by using four arbitrary positive numbers and construct the watermark W_1 as mentioned above.
2) Apply SVD on A : $A = U \times S \times V^t$ with $S = diag(S_i)$
3) Perform SVD on W_1 :

$$W_1 = \begin{pmatrix} U_0 & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} \partial & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} U_0{}^t & 0 \\ 0 & I \end{pmatrix} \qquad (10)$$

With $\partial = diag(\delta_1^1, \delta_2^1, \delta_3^1, \delta_4^1)$ and I is $4(m-1) \times 4(m-1)$ identity matrix.

4) Put

$$Y_i = S_i + \alpha \partial_i^{'} \qquad (11)$$

with $\partial_1^{'} = \delta_1^1$, $\partial_2^{'} = \delta_2^1$, $\partial_3^{'} = \delta_3^1$, $\partial_4^{'} = \delta_4^1$ and $\forall i > 4$ $\partial_i^{'} = 0$.

So

$$A^* = U \times diag(Y_i) \times V^t \qquad (12)$$

A^* is the watermarked image.

The figure 1 conclude the watermark insertion procedure.

3.3. Watermarking detection and extraction procedure

We don't require the original image A to detect the watermark, we only require the watermarked image A^*, the scaling factor α and the key $K_2 = (S_1, S_2, S_3, S_4)$ formed by the first four values of S .

1) Apply SVD to A^*

$$A^* = U^* \times S^* \times V^{*t} \qquad (13)$$

2) Calculate

$$x_i = \frac{S_i^* - S_i}{\alpha} \qquad (14)$$

for the first four elements.

If $x_3 = x_4$ then the mark is detected else the watermark is not present on the image.

To extract the mark we compute:

$$W^* = \begin{pmatrix} U_0 & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} X & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} U_0{}^t & 0 \\ 0 & I \end{pmatrix} \qquad (15)$$

where $X = diag(x_1, x_2, x_3, x_4)$ and I is $4(m-1) \times 4(m-1)$ identity matrix.

Remarks:

1) If we use a watermark W_k with k blocks, to detect or extract the watermark we only require the scaling factor α and a key $K_2 = (S_1, \ldots, S_{4k})$ of length 4k which contains the

first 4k values of S. In this case the sequence X $=(x_i)$ is of length 4k and the mark is detected if $x_{4i-1}=x_{4i}$ for $i=1,\ldots,k$.

2) In Chandra algorithm [5], to extract the watermark W, (U_W ,V_W) are required, in the proposed scheme $U_W = V_W$ is a constant matrix and independent of the watermark, thus our proposed algorithm is blind.

4. EXPERIMENTAL RESULTS

To demonstrate the efficiency and the performance of the proposed image watermarking scheme we implemented the proposed algorithm in Matlab, we used eight test images, of size 512 Cameraman Lena, Peppers, Baboon, Zelaine, Barbara, Goldhill and boat (Figure 2).

The quality of the watermarked image is assessed with the PSNR (Peak signal-to-noise ratio):

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)\, db \tag{16}$$

In order to evaluate the quality of the extracted watermark, we use normalized correlation (NC) metric as:

$$NC(W,W') = \frac{1}{W_h \times W_w}\sum_{i=0}^{W_h-1}\sum_{j=0}^{Ww-1} W(i,j)\times W'(i,j) \tag{17}$$

Where W_h and W_w are the height and width of the watermarked image, respectively. $W(i,j)$ and $W'(i,j)$ denote the coefficients of the inserted signature and the extracted signature respectively.

The PSNR values of the watermarked images by our method indicate that our method in general achieves very good quality as it shown in (Table 1). So the proposed method preserves good transparency for the watermarked images.

In the proposed method we have a variety for generating the watermark which can be created using n blocks, Table (2) shows the quality of the extracted watermark defined by NC under deferent image processing attacks using deferent Watermarks, the values of the NC in the table are the average values of the NC for the watermarks of the eight test images, And the scale factor $\alpha = 0.03$.

Table1. The PSNR values of the watermarked images of our method using variety of watermarks

Number of blocks	Lena	Peppers	Barbara	Baboon	GoIdhiII	Zelaine	Cameraman	Boat
1	56.6994	55.9094	56.9139	55.6458	57.2825	52.5031	56.2456	57.1737
3	55.5982	55.2634	55.5102	54.6902	55.5499	50.5651	57.7976	55.6458
5	55.7382	55.1153	57.1737	55.0781	55.4955	55.4154	55.5001	55.2064
10	55.0831	53.5932	55.2064	55.1058	55.1460	53.1938	52.1151	54.6902
30	55.8089	54.5946	53.3403	51.6568	54.6665	57.5347	52.2868	51.5035
64	56.0630	55.4747	51.5035	50.4369	54.6762	51.4444	50.4884	52.9705
80	55.4090	56.2183	50.2628	49.4199	52.9705	56.4001	49.2424	52.8710
100	55.4366	56.2190	50.1065	49.1576	52.8710	53. 3321	49.2372	52.8454
128	55.3805	56.2759	50.0764	49.2020	52.8454	51.5657	51.0011	52.8710

It is clear from the table that our method achieves a good robustness against variety of image processing attacks, furthermore, it can be seen that the rotation process is the only attack that can take a less effect on the watermark while increasing the number of blocks, while it makes the watermark more robust to other attacks.

To prove the robustness and imperceptibility of our method we compare the simulation results with many state of the art schemes

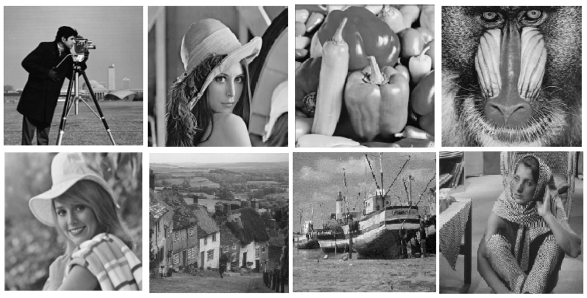
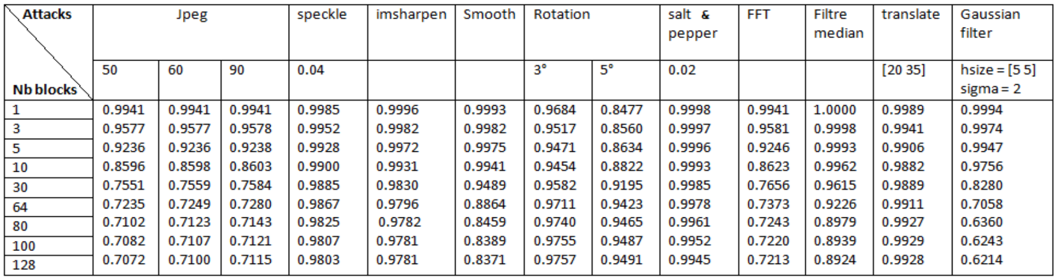


Figure 2.The host test images.

The NC values shown in table 3 indicate that our scheme achieve better robustness than other schemes in most attacks, and in the attacks that our scheme doesn't seems to be the more robust in it still achieve a good NC values >8.5.

Table 2 the robustness of the proposed method against image processing attacks using variety of watermarks



Attacks Nb blocks	Jpeg			speckle	imsharpen	Smooth	Rotation		salt & pepper	FFT	Filtre median	translate	Gaussian filter
	50	60	90	0.04			3°	5°	0.02			[20 35]	hsize = [5 5] sigma = 2
1	0.9941	0.9941	0.9941	0.9985	0.9996	0.9993	0.9684	0.8477	0.9998	0.9941	1.0000	0.9989	0.9994
3	0.9577	0.9577	0.9578	0.9952	0.9982	0.9982	0.9517	0.8560	0.9997	0.9581	0.9998	0.9941	0.9974
5	0.9236	0.9236	0.9238	0.9928	0.9972	0.9975	0.9471	0.8634	0.9996	0.9246	0.9993	0.9906	0.9947
10	0.8596	0.8598	0.8603	0.9900	0.9931	0.9941	0.9454	0.8822	0.9993	0.8623	0.9962	0.9882	0.9756
30	0.7551	0.7559	0.7584	0.9885	0.9830	0.9489	0.9582	0.9195	0.9985	0.7656	0.9615	0.9889	0.8280
64	0.7235	0.7249	0.7280	0.9867	0.9796	0.8864	0.9711	0.9423	0.9978	0.7373	0.9226	0.9911	0.7058
80	0.7102	0.7123	0.7143	0.9825	0.9782	0.8459	0.9740	0.9465	0.9961	0.7243	0.8979	0.9927	0.6360
100	0.7082	0.7107	0.7121	0.9807	0.9781	0.8389	0.9755	0.9487	0.9952	0.7220	0.8939	0.9929	0.6243
128	0.7072	0.7100	0.7115	0.9803	0.9781	0.8371	0.9757	0.9491	0.9945	0.7213	0.8924	0.9928	0.6214

Beside the robustness the proposed method has a good PSNR values and the quality of the watermarked image is very good as it is shown in Table 4 where we compared the PSNR of the watermarked images of the proposed scheme with Lai, Chih-Chin et al [20] scheme and Tsai, Hung-Hsu et al [21] scheme, the scale factors were in an interval from 0.01 to 0.09 during this the results indicate that our method has a better imperceptibility. The watermarked imagesof our proposed method looks exactly the same as the host images, so the watermarking procedure preserve the quality of the images.

TABLE 4. Comparison of PSNR for Lai, Chih-Chin et al [20]Tsai, Hung-Hsu et al [21] andour scheme.

Method	The scale factors α				
	0.01	0.03	0.05	0.07	0.09
Lai, Chih-Chin et al [20]	51.14	51.14	50.89	49.52	47.49
Tsai, Hung-Hsu et al [21]	47	37	33	28	about 25
Proposed method	56.70	56.68	56.53	55.97	55.87

5. SYSTEM SECURITY

System security of the proposed method is based on proprietary knowledge of keys which are required to embed or extract an image watermark.

As the security level is the number of observations the opponent needs to successfully estimate the secret key, the key space must be very large.

If we use a watermark with one block and for example we suppose that each of the four components $D_1^1 > 0$, $D_2^1 > 0$, $S_2^1 > 0$, $h^1 > 0$ of the key K_1 has r decimal digits, in this case the size of key space of K_1 equals $10^{4r} \succ 2^{12r}$; then for $r \geq 15$ the size of key space of K_1 is very large, we have the same result for the extraction key K_2 .

The security of our technique can be improved by increasing *k* the number of watermark blocks and the complexities can be controlled by manipulation of *k*.

6. APPLICATIONS

We now describe some applications of the proposed method.

6.1. Copyright protection

Protection of intellectual property has become a prime concern for creators and publishers of digital contents. To solve the problem of legal ownership for digital multimedia data, it must use “digital watermark”, there is need to be associated additional information with a digital content, a copyright notice may need to be associated with an image to identify the legal owner, a serial number to identify a legitimate user.

For our method the distributor generates an insertion key

$$K_1 = (D_1^1, D_2^1, S_2^1, h^1)$$

Where h^1 is the information about the copyright owner and $S_2^1$is the information about the receiver, he embeds the associated watermark in the host image and sends the watermarked image to the legitimate receiver. The extraction key K_2 or the algorithm will only be known by the distributor and other trusted parties. For the proof of the ownership of the embedded image, using the key K_2 , the distributor extracts the mark and calculates the singular values $(\delta_1^1, \delta_2^1, \delta_3^1, \delta_4^1)$

and according to the choice of $c_1^1, c_2^1, c_3^1, c_4^1$ and by (4) deduces the copyright notice.

$$h^1 = \sqrt{\delta_2^1} - \sqrt{\delta_3^1}$$

and serial number of the user

$$S_2^1 = \frac{\sqrt{\delta_1^1} - \sqrt{\delta_2^1}}{2}$$

In order to solve the deadlock problem [19], in generation of K_1 , D_1^1 and D_2^1 can be computed from the host image *A* using a secure hash function *f* for example let:

$$D_1^1 = f(A)$$
$$D_2^1 = f(A^t)$$

The second key K_2 is also original image dependent, this makes counterfeiting very difficult. The proposed scheme for copyright protection is resumed in figure 3.

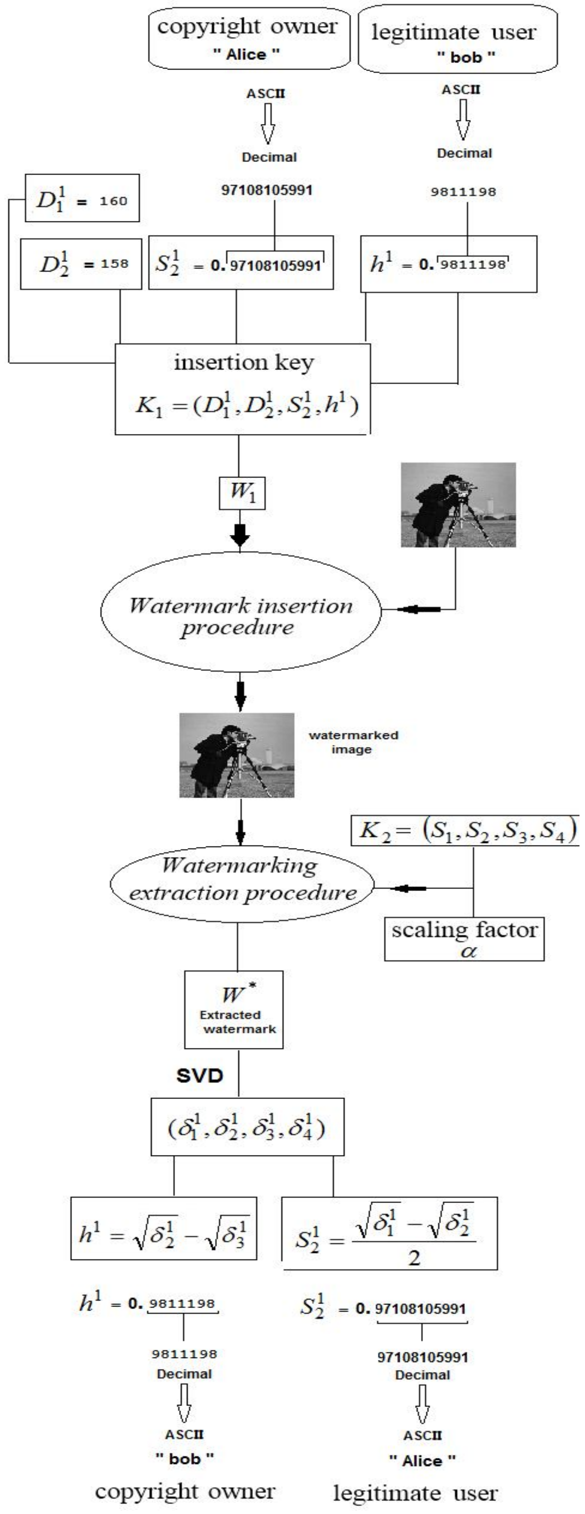


Figure 3. the proposed scheme for copyright protection

6.2. Illicit distribution

By using the internet, the online purchasing and distribution of digital images can be performed easily. The good distribution scheme is to distribute data without the possibility for the receivers to redistribute it to unauthorized user.

If a user illegally distributes an image then, as above by extraction procedure, we obtain
$h^1 = \sqrt{\delta_2^1} - \sqrt{\delta_3^1}$
the serial number of the user, so that redistributed copies can be traced back to the pirate.

6.3. Copy control

Embedding mark in an image can prevent illegal copying, for our proposed scheme we can use the second bloc and we take $D_1^2 < D_1^1 , D_2^2 < D_2^1$ Then by (4) we have $(D_1^2)^2 + (D_2^2)^2 = \delta_3^2 = \delta_4^2$

Hence δ_3^2 can be considered for example as information about “no copy”, in this way a copying device might inhibit coping of image if it detects an information (δ_3^2) in watermark that indicates coping is prohibited, for this application, copying device must include watermark detection circuitry.

We can increase the number of blocks of W_k so that the mark contains other information as addresses or distribution path parameters.

Then the number of blocks of the watermark is related to the desired capacity.

7. CONCLUSION

In this paper we have proposed a new blind robust watermarking technique which originality stands on using positive semi-definite matrices for which the spectral decomposition coincides with the singular value decomposition.
The proposed watermarking scheme is robust against a wide variety of attacks, as indicated in the experimental results Moreover, the scheme overcomes the drawbacks of the deadlock problem, and the comparison analysis shows that our scheme provides a higher capacity and achieves better image quality for watermarked images, and it can be used for discouraging illicit copying and distribution of copyright material.

REFERENCES

[1] Surekha, B., and G. N. Swamy. "A spatial domain public image watermarking." International Journal of Security and Its Applications 5.1 (2011): 12.

[2] Nasir, Ibrahim, Ying Weng, and Jianmin Jiang. "A new robust watermarking scheme for color image in spatial domain." Signal-Image Technologies and Internet-Based System, 2007. SITIS'07. Third International IEEE Conference on. IEEE, 2007.

[3] Mukherjee, Dipti Prasad, SubhamoyMaitra, and Scott T. Acton. "Spatial domain digital watermarking of multimedia objects for buyer authentication." Multimedia, IEEE Transactions on 6.1 (2004): 1-15.

[4] Wang, Feng-Hsing, Lakhmi C. Jain, and Jeng-Shyang Pan. "Genetic watermarking on spatial domain." Intelligent Watermarking Techniques 7 (2004): 377.

[5] Chandra, DV Satish. "Digital image watermarking using singular value decomposition." Circuits and Systems, 2002. MWSCAS-2002. The 2002 45th Midwest Symposium on. Vol. 3. IEEE, 2002..

[6] Chang, Chin-Chen, Piyu Tsai, and Chia-Chen Lin. "SVD-based digital image watermarking scheme." Pattern Recognition Letters 26.10 (2005): 1577-1586.

[7] Al-Haj, Ali. "Combined DWT-DCT digital image watermarking." Journal of computer science 3.9 (2007): 740.

[8] W. H. Lin, Y. R. Wang, and S. J. Horng, "A Blind Watermarking Scheme Based on Wavelet Tree Quantization," The Second International Conference on Secure System Integration and Reliability Improvement, 2008, pp. 89-94

[9] Ghouti, Lahouari, et al. "Digital image watermarking using balanced multiwavelets." Signal Processing, IEEE Transactions on 54.4 (2006): 1519-1536.

[10] Zheng, Dong, Jiying Zhao, and Abdulmotaleb El Saddik. "RST-invariant digital image watermarking based on log-polar mapping and phase correlation." Circuits and Systems for Video Technology, IEEE Transactions on 13.8 (2003): 753-765. . .

[11] Ouhsain, Mohamed, and A. Ben Hamza. "Image watermarking scheme using nonnegative matrix factorization and wavelet transform." Expert Systems with Applications 36.2 (2009): 2123-2129.

[12] Oussama, Noui, and Noui Lemnouar. "A blind robust watermarking scheme based on SVD and circulant matrices." Second International Conference on Computational Science & Engineering (CSE - 2014). pp 65-77

[13] R. Liu and T. Tan, "A SVD-based watermarking scheme for protecting rightful ownership," IEEE Transactions on Multimedia, vol. 4, no. 1, pp. 121-128, 2002.

[14] E. Ganic and A. M. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies," ACM Multimedia and Security Workshop 2004, Germany, 2004, pp. 20-21.

[15] C.H. Lin, J.C. Liu, and P.C. Han, "On the security of the full-band image watermark for copyright protection," IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2008, pp. 74-79.

[16] Mukherjee, Soumya, and Arup Kumar Pal. "A DCT-SVD based robust watermarking scheme for grayscale image." In Proceedings of the International Conference on Advances in Computing, Communications and Informatics, pp. 573-578. ACM, 2012.

[17] Yang, Jar-Ferr, and Chiou-Liang Lu. "Combined techniques of singular value decomposition and vector quantization for image coding." Image Processing, IEEE Transactions on 4, no. 8 (1995): 1141-1146.

[18] Bhatia, Rajendra. Positive definite matrices. Princeton University Press, 2009.

[19] Craver, Scott, Nasir Memon, Boon-Lock Yeo, and Minerva M. Yeung. "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications." Selected Areas in Communications, IEEE Journal on 16, no. 4 (1998): 573-586..

[20] Lai, Chih-Chin, and Cheng-Chih Tsai. "Digital image watermarking using discrete wavelet transform and singular value decomposition." Instrumentation and Measurement, IEEE Transactions on 59, no. 11 (2010): 3060-3063.

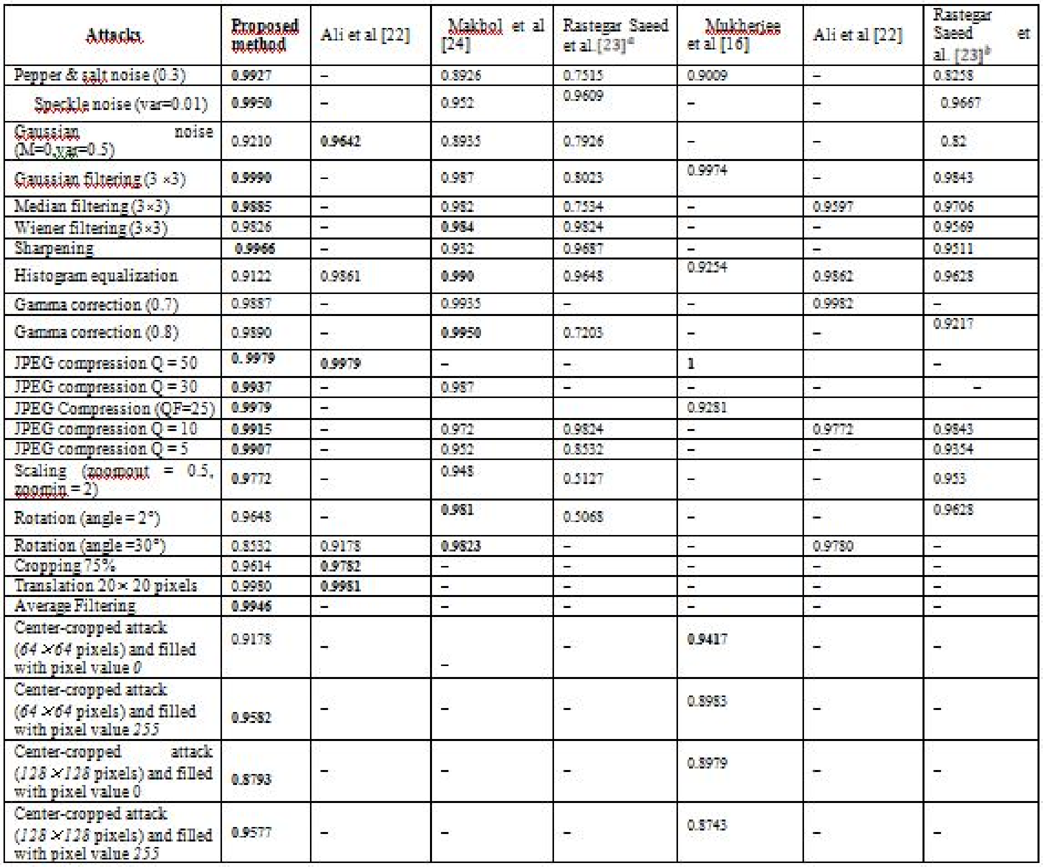
[21] Tsai, Hung-Hsu, Yu-JieJhuang, and Yen-Shou Lai. "An SVD-based image watermarking in wavelet domain using SVR and PSO." Applied Soft Computing 12, no. 8 (2012): 2442-2453.

[22] Ali, Musrrat, and Chang WookAhn. "An optimized watermarking technique employing SVD in DWT domain." In Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, p. 86. ACM, 2013.

[23] Rastegar, Saeed, FatemeNamazi, KhashayarYaghmaie, and Amir Aliabadian. "Hybrid watermarking algorithm based on Singular Value Decomposition and Radon transform." AEU-International Journal of Electronics and Communications 65, no. 7 (2011): 658-663.

[24] Makbol, Nasrin M., and Bee EeKhoo. "Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition." AEU-International Journal of Electronics and Communications 67, no. 2 (2013): 102-112.

Table 3. Comparison of robustness of our scheme and other state of the art schemes



Attacks	Proposed method	Ali et al [22]	Makhol et al [24]	Rastegar Saeed et al. [23]^a	Mukherjee et al [16]	Ali et al [22]	Rastegar Saeed et al. [23]^b
Pepper & salt noise (0.3)	**0.9927**	–	0.8926	0.7515	0.9009	–	0.8258
Speckle noise (var=0.01)	**0.9950**	–	0.952	0.9609	–	–	0.9667
Gaussian noise (M=0,var=0.5)	0.9210	**0.9642**	0.8935	0.7926	–	–	0.82
Gaussian filtering (3 ×3)	**0.9990**	–	0.987	0.8023	0.9974	–	0.9843
Median filtering (3×3)	**0.9885**	–	0.982	0.7534	–	0.9597	0.9706
Wiener filtering (3×3)	0.9826	–	**0.984**	0.9824	–	–	0.9569
Sharpening	**0.9966**	–	0.932	0.9687	–	–	0.9511
Histogram equalization	0.9122	0.9861	**0.990**	0.9648	0.9254	0.9862	0.9628
Gamma correction (0.7)	0.9887	–	0.9935	–	–	0.9982	–
Gamma correction (0.8)	0.9890	–	**0.9950**	0.7203	–	–	0.9217
JPEG compression Q = 50	**0. 9979**	**0.9979**	–	–	**1**		–
JPEG compression Q = 30	**0.9937**	–	0.987	–	–	–	–
JPEG Compression (QF=25)	**0.9979**	–			0.9281		
JPEG compression Q = 10	**0.9915**	–	0.972	0.9824	–	0.9772	0.9843
JPEG compression Q = 5	**0.9907**	–	0.952	0.8532	–	–	0.9354
Scaling (zoomout = 0.5, zoomin = 2)	**0.9772**	–	0.948	0.5127	–	–	0.953
Rotation (angle = 2°)	0.9648	–	**0.981**	0.5068	–	–	0.9628
Rotation (angle =30°)	0.8532	0.9178	**0.9823**	–	–	0.9780	–
Cropping 75%	0.9614	**0.9782**	–	–	–	–	–
Translation 20× 20 pixels	0.9980	**0.9981**	–	–	–	–	–
Average Filtering	**0.9946**	–	–	–	–	–	–
Center-cropped attack (*64 ×64* pixels) and filled with pixel value *0*	0.9178	–	–	–	**0.9417**	–	–
Center-cropped attack (*64 ×64* pixels) and filled with pixel value *255*	**0.9582**	–	–	–	0.8983	–	–
Center-cropped attack (*128 ×128* pixels) and filled with pixel value 0	**0.8793**	–	–	–	0.8979	–	–
Center-cropped attack (*128 ×128* pixels) and filled with pixel value *255*	**0.9577**	–	–	–	0.8743	–	–