A Robust Image Watermarking Scheme using Singular Value Decomposition

B.Chandra Mohan
JNTU College of Engineering, ECE Department, Kakinada, India
chandrabhuma@yahoo.co.in

S. Srinivas Kumar
JNTU College of Engineering, ECE Department, Kakinada, India
Email: samay_ssk2@yahoo.com

***Abstract*— This paper presents a robust image watermarking scheme for multimedia copyright protection. In this work, host image is partitioned into four sub images. Watermark image such as 'logo' is embedded in the two of these sub images, in both D (singular and diagonal matrix) and U (left singular and orthogonal matrix) components of Singular Value Decomposition (SVD) of two sub images. Watermark image is embedded in the D component using Dither quantization. A copy of the watermark is embedded in the columns of U matrix using comparison of the coefficients of U matrix with respect to the watermark image. If extraction of watermark from D matrix is not complete, there is a fair amount of probability that it can be extracted from U matrix. The proposed algorithm is more secure and robust to various attacks, viz., JPEG2000 compression, JPEG compression, rotation, scaling, cropping, row-column blanking, row-column copying, salt and pepper noise, filtering and gamma correction. Superior experimental results are observed with the proposed algorithm over a recent scheme proposed by Chung et al. in terms of Bit Error Rate (BER), Normalized Cross correlation (NC) and Peak Signal to Noise Ratio (PSNR).**

***Index Terms*— Digital image watermarking, Singular values, Singular value decomposition, Dither quantization.**

I. INTRODUCTION

Digital image watermarking has received increasing attention in recent times due to rapid growth in the internet traffic. It is gaining popularity due to its significance in content authentication and copyright protection for digital multimedia data. A digital watermark is a sequence of information containing the owner's copyright for the multimedia data [1]. It is inserted invisibly in another image (host image) so that it can be extracted at later times for the evidence of rightful ownership. Digital image watermarking techniques can be categorized into one of the two domains, viz., spatial and transform, according to the embedding domain of the host image. The simplest technique in the spatial domain methods is to insert the watermark image pixels in the least significant bits (LSB) of the host image pixels [2,3]. The data hiding capacity in these methods is high. However, these methods are hardly robust. Watermarking in transform domain is more secure and robust to various attacks. Image watermarking algorithms using Discrete Fourier Transform (DFT) [4], Discrete Cosine Transform (DCT) [5,6], Discrete Wavelet Transform (DWT) [7,8] and Singular Value Decomposition (SVD) [9,10,11,12,13,14,15,16,17,18] are available in the literature. The basic philosophy in majority of the transform domain watermarking schemes is to modify transform coefficients based on the bits in the watermark image. Most of the domain transformation watermarking schemes works with DCT and DWT. However, SVD is one of the most powerful numerical analysis technique and used in various applications.

Gorodetski et al. [9] used SVD domain for watermarking a 600x512 RGB image. They quantized the Singular Value (SV) of each 4x4 block of R, G and B. The watermark is a 240x120 gray scale image. But, this is shown to resist only for JPEG compression. Liu and Tan [10] applied SVD to the entire host image. The watermark is a pseudo gaussian random number matrix weighed with appropriate scaling factor is added to the diagonal matrix of SVs. The modified D (Diagonal matrix) is inserted back in the host image. This method is able to resist Gaussian Noise, Gaussian Low pass filter, JPEG with 5% compression, rotation of 30^0 and cropping. Chandra et al.[11] proposed a method based on the SVD of both the host image and visual watermark. The SVs of the watermark are multiplied by a scaling factor and added to the SVs of the host image. The attacks used are JPEG (QF =25 and 10), and 3x3 low pass filter. But this method is non-blind in nature. In 2002, Sun et al. [12] proposed an SVD based watermarking scheme, wherein the D component with a diagonal matrix is explored for embedding. The basic mechanism used was the quantization of the largest component with a fixed constant integer, called Quantization coefficient. A trade-off can be achieved between transparency and robustness by varying the quantization coefficient. However, this method failed in extracting the watermark with zero error rate. The original watermark image and retrieved watermark image are not exact. Later in 2005, Chang et

al. [13] proposed a watermarking scheme based on the SVD domain. U matrix of SVD is used for the watermark embedding. The absolute difference between the two rows of U matrix is used for the watermark embedding. They explored the positive relationships between the rows of U and V matrices that are preserved after JPEG compression also. The attacks shown in their work are only JPEG compression, noise, cropping, sharpening, blurring and tampering. Kumar et al. [14] have proposed a singular value decomposition based image watermarking scheme using dither quantization. Recently, Chung [15] et al., proposed two notes on the SVD based watermarking algorithm. As per the proposal from Chung et al. if the watermark is embedded in the columns of U matrix and rows of V^T, the perceptibility of the host image is improved. But, the proposed method by Chung et al., is not robust to many attacks since watermark embedding is in U and V^T matrices. Magnitudes of U and V matrix elements are very small and so, even a small modification in either U or V components alters the watermark retrieval. Many of the algorithms proposed above suffer from either with the poor robustness or non-blind in nature.

In this work, a watermarking scheme is proposed which is robust, reasonably good capacity (32x32 logo is embedded in 512x512 image) and blind in nature. The proposed method uses SVD domain and Dither quantization for embedding the watermark in both D and U. Magnitudes of D matrix coefficients are very high compared to both U and V. In the proposed method, the largest singular values of the host image (D matrix coefficients) and coefficients of the U matrix are modified to embed the watermark data such as logo. The host image is partitioned into four sub images. Instead of using the entire host image for watermark embedding, only two sub images of size 256x256 are used. This is to ensure that the visual quality of the watermarked image is not degraded. With the two sub images for watermark embedding, a reasonably good quality image with a Peak Signal to Noise Ratio (PSNR) [14] of more than 40 dB can be obtained. The choice of the top left and bottom right is purely arbitrary. The number of sub images can be increased by partitioning the host image. However, the information hiding capacity is reduced. The results are compared with the Chung et al. method. After extensive experimentation with various image attacks, it is believed that the proposed watermarking scheme is superior to Chung et al., method in terms of performance indices Bit Error Rate (BER) [15], Normalized Cross correlation (NC) [14] and PSNR values.

The rest of the paper is organized as follows. SVD transformation is discussed in section II. Dither quantization is discussed in section III. Proposed algorithm is elaborated in section IV. Experimental results are given in section V. Concluding remarks are given in section VI.

II. Singular Value Decomposition (SVD)

SVD is a mathematical tool used to analyze matrices. In SVD, a square matrix is decomposed into three matrices of same size. For example, a real matrix A of size $N \times N$ can be decomposed into a product of 3 matrices $A = UDV^T$, where U and V are orthogonal matrices such that $U^T U = I$, $V^T V = I$ and D=diag $(\lambda_1, \lambda_2, ...)$. '$I$' is an identity matrix. The diagonal entries are called the singular values of A, the columns of U are called the left singular vectors of A, and the columns of V are called the right singular vectors of A. This decomposition is known as the Singular Value Decomposition (SVD) of A, and can be written as

$$SVD(A) = [U \quad D \quad V] \tag{1}$$

$$SVD(A) = \lambda_1 U_1 V_1^T + \lambda_2 U_2 V_2^T + ... + \lambda_r U_r V_r^T \tag{2}$$

$$A' = UDV^T \ . \tag{3}$$

U and V are the real $N \times N$ unitary matrices with small singular values. D is a diagonal matrix of $N \times N$ size with large singular values. Here, r is the rank of matrix A. A' is the reconstructed matrix after applying the inverse SVD transformation. The singular values satisfy the relation $\lambda_1 \geq \lambda_2 \geq ... \lambda_r \geq 0$.

Singular values represent the algebraic properties of an image [17]. Singular values possess the algebraic and geometric invariance to some extent. The properties of the singular values are reviewed as follows.

A. Theorem 1 (SVD).

If $A \in R^{mxn}$, then there exist orthogonal matrices

$$U = [u_1, ..., u_m] \in R^{mxn} \text{ and } \quad V = [v_1, ..., v_n] \in R^{mxn}$$

such that $U^T AV = diag(\sigma_1, ..., \sigma_p)$.

where, $p = \min(m, n), \sigma_1 \geq \sigma_2 \geq ... \sigma_p \geq 0.$ σ_i, i=1,2,…p are the singular values of A. The singular values are the square roots of the eigen values λ_i of AA^H or $A^H A$, that is $\sigma_i = \sqrt{\lambda_i}$.

B. Theorem 2 (The stability of SV).

The stability of singular value indicates that, when there is a little disturbance with A, the variation of its singular value is not greater than 2-norm of disturbance matrix. 2-norm is equal to the largest singular value of the matrix.

C. Theorem 3 (The scaling property).

If the singular values of A^{mxn} are $\sigma_1, \sigma_2, ... \sigma_k$, the singular values of $\alpha * A^{mxn}$ are $\sigma_1^*, \sigma_2^*, ... \sigma_k^*$, then

$$|\alpha|(\sigma_1, \sigma_2, ...\sigma_k) = (\sigma_1^*, \sigma_2^*, ...\sigma^*_k). \quad (4)$$

D. Theorem 4 (The rotation invariant property).

If *P* is a unitary and rotating matrix, the singular values of *PA (rotated matrix)* are the same as those of *A*.

E. Theorem 5 (The translation invariance property).

The original image *A* and its rows or columns interchanged image have the same singular values.

F. Theorem 6 (The transposition invariance property).

$$\text{If} \quad AA^T u = \lambda^2 u$$

$$\text{then,} \quad A^T Av = \lambda^2 v, \quad (5)$$

so that *A* and A^T have same singular values.

The above mentioned (stability of SV, scaling invariance of SV, rotational invariance of SV, translation and transposition invariance of SV) properties of SVD are very much desirable in image watermarking. When the watermarked image undergoes attacks like rotation, scaling and noise addition, the watermark can be retrieved effectively from the attacked watermarked image due to the above said properties.

III. Dither Quantization

In an ideal watermarking scheme, one signal (a digital watermark) is embedded within another signal (host image) signal to form a third signal (watermarked image) signal. The embedding should be done in such a way that minimizes the distortion between the host signal and watermarked signal and maximizes the information embedding rate and robustness of the embedding. All the three requirements are usually conflicting, and hence embedding process must be designed to efficiently trade-off these requirements. In the Dither quantization based watermarking schemes, the embedded information modulates a dither signal and the host signal is quantized with an associated dithered quantizer. Dither quantization based schemes have considerable performance advantages over conventional spread spectrum based schemes [20]. The conventional spread sprectrum embedding function combines the host image and the watermark image in a linear way, and hence the watermark image can be extracted with ease. In contrast, dither quantization based schemes effectively hide the exact value of the host signal.

In the proposed watermarking scheme, a binary watermark is embedded in the gray scale host image. A binary watermark image consists of '1's or '0's. Dither quantizers are quantizer ensembles [21]. Each quantization cell in the ensemble is constructed from a basic quantizer. The basic quantizer is shifted to get the reconstruction point. The shift depends on the watermark bit. The basic quantizer is a uniform scalar quantizer with a fixed step size *T*. A quantizer in the ensemble consists of two quantizers shifted by *T/2* with respect to each other. The largest component of *D* matrix of an 8x8 block is quantized using either quantizer 1 or quantizer 2 that depends on watermark bit to be embedded. The quantized value is the center of the quantizer.

IV. Proposed Method

In the proposed method, the D matrix and U matrix are explored for embedding the watermark. The D component matrix contains the largest coefficients. These coefficients are modified in such a way that the watermarked image quality is not degraded. The modification of the coefficients is based on the Dither quantization. After the modification of singular values, inverse SVD is applied and the watermarked image is obtained. The watermark embedding algorithm is presented in the following steps:

A. Host Image Partition:

1. The host image $f(i, j)$ of size $N \times N$ is partitioned into four sub images as shown in Fig. 2. The watermark image is permuted with a secret key *K*.

2. Four sub images $f_{tl}(p,q)$ (top left), $f_{tr}(p,q)$ (top right), $f_{bl}(p,q)$ (bottom left) and $f_{br}(p,q)$ (bottom right) of the host image are defined as

$$f_{tl}(p,q) = f(i,j) \quad \begin{matrix} 1 \le i \le N/2, \\ 1 \le j \le N/2 \end{matrix} \quad (6)$$

$$f_{tr}(p,q) = f(i,j) \quad \begin{matrix} 1 \le i \le N/2, \\ N/2+1 \le j \le N \end{matrix} \quad (7)$$

$$f_{bl}(p,q) = f(i,j) \quad \begin{matrix} N/2+1 \le i \le N, \\ 1 \le j \le N/2 \end{matrix} \quad (8)$$

$$f_{br}(p,q) = f(i,j) \quad \begin{matrix} N/2+1 \le i \le N, \\ N/2 \le j \le N \end{matrix} \quad (9)$$

where, $1 \le p \le N/2$ *and* $1 \le q \le N/2$.

The watermark is embedded in the sub images $f_{tl}(p,q)$ and $f_{br}(p,q)$ only to improve imperceptibility of the watermark in the watermarked image and hence better PSNR.

B. Watermark Embedding in D Matrix:

3. Block based SVD Transformation is applied on $f_{tl}(p,q)$, $1 \le p \le N/2$ *and* $1 \le q \le N/2$ with a block size of $M \times M$.

TABLE I. QUANTIZATION TABLE FOR THE LARGEST SINGULAR VALUES

bin no.	d_{low}	d_{high}
1	d_{min} - T	d_{min}
2	d_{min}	$d_{min}+T$
3	$d_{min}+T$	$d_{min}+2T$
b_{n-1}	d_{max} - T	d_{max}
.	..	..
.	..	..
b_n	d_{max}	$d_{max}+T$

4. From each block of D matrix , obtain the largest coefficient $D(1,1)$. From these $D(1,1)$'s, a matrix D_{large} is formed. The size of D_{large} is, same as that of watermark image.

5. The entire range d_{min} (minimum value of D_{large}) to d_{max} (maximum value of D_{large}) is divided into various bins as shown in Table I. A step size of T is taken as the difference from one bin to another bin.

6. Each element of D_{large} matrix is checked for its position in Table I.

After identifying the bin number, D_{large} is modified as follows:
(i)If watermark bit is '1' then it belongs to *Range1,* where *Range1* is defined as

$$Range1 = d_{low}(n) \quad \text{to} \quad \frac{d_{low}(n)+d_{high}(n)}{2} \tag{10}$$

D_{large} is modified as

$$D_{large} = \frac{d_{low}(n)+(d_{low}(n)+d_{high}(n))/2)}{2} \tag{11}$$

(ii)If watermark bit is '0' then it belongs to *Range2* where *Range2* is defined as

$$Range2 = \frac{d_{low}(n)+d_{high}(n)}{2} \text{ to } d_{high}(n) \tag{12}$$

D_{large} is modified as

$$D_{large} = \frac{d_{high}(n)+(d_{low}(n)+d_{high}(n))/2)}{2} \tag{13}$$

7. After the modification applied in step 6, inverse SVD is applied to get the first portion of the watermarked image $f_{tlw}(p,q)$.

Robustness of the method against attacks and imperceptibility of watermark image can be improved with the increase in the number of bins and the decrease in step size.

C. Watermark Embedding in U Matrix:

8. Block based SVD Transformation is applied on sub image $f_{br}(p,q)$, $1 \le p \le N/2$ *and* $1 \le q \le N/2$ with a block size of $M \times M$.
9. Watermark image $w(i,j)$, $1 \le i \le N/2M$ *and* $1 \le j \le N/2M$ is embedded in the columns of each block of U matrix. For each $M \times M$ block of U matrix, u_{11} (first row 1st column) and u_{21} (2nd row 1st column) are modified as follows:

$$u_{diff} = |u_{11}| - |u_{21}|$$

$$\text{If} \quad w(i,j)=1 \;\&\; u_{diff} > \alpha$$
$$\text{or}$$
$$w(i,j)=0 \;\&\; u_{diff} < \alpha$$
$$u_{21} = -\left|\,|u_{21}| - (\alpha - u_{diff})/2\right|$$
$$u_{11} = -\left|\,|u_{11}| + (\alpha - u_{diff})/2\right| \tag{14}$$

$$\text{If} \quad w(i,j)=1 \;\&\; u_{diff} < \alpha$$
$$\text{or}$$
$$w(i,j)=0 \;\&\; u_{diff} > \alpha$$
$$u_{21} = -\left|\,|u_{21}| - (\alpha + u_{diff})/2\right|$$
$$u_{11} = -\left|\,|u_{11}| + (\alpha + u_{diff})/2\right| \tag{15}$$

where '| |' indicates the absolute value. The above modification is applied to the coefficients of each block of U matrix. Here, α is a constant.

10. After the modification of U matrix coefficients, inverse SVD is applied to each block to get the second portion of the watermarked image $f_{brw}(p,q)$.
11. All the sub images $f_{tlw}(p,q)$, $f_{tr}(p,q)$, $f_{bl}(p,q)$, and $f_{brw}(p,q)$ are combined appropriately to get the final watermarked image $F(i,j)$.

Watermark embedding strategy adopted here in the U matrix is in similar lines to Chung et al. method. For certain image attacks like gamma correction, contrast and brightness enhancement, watermark embedding using comparison of the magnitudes of columns of U matrix proves to be superior to the absolute modification of the coefficients using Dither quantization. Similar strategy works well for the rows of V^T matrix. Flowchart for the embedding scheme is shown in Fig. 1.

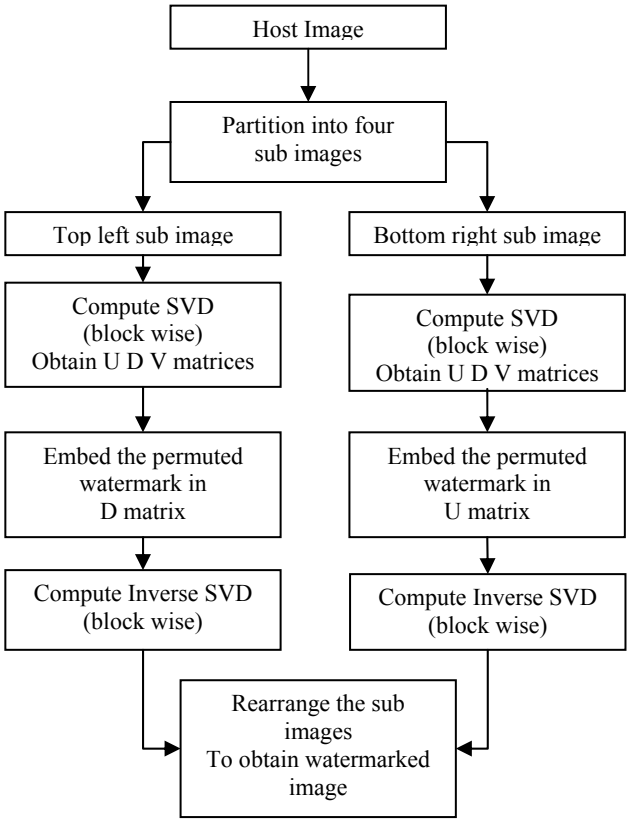


Figure 1. Flowchart for embedding watermark

D. Watermarked Image (F(i,j)) Partition:

1. The watermarked image $F(i, j)$ of size $N \times N$ is partitioned into four quarters and four sub images $f_{tlw}(p,q)$ (top left watermarked), $f_{tr}(p,q)$ (top right un marked) , $f_{bl}(p,q)$ (bottom left un marked) and $f_{brw}(p,q)$ (bottom right watermarked) are obtained .

E. Watermark Extraction from D Matrix

2. SVD transformation is applied on top left portion $f_{tlw}(p,q)$.

3. From each block of *D* matrix obtained from SVD of $f_{tlw}(p,q)$, the largest coefficient *D(1,1)* is extracted.

4. The value of *D(1,1)*is checked for its positioning the quantization table (Table I). From this step, bin position is identified.

5. From the bin position obtained in step 4, now the *D(1,1)* value is checked for its position, *Range1* or *Range2.* If it is in *Range1*, the watermark bit is '1'. Otherwise, the watermark bit is '0'.

Steps 1 to 5 are repeated for all the largest coefficients of all the blocks of D component. In this way, the watermark image of size $\frac{N}{2M} \times \frac{N}{2M}$ is extracted. The original watermark image is extracted from the permuted one by using the secret key K.

F. Watermark Extraction from U Matrix:

6. SVD transformation is applied on the watermarked sub image $f_{brw}(p,q)$.

7. Elements u_{11} and u_{21} of U matrix generated from the previous step are compared for generating watermark.

   $w(i, j) = 1$ if $|u_{11}| > |u_{21}|$ for $1 \le i \le N/2,$ $1 \le j \le N/2$

   $w(i, j) = 0$ otherwise.

8. Watermark image is extracted from the permuted one by using the secret key *K*.

Flowchart for the extraction of watermark is given in Fig. 2.

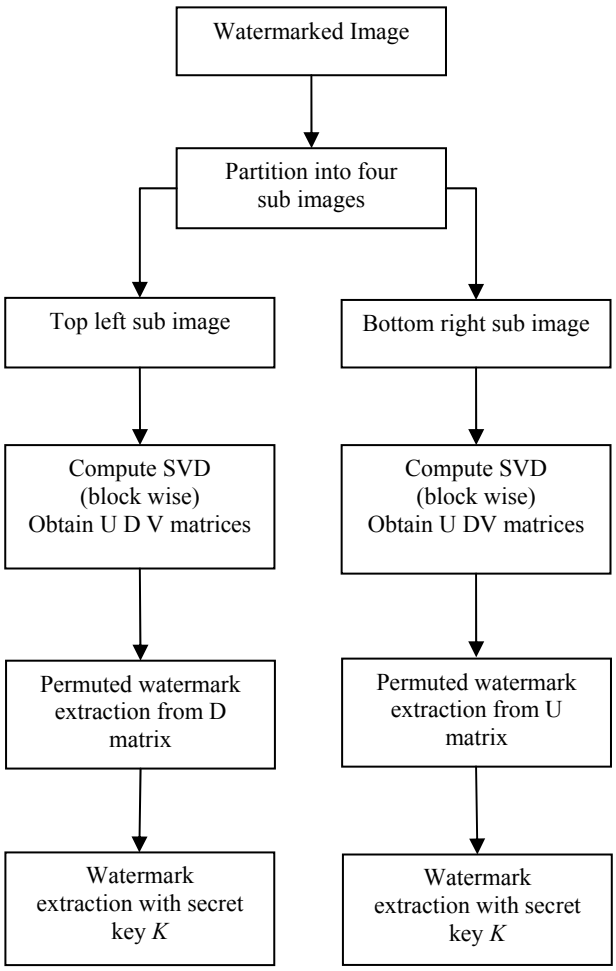


Figure 2. Flowchart for extracting watermark

Figure 3(a). Host image Lena (512x512) (b). Watermark image (c). Permuted watermark image

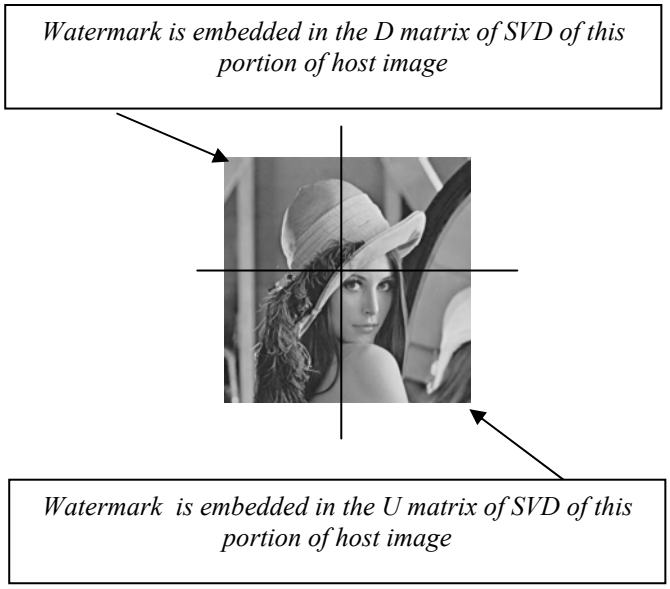


Figure 4. Partitioned host image Lena

TABLE II: COMPARISON OF THE PROPOSED WATERMARKING METHOD AND THE METHOD OF [15]

Type of Attack	Chung et al. [15] Method (Threshold=0.012)		Best BER & NC Proposed Method	
	BER	NC	BER	NC
JPEG QF=70	0.072	0.745	0	1
Gaussian Noise 5%	0.061	0.765	0.027	0.88
Cropping 25% (Upper left area)	0.059	0.782	0	1

Figure 5. 512x512 Watermarked Lena (PSNR= 43.11 dB)

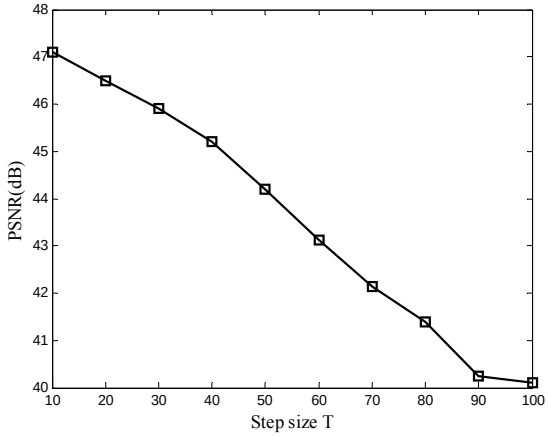


Figure 6. Step size (T) vs PSNR (dB)

V. EXPERIMENTAL RESULTS

The host image considered for the experimentation is 512 x 512 Lena, as shown in Fig. 3(a). The watermark image is of 32 x 32 size which is a logo as shown in Fig. 3(b). Fig. 3(c) shows the permuted watermark image. The host image is partitioned into four sub images. The watermark is embedded in two sub images as shown in Fig. 4. The parameters used in the simulations are step size of T=60, blocksize of MxM is 8x8 and $\alpha = 0$. Fig. 5 indicates that visual appearance of the watermarked image is good with a PSNR of 43.11 dB, showing no significant artefacts or distortions because of the process of watermarking. PSNR of the watermarked image in the case of Chung et al. method is 38.69 dB. Step size T can be decreased further to get a better PSNR, but the robustness suffers. The variation of PSNR (in dB) with step size T is shown in Fig. 6. An optimum value of T=60 is selected in the experimentation. The performance of the proposed algorithm has been tested using MATLAB software version 7.0. The metrics used to assess the performance of the proposed algorithm are PSNR, NC and BER. BER is the ratio of number of erroneous bits in the extracted watermark (compared to the original watermark) to the total number of bits of the watermark image. A comparison of the proposed method with Chung et al. method is given in Table II.

The attacks used to test the robustness of the watermark are JPEG2000, JPEG compression, rotation,

resizing, low pass filtering, median filtering, cropping, row column blanking, row column copying, salt and pepper noise, bit plane removal, image tampering and gamma correction. JPEG2000 attack is tested using the MORGAN JPEG2000 tool box [19]. The extracted watermarks after applying various attacks are shown in Figs. 7,8 & 9. The PSNR values of the attacked images are indicated at the bottom of the figure. The numbers in the bracket indicates NC value and BER value respectively.

The watermarked image is compressed using lossy JPEG compression. The index of the JPEG compression ranges from 0 to 100, where 0 is the best compression and 100 is the best quality. The proposed scheme works well even for extreme compression. Similarly, JPEG2000 compression is used to test the robustness with varying quality factor. The results are found to be good indicating that the proposed method is able to survive after JPEG2000 compression.

The watermarked image is rotated by 20^0 to the right and then rotated back to their original position using bilinear interpolation. The resizing operation initially reduces or increases the size of the image and then generates the original image by using an interpolation technique. This operation is a lossy operation and hence the watermarked image also looses some watermark information. In this experiment, initially the watermarked image size is reduced from 512x512 to 256x256. Later, its dimensions are increased to 512x512 by using bilinear interpolation.

For low pass filtering attack, a 3x3 mask consisting of 0.9 intensity values is used. The median filter is a non linear spatial filter which is usually used to remove noise spikes from an image. The watermarked image is attacked by median filtering with a 3x3 mask.

The cropping operation (lossy operation) deletes some portion of the image. The extracted watermark is still recognizable even after 25% of cropping. In row column blanking attack, a set of rows and columns are deleted. In this experiment 10,30,40,70,100,120 &140 of rows and columns are removed. The extracted watermark showed good similarity with the original watermark.

In row-column copy attack, a set of rows and columns are copied to the adjacent or random locations. In this experiment, 10^{th} row is copied to 30^{th} row, 40 to 70, 100 to 120 and 140^{th} row is copied to 160^{th} row. The extracted watermark is clearly visible. The watermarked image is attacked by salt and pepper noise with a noise density of 0.01. The extracted watermark is still recognizable but, not good as compared to the watermark, extracted by various other attacks, except rotation. In bit plane removal attack, the least significant bits of the watermarked image pixel intensity values are made '0'. In gamma correction, the intensity of the watermarked image is changed according to a predefined intensity transformation. The proposed algorithm is also resilient to bitplane removal and gamma correction, as shown in Fig. 8. The watermark image can be extracted even after adjusting the watermarked image brightness as shown in Fig. 9.

Further, the proposed algorithm is secure. The watermark image embedded in the host image is a permuted (scrambled) watermark with a secret key K. The unauthorized users, without the secret key K cannot extract the watermark even with the help of the watermark embedding algorithm and hence it is secure.

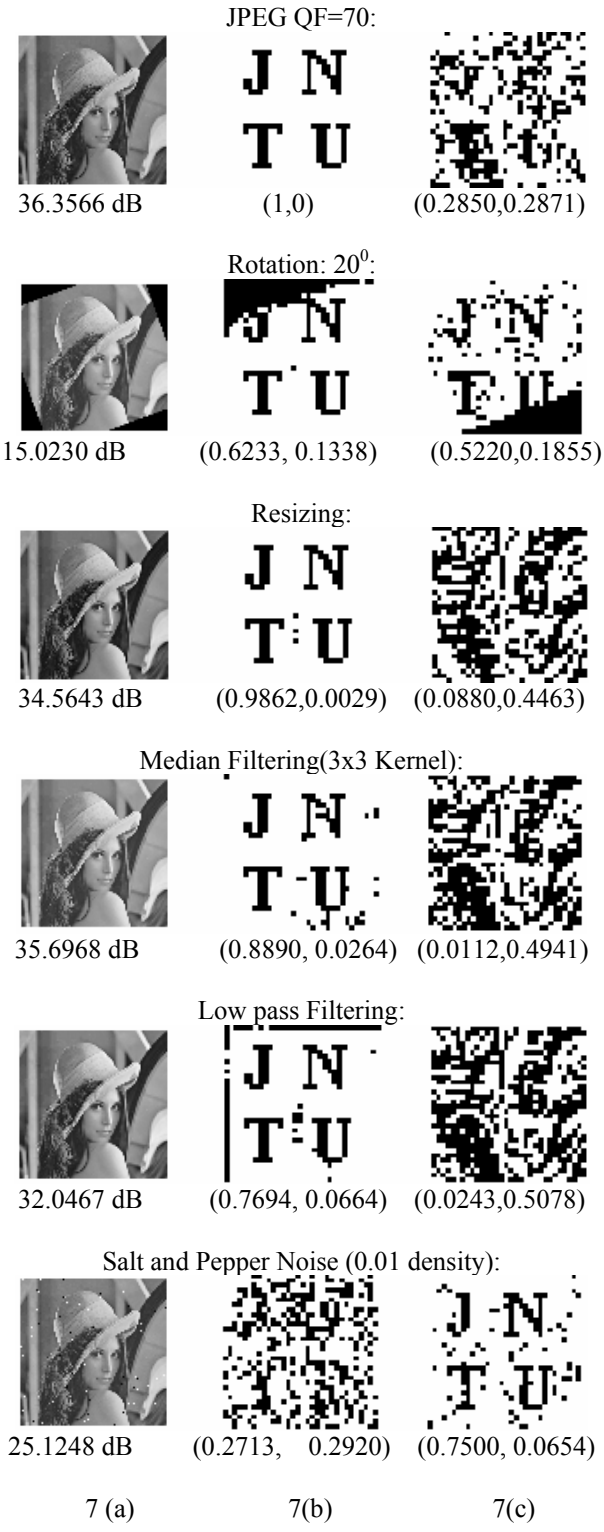
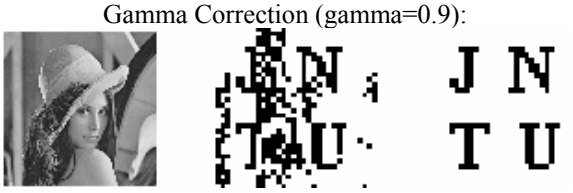


Figure 7(a).Attacked watermarked image with PSNR
(b).Extracted watermarks from D matrix
(c).Extracted watermarks from U matrix

Cropping (25%):

11.5995 dB (-, 0.8818) (1,0)

Gamma Correction (gamma=0.9):

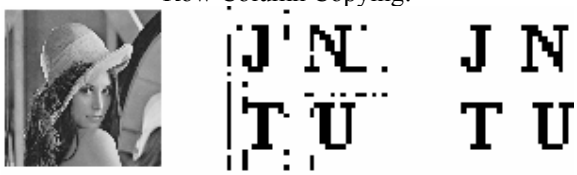


30.1799 dB (0.4328, 0.2197) (1,0)

Row Column Blanking:

21.3068 dB (0.5633, 0.1426) (1,0)

Row Column Copying:



32.3336 dB (0.7822, 0.0586) (1,0)

Bit Plane Removal (LSB):

40.1154 dB (1,0) (0.9814,0.0039)

JPEG 2000 QF=70:

41.4539 dB (1,0) (0.9817,0.0039)

8 (a) 8 (b) 8(c)

Figure 8(a). Attacked watermarked image
(b).Extracted watermarks from D matrix
(c).Extracted watermarks from U matrix

Brightness Adjustment (20%):

10.7003 dB (0.4794, 0.2461) (0.6013, 0.1426)

9(a) 9(b) 9(c)

Figure 9(a).Attacked watermarked image
(b).Extracted watermarks from D matrix
(c).Extracted watermarks from U matrix

VI. CONCLUSIONS

In this paper, a robust watermarking scheme based on SVD is proposed. The watermark image is embedded in both *D* and *U* matrices. Since, the same watermark is embedded twice in the same image, the rate of watermark survival is high. Robustness is achieved by using the Dither quantization for *D* matrix and altering coefficients of *U* matrix. The quality of the watermarked image is good in terms of perceptibility and PSNR (43.11dB). This method is superior to Chung et al. method in terms of both PSNR and robustness (low BER & high NC). The proposed algorithm is shown to be robust to JPEG2000 compression, JPEG compression, rotation, scaling, cropping, median filtering, low pass filtering, row-column copying, row-column blanking, bit plane removal, salt and pepper noise and gamma correction. This indicates that an embedded watermark is still recoverable even after the common image processing operations on the watermarked image and hence highly suitable for the copyright protection.

REFERENCES

[1] I.J.Cox, J.Kilian, T.Leighton and T.Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Transactions on Image Processing,* 6(12), 1673-1687, December, 1997.

[2] C.I.Podilchuk and E.J.Delp, "Digital Watermarking: Algorithms and Applications", *IEEE Signal Processing Magazine,* pp.33-46, July 2001.

[3] I.J.Cox, M.L.Miller, and J.A. Bloom, *Digital watermarking*, Morgan Kaufmann Publishers, San Francisco, CA, 2002.

[4] Tao Peining and Eskicioglu Ahmet M, "An Adaptive Method for Image Recovery in the DFT Domain", *Journal of Multimedia*, Vol.1, No.6, September 2006.

[5] Barni, F. Bartolini, A. Piva . "A DCT domain system for robust image watermarking", *IEEE Transactions on Signal Processing,* 66, 357-372, 1998.

[6] Chu, W.C, "DCT based image watermarking using sub sampling", *IEEE Trans Multimedia* 5, 34-38, 2003.

[7] M.Barni, M., Bartolini, F., V., Piva, A, "Improved wavelet based watermarking through pixel-wise masking," *IEEE Trans Image Processing* 10, 783-791, 2001.

[8] Y. Wang, J.F.Doherty and R.E.Van Dyck, "A wavelet based watermarking algorithm for ownership verification of digital images", *IEEE Transactions on Image Processing,* 11, No.2, pp.77-88, February 2002.

[9] V. I. Gorodetski, L. J. Popyack, V. Samoilov and V. A. Skormin, "SVD-based Approach to Transparent Embedding Data into Digital Images", *International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS 2001),* St. Petersburg, Russia, May 21-23, 2001.

[10] R.Liu, T.Tan, "An SVD-based watermarking scheme for protecting rightful ownership", *IEEE Trans. Multimedia,* (4),1, pp, 121-128, 2002.

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

[12] Sun, R., Sun, H., Yao, T, "A SVD and quantization based semi-fragile watermarking technique for image authentication" *Proc. IEEE International Conf. Signal Processing,* 2. 1592-95, 2002.

[13] Chin-Chen Chang, Piyu Tsai, Chia-Chen Lin, "SVD based digital image watermarking scheme". *Pattern Recognition Letters* 26, 1577-1586, 2005.

[14] S.Srinivas Kumar, B.Chandra Mohan and B.N.Chatterji, "An Oblivious Image Watermarking Scheme using Singular Value Decomposition," *IASTED International Conference on Signal and Image Processing (ICSIP'07),* Honolulu, Hawaii, USA, August 20-22, 2007.

[15] Chung K,Yang W ,Huang Y, Wu S, Hsu Yu-Chiao, "On SVD-based watermarking algorithm" *Applied Mathematics and Computation* Elsevier, 188, 54-57, 2007.

[16] E.Ganic and A.M.Eskiciougulu, "Secure DWT-SVD Domain Image Wtermarking: Embedding Data in All Frequencies", *ACM Multimedia and Security Workshop* 2004, Magdeburg, Germany, September 20-21, 2004.

[17] Jieh-Ming Shieh, Der-Chyuan Lou and Ming-Chang Chang, "A semi-blind digital watermarking scheme based on singular value decomposition", Computer Standards and Interfaces 28, 428-440, 2006.

[18] Ganic E, Zubair N, Eskicioglu AM. "An optimum watermarking scheme based on singular value decomposition", *International Conference on Communication Network and Information Security,* Uniondale, Ny, p.85-90, 2003.

[19] ZI-Quan Hong, "Algebraic Feature Extraction of image for recognition" *Pattern Recognition*, Vol.24, No.l3, pp.211-219, 1991.

[20] Brian Chen and G.W.Wornell, "Digital Watermarking and information embedding using dither modulation", *Proceedings of the IEEE workshop on Multimedia Signal Processing (MMSP-98)*, Redondo Beach, CA, December 1998.

[21] Brian Chen and G.W.Wornell, "Preprocessed and postprocessed quantization index modulation methods for digital watermarking", *Proceedings of SPIE: Security and Watermarking of Multimedia Contents* II, Vol.3971,1999.

[22] http://www.morgan-multimedia.com

Chandra Mohan B was born in Chirala, India . He received the bachelor degree in electronics & communication engineering from Bapatla Engineering College, Bapatla, in 1990, the master degree in microwave engineering from Cochin University of Science and Technology in 1992. He is currently a PhD student in electronics and communication engineering at the ECE department, JNTU College of Engineering, Kakinada, India.

His research interests include digital image processing, communication engineering.

Srinivas Kumar S received the bachelor degree in electronics & communication engineering from Nagarjuna University, Guntur, in 1985, the master degree in electronics & instrumentation from JNTU College of Engineering, Kakinada, India in 1987. He obtained his PhD degree from Indian Institute of Technology, Kharagpur in 2003. Presently, he is professor in the department of ECE.

Prof.Kumar's teaching and research interests include digital image processing, artificial neural networks and fuzzy set theoretic techniques.

.