A Robust Hybrid Digital Image Watermarking using SVD and DWT technique

Ms. Nitika Agarwal[1] Ms. Neha Singh[2]
[1]Scholar, M.Tech, Institute of Engineering and Technology, Alwar
[2]Associate Prof., Dept. of ECE, Institute of Engineering and Technology, Alwar
nitika.agarwal9@gmail.com, nneha.singh01@gmail.com

Abstract: - This paper presents the hybrid digital image watermarking technique. Taking the advantages of discrete wavelet Transform (DWT), the host image is decomposed into its significant components. The D component of Singular value decomposition (SVD) of approximate sub image of host image is taken. Watermark image is embedded in D component using Dither Quantization. The proposed algorithm uses advantages of SVD and DWT technique. The algorithm is more secure and robust to various attacks, viz., Gaussian noise, salt & pepper noise, speckle noise, Poisson noise, JPEG compression, median filtering, scaling and rotation. Superior experiment results are obtained from proposed algorithm in terms of Bit Error Rate (BER) and Peak signal to noise ratio (PSNR).

Keywords: - Steganography, Digital Watermarking, Hybrid watermarking, transform domain watermarking, Wavelet domain watermarking, Dither Quantization, Singular Value Decomposition.

1. INTRODUCTION

The techniques involved in hiding some information in digital content are collectively referred to as *information hiding techniques*. When used on digital images, these can be classified [1] as steganography or watermarking techniques. *Steganography* refers to the science of invisible communication striving to hide the very presence of the message itself. Digital watermarking is the process of embedding information into digital multimedia content such that the information can later be extracted or detected for a variety of purposes [2] including copy prevention and control. A digital watermark [3] is used for this purpose which is a digital signal or pattern inserted into a digital image and may also serve as a digital signature. It helps to determine the authenticity and ownership of an image.

It is desirable that the watermark is irremovable from the cover image and resists several intentional and unintentional operations with the watermarked image which may possibly disable the watermark. Commonly, these operations (especially the intentional ones) are referred as attacks against watermarks and include [4, 5] geometric distortions like rotation, translation, scaling and cropping, resampling and requantization, recompression, filtering, rewatermarking, forgery and collusion. For protection against these attacks, the watermarking technique need to trade off between [2, 4] the security, imperceptibility, capacity, robustness, tamper resistance, computational cost, data payload and key restrictions.
The terms Steganography and watermarking are exchangeable. The important areas of application [2, 5, 6] for watermarking are owner identification, copyright protection, broadcast monitoring, medical applications, fingerprinting and data authentication.

The paper is organized as follows: Section 2 gives the techniques used in proposed algorithm followed by proposed algorithm in section 3. Section 4 discusses results of proposed technique and section 5 is conclusion.

2. HYBRID DIGITAL WATERMARKING TECHNIQUE

Multiple techniques in the transform domains are simultaneously used to watermark the digital images. This forms a new class of watermarking: Hybrid watermarking. Many algorithms have been published and many are in process. This class attracts most researchers as it enables them to exploit the advantages of each of the transform used to suppress the limitations and disadvantages of the other transforms. [7] Maps zigzag sequence of DCT coefficients of the cover image in to 4 quadrants followed by taking SVD for each block. The same process is done on the watermark. Thus, four watermarks are embedded one in each block. The coefficients of each block are modified with those of the watermark. The inverse transforms in the reverse sequence, produces watermarked image.

The proposed algorithm is hybrid digital image watermarking technique which uses combination of two transform domain techniques viz. Singular value decomposition (SVD) and Discrete wavelet transform (DWT). First we will discuss these two techniques separately and considering the advantages of these techniques we formulate hybrid proposed algorithm.

SINGULAR VALUE DECOMPOSITION (SVD)

SVD decomposes matrix into three matrices of same size. Let A be M X N matrix with M ≥ N, Then, A= UDVT where the diagonal elements of D are the singular values (SVs) [8, 9] which specify the luminance of an image layer while the corresponding pair of singular vectors in U and V specify the geometry of the image. The main properties of SVD from the viewpoint of image processing applications are: 1) the SVs of an image have very good stability, i.e., when a small perturbation is added to an image, its SVs do not change significantly; and 2) SVs represent intrinsic algebraic image properties.

The simplest approach is where the watermark image is embedded directly in the SVD domain. A single image is used as watermark which is embedded in the whole image. This method is blind but requires the singular values or the orthogonal matrices for retrieving the watermark.

Liu and Tan [10] used a non-blind image watermarking method which adds the scaled watermark to the matrix D and takes the SVD of this modified D, (D+aW) matrix to get UW, DW and VW. Watermarked image, AW is obtained by multiplying U, DW and V'. The watermark is detected using UW, D and VW as the keys. The possibly attacked image AW* is decomposed using SVD to U, DW and V. The obtained D* W matrix is used with the keys UW and VW, to obtain the approximate S which is used to find the approximate watermark W = (D*W – S)/a. However the keys used already include the information of original watermark unintentionally. So the modified approach was proposed by [2] which avoided using SVD on the modified D but directly used it to produce watermarked image with original U and V. The recovery procedure remains the same with original U, V and D as the keys.

The matrix U along with matrix D is exploited by [8] using block based SVD to embed the watermark. The coefficients of D matrix are modified based on the Dither quantization [8, 9, 11], in such a way that the watermarked image quality is not degraded. The watermark bits are embedded in the columns of U matrix based on the difference in the values of these columns. [8, 11] used these approaches to embed two watermarks in the same image at two different locations. Any modification of D component degrades the perceptibility of the watermarked image, so, [9] improved perceptibility by embedding the watermark in some selected complex blocks based on the number of edges in a block. A block is qualified as a complex block, if the number edges in it are greater than a threshold value.

DISCRETE WAVELET TRANSFORM (DWT)

Discrete Wavelet Transform (DWT) allows images to be viewed and processed at multiple resolutions and provides a powerful insight into an image's spatial and frequency characteristics. The term DWT refers to a class of transformations that differ not only in the transformation kernels employed, but also the fundamental nature of those functions and in the way in which they are applied. Since the DWT encompasses a variety of unique but related transformations so each DWT is characterized by a transform kernel pair or set of parameters that defines the pair. The basic functions of DWT are based on small waves, called wavelets, of varying frequency and limited duration. To obtain DWT, filtering splits the signal into low-pass and high-pass components and down-samples each. On each successive step the lowest frequency signal component is split in to a low-pass and high-pass component, gaining better frequency resolution at the expense of temporal resolution. Level of DWT refers to the passes of DWT.

Each pass of DWT produces four frequency bands. The simplest approach is to embed watermark in the DWT coefficients. [4, 12] embeds PN sequences to the coefficients of medium and high frequency bands based on watermark bits. Correlation is then used to recover the watermark. [13] embeds the watermark bits in the sub-band of middle frequency after 3 level decomposition which has minimum energy by modifying the coefficients according to some predefined rule. [14] used the horizontal band for embedding because embedding in the approximation sub-band produces perceptible artifacts in the watermarked image. [15] embeds the watermarking data on selected groups of wavelet coefficients of the input image. Two groups of coefficients are formed after detecting the edges using a Sobel edge detector and a threshold value. Another group is formulated by a morphological dilation operation applied on the edge coefficients. The selected coefficients reside on the detail sub bands and describe the edges of the image or the region around them. The watermark strength is tuned according to the subband level and the group that each coefficient resides in. Thus, exploiting the HVS, which is less sensitive to alterations on high frequencies, the embedded information becomes invisible. The evaluation of the proposed method shows very good performance as far as invisibility and robustness is concerned. The proposed scheme behaves very well in various common signal processing operations as compression, filtering, noise, scaling and cropping.

DWT is best suited to resist compression effects [16] on watermarking because JPEG2000 is the mostly used compression standard which itself is based on DWT. [16] preprocesses the cover image according to the JPEG2000 standard before embedding to develop a robust technique to compression.

2-level decomposition is used by [17] to preprocess the original image and compare the horizontal coefficients of the two levels by calculating local relationship of wavelet coefficient. The embedded region which is calculated with a threshold in the LH2 sub-band is decided by the priority order of interrelation. The algorithm is shown to be relatively robust in regard of such attacks as JPEG, Sharpening and Blurring.

Watermarking is done in the high frequency coefficients too. [19] decomposes an input image into non-overlapping blocks and embeds a watermark into the high frequency wavelet coefficients of each block. Arbitrary wavelet and block size are derived to avoid the underflow and overflow conditions. Embedded payload contains message and information for reconstructing exact original image.

Multiple watermarks can also be embedded to increase the robustness of the technique against cropping, scaling and compression. [8,18] exploited this second dimension of watermarking, by embedding two watermarks simultaneously in one cover image using DWT and [8] used this approach with SVD.

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 tradeoff 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 spectrum 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 quantizer 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.

3. PROPOSED METHOD

In the proposed method, the DWT and D matrix SVD technique are explored for embedding the watermark. The host image is divided into four sub images using DWT. The D components of the approximate sub image are extracted for embedding 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 vertical sub image is obtained. On taking the inverse DWT the watermarked image is obtained. The watermark embedding algorithm is presented in the following steps:

A. Host Image Partition using DWT technique:

The host image of size N X N is partitioned into four sub images using DWT. The watermark is embedded in the sub images and only to improve imperceptibility of the watermark in the watermarked image and hence better PSNR.

B. Watermark Embedding in D Matrix:

1. Block based SVD Transformation is applied on approximate component of DWT host image.
2. From each block of *D* matrix, obtain the largest coefficient *D (1, 1)*. From these *D (1, 1)*'s, a matrix *Dlarge* is formed. The size of *Dlarge* is, same as that of watermark image.
3. The entire range *dmin* (minimum value of *Dlarge*) to dmax (maximum value of *Dlarge*) 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.
4. Each element of *Dlarge* matrix is checked for its position in Table I.

After identifying the bin number, *Dlarge* is modified as follows:

(i) If watermark bit is '1' then it belongs to *Range1*, where *Range1* is defined as

$$Range1 = dlow\,(n) \quad \text{to} \quad (dlow\,(n) + dhigh\,(n))/2$$

Dlarge is modified as

$$Dlarge = [dlow\,(n) + (dlow\,(n) + dhigh\,(n))\,/\,2)]/2$$

Bin no.	***Dlow***	***Dhigh***
1	*dmin – T*	*Dmin*
2	*Dmin*	*dmin+T*
3	*dmin+T*	*dmin+2T*
bn-1	*dmax – T*	*Dmax*
.	..	..
.	..	..
Bn	*Dmax*	*dmax + T*

TABLE I. QUANTIZATION TABLE FOR THE LARGEST SINGULAR VALUES

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

$$Range2 = [dlow\ (n) + dhigh\ (n)]/2 \text{ to } dhigh\ (n)$$

Dlarge is modified as

$$Dlarge = [dhigh\ (n) + (dlow\ (n) + dhigh\ (n))\ /\ 2)]/2$$

5. After the modification applied in step 4, inverse SVD is applied to get the first portion of the watermarked image.

6. To obtain watermarked image inverse DWT is applied to the image in step 5.

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. Watermarked Image Partition:

The watermarked image of size $N \times N$ is partitioned into four sub images using DWT.

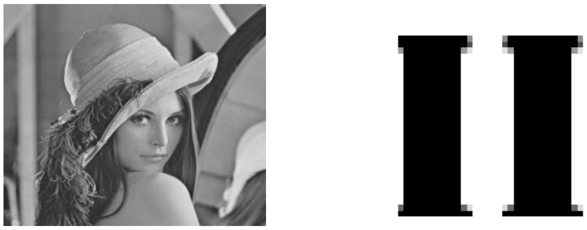
D. Watermark Extraction from D Matrix

1. SVD transformation is applied on vertical component of DWT sub image.
2. From each block of *D* matrix obtained from SVD, the largest coefficient *D (1,1)* is extracted.
3. The value of *D (1,1)*is checked for its positioning the quantization table (Table I). From this step, bin position is identified.
4. From the bin position obtained in step 3, 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 4 are repeated for all the largest coefficients of all the blocks of D component. In this way, the watermark image is extracted.

4. EXPERIMENTAL RESULTS

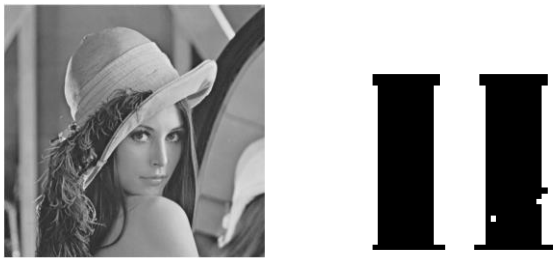
The cover images used as cover object is a 512 X 512, 8-bit, .bmp image with 256 gray levels are Lena.bmp as shown in figure1(a). The choice of watermark image for algorithm depends upon the capacity of the data the technique can hide in a given sized cover object. The large images can be cropped according to the need of the algorithm. The image used as watermark is shown in figure1 (b).



(a) (b)

Figure 1 :(a) Lena image (b) Watermark

Figure 2(a) shows the Lena watermarked image from which the retrieved watermark is shown in figure 2(b).The PSNR of the watermarked image is 3.5749e+003 and the BCR of the retrieved watermark is 99.0234. This technique is more robust as the retrieved watermark is 99% similar to the original watermark. The PSNR value obtained fulfills the criteria of robustness of the algorithm.



(a) BCR= 99.0234 (b)

Figure 2: (a) cover image watermarked using DWT and D matrix of the SVD of the cover image. (b) Retrieved watermark.

The graph in figure 3 shows the higher PSNR can be obtained with increase in the number of bins but this is at the expense of BCR of the retrieved watermark, since BCR falls at larger number of bins. Though the variation in BCR with number if bins is complex, however if the number of bins is reduced to as low as 12, the watermark becomes visible.

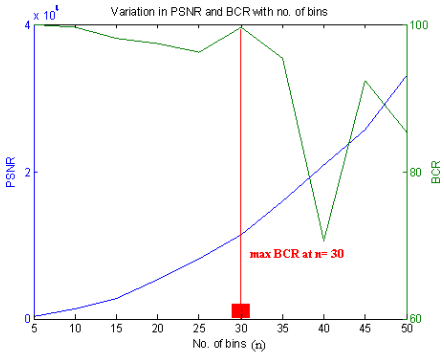
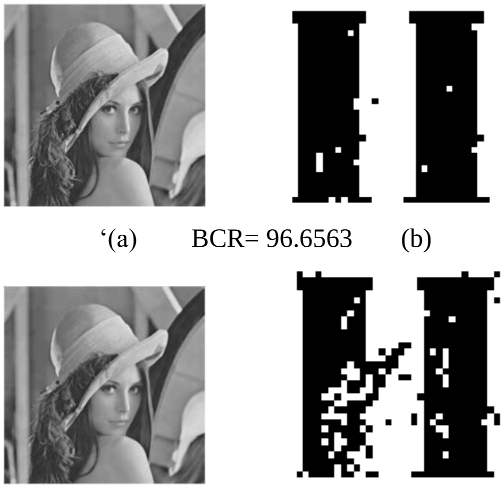


Figure 3: Variation of PSNR and BCR with change number of bins.

The attacks used to test the robustness of the watermark are JPEG2000, JPEG compression, rotation, resizing, median filtering, cropping, salt and pepper noise ,Gaussian noise, speckle noise, Poisson noise. The extracted watermarks after applying various attacks are shown in Figs. 4 to 11. The BCR values of the retrieved watermark are indicated at the bottom of the figure.

Median Filtering

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.



‘(a) BCR= 96.6563 (b)

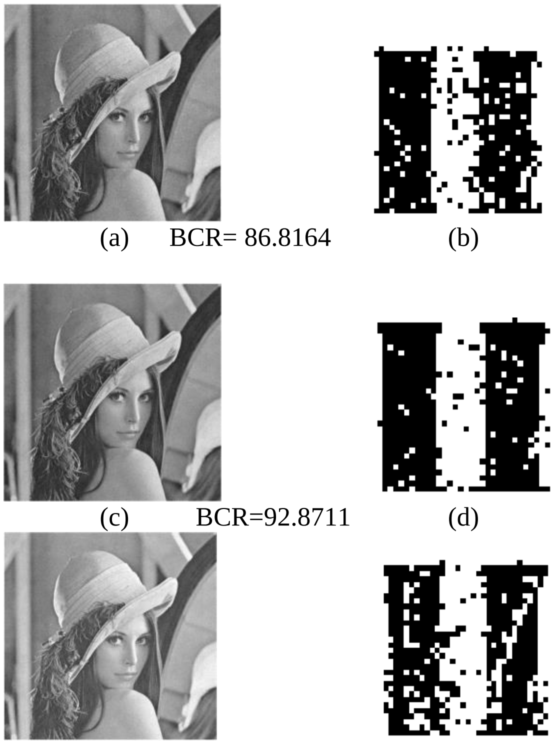
(c) BCR=88.7695 (d)

Figure 4: (a) Watermarked image attacked by median filter (3X3) (b) Recovered watermark from watermarked image attacked by median filter (3X3). (c) Watermarked image attacked by median filter (5X5). (d) Recovered watermark from image attacked by filter (5 X 5).

Noise

Watermarked image is attacked by various noises Gaussian noise with variable mean and variance values, salt & pepper noise, speckle noise and poisson noise. The BCR values obtained from the retrieved watermarks are quite good. We can say that proposed algorithm is resistant to noise. The figure below shows the watermarked image attacked by noise and recovered watermark with their respective BCR values.

Gaussian Noise



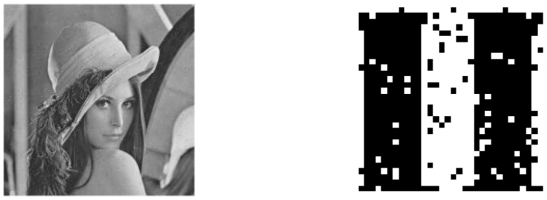
(a) BCR= 86.8164 (b)

(c) BCR=92.8711 (d)

(e) BCR=82.5195 (f)

Figure 5: (a) Watermarked image attacked by Gaussian noise (mean =0 variance=0.002). (b) Recovered watermark from watermarked image attacked by Gaussian noise (mean =0 variance=0.002). (c) Watermarked image attacked by Gaussian noise (mean =0 variance=0.001). (d) Recovered watermark from watermarked image attacked by Gaussian noise (mean =0 variance=0.001). (e) Watermarked image attacked by Gaussian noise (mean =0.1 variance=0.001). (f) Recovered watermark from watermarked image attacked by Gaussian noise (mean =0.1 variance=0.001).

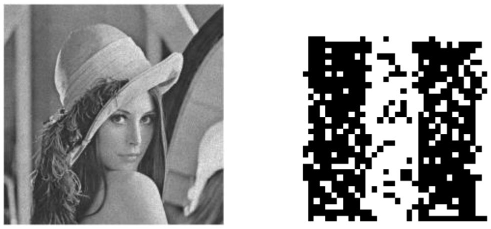
Salt & Pepper Noise



(a) BCR=91.6016 (b)

Figure 6: (a) Watermarked image attacked by salt & pepper noise. (b) Recovered watermark from image attacked by salt & pepper noise.

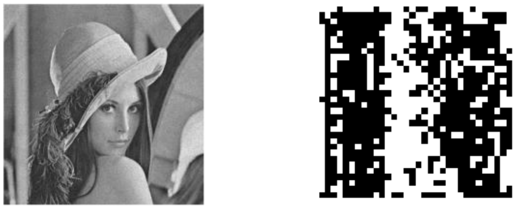
Speckle Noise



(a) BCR=81.0547 (b)

Figure 7: (a) Watermarked image attacked by salt & pepper noise. (b) Recovered watermark from watermarked image attacked by salt & pepper noise.

Poisson Noise

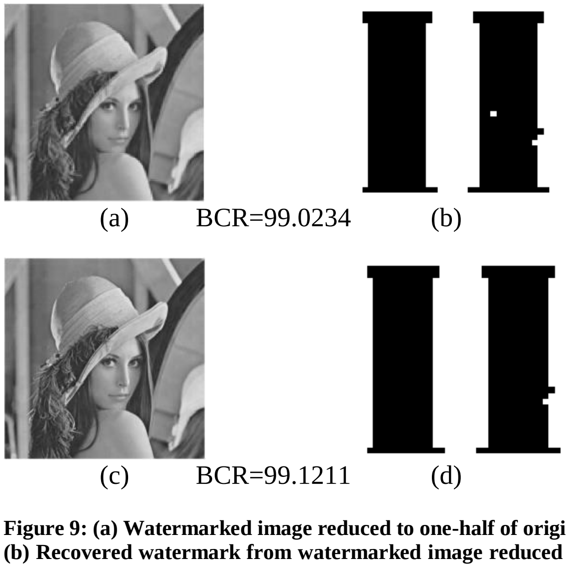


(a) BCR=75.8759 (b)

Figure 8: (a) Watermarked image attacked by Poisson noise. (b) Recovered watermark from watermarked image attacked by Poisson noise.

Resizing

In this experiment, initially the watermarked image size is reduced to one half of original size. The watermarked image is increased to double its size in next case. Both result in watermark with very good BCR values. Hence the proposed algorithm robust against resizing attacks.



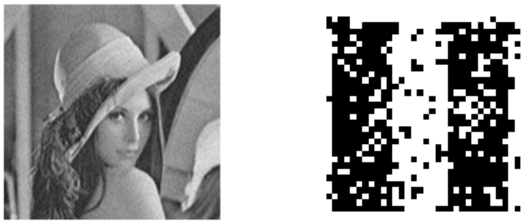
(a) BCR=99.0234 (b)

(c) BCR=99.1211 (d)

Figure 9: (a) Watermarked image reduced to one-half of original size (b) Recovered watermark from watermarked image reduced to one-half of the original size. (c) Watermarked image increased to two times of original size. (d) Recovered watermark from Watermarked image increased to two times of original size.

Compression

The watermarked image is compressed using lossy JPEG compression. 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.

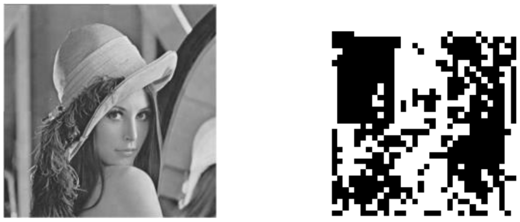


(a) BCR=82.7148 (b)

Figure 10: (a) JPEG compressed Watermarked image (compr coeff= 5000). (b) Recovered watermark from JPEG compressed image with (compr coeff= 5000).

Rotation

The watermarked image is rotated by 0.1 degree 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 loses some watermark information.



(a) BCR=74.0234 (b)

Figure 11: (a) Watermarked image is rotated by 0.1 degree. (b) Recovered watermark from rotated watermarked image.

5. CONCLUSIONS

In this paper, a robust hybrid watermarking scheme based on SVD and DWT is proposed. The combination of the two transforms DWT and SVD improves the watermarking performance considerably when compared to DWT –Only or SVD – Only watermarking approach. The technique fully exploits the respective feature of these two transform domain methods efficiently. Robustness is achieved by using the Dither quantization for *D* matrix and DWT technique. The quality of the watermarked image is good in terms of perceptibility and PSNR value.

This method is superior in terms of both PSNR and robustness (low BER & high NC). The proposed algorithm is shown to be robust to JPEG2000 compression, noise, rotation, resizing and median filtering. 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. This scheme is robust against all sorts of attacks. It has very high data hiding capacity.

REFERENCES

1. Motameni H., Norouzi M., Jahandar M., Hatami A., "Labeling Method in Steganography". *Proceedings of World Academy of Science, Engineering and Technology*, Volume 24, October 2007, ISSN 1307-6884.

2. Pei S., Liu H., "Improved SVD based Watermarking for Digital Images", *Sixth Indian Conference on Computer Vision, Graphics and Image Processing, IEEE Computer Society*, 2008.

3. Singh Neha, Nandi Arnab," Digital Watermarking: Mark this Technology!".

4. Vallabha V.H.,"Multiresolution Watermark Based on Wavelet Transform of Digital Images", Multiresolution watermarking of Digital Images, Cranes Software International Limited.

5. Miller Matt L., Cox Ingemar J., Linnartz Jean-Paul M. G., Kalker Ton, "A Review of Watermarking Principles and Practices". *Chapter 18, Digital Signal Processing in Multimedia Systems,* Ed. K. K. Parhi and T. Nishitani, Marcell Dekker Inc., 461-485, (1999).

6. Potdar Vidyasagar M., Han Song, Chang Elizabeth, " A Survey of Digital Image Watermarking Techniques". *3rd IEEE International Conference on Industrial Informatics* , 2005.

7. Sverdlov Alexander, Dexter Scott, Eskicioglu Ahmet M., " Secure DCT-SVD Domain Image Watermarking: Embeddig Data in All Frequencies", Unknown.

8. Mohan B. Chandra, Kumar S. Srinivas, "A Robust Image Watermarking Scheme Using Singular Value Decomposition". *Journal of Multimedia*, Volume 3, No. 1, May 2008.

9. Mohan B. Chandra, Kumar S. Srinivas, Chhatterji B. N., "A Robust Digital Image Watermarking Scheme Using Singular Value Decomposition (SVD), Dither Quantization and Edge Detection". *ICGST-GVIP Journal*, ISSN:1687-398X, Volume 8, issue 1, June 2008.

10. Liu R., Tan Tieniu, "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership", *IEEE Transactions of Multimedia,* Vol. 4, No. 1, March 2002.

11. Singh N., Sharma M.M., "Singular Value Decomposition Technique for Digital Image Watermarking", National Conference on Advances in Wireless and Optical Communication Technique, 2010.

12. Maity Santi P., Kundu Malay K., " A Blind CDMA Watermarking Scheme in Wavelet Domain", *0-7803-8554-3, IEEE, 2004*, 2633- 2636.

13. Tay P., Havlicek J.P., " Image Watermarking Using Wavelets", IEEE, 2002.

14. Hajjara Suhad, Abdallah Moussa, Hudaib Amjad," Digital Image Watermarking Using Localized Biorthogonal Wavelets", *European Jounal of Scientific Research*, Vol.26 No. 4, 2009, 594-608.

15. Ellinas John N., "A Robust Wavelet-Based Watermarking Algorithm Using Edge Detection", *PWASET Volume 25 November 2007*, 438-443.

16. Dazhi Zhang, Boying Wu., Jiebao Sun, "A Robust Image Watermarking Algorithm Against JPEG2000", *IEEE Proceedings of International Conference on Communications and Mobile Computing,* 2009,430-434.

17. Park Ki Hong, Kim Yoon Ho, Lee Joo Shin, "Watermarking using the local relation of wavelet coefficient", IEEE *Proceedings of Second International Conference on Future Generation Communication and Networking*, 2008. 209-212.

18. Sharkas Maha, ElShafie Dahlia, and Hamdy Nadder, "A Dual Digital-Image Watermarking Technique", Proceedings of World Academy of Science, Engineering and Technology, Volume 5, April 2005, 136-139.

19. Lee Sunil and Yoo Chang D. and Kalker Ton, *Fellow, IEEE "*Reversible Image Watermarking Based on Integer-to-Integer Wavelet Transform"

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).*

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.