

# Improved BEMD-DWT-DCT-SVD Robust Watermarking Technique for Still Images

A. M. El-Assy

Egypt- Mansoura University-  
Electronics and  
Communications Engineering  
Mansoura-Egypt

M. A. Mohamed

Egypt- Mansoura University-  
Electronics and  
Communications Engineering  
Mansoura-Egypt

M. E. A. Abou-El-Seoud

Egypt- Mansoura University-  
Electronics and  
Communications Engineering  
Cairo- Egypt

## ABSTRACT

As a result of the growth of the technology the Protection of digital multimedia content has become a difficult, However; the imperceptible and robust image watermarking algorithm have been presented to defend the copyright protection. In this paper we presented a proposed method based on Bidimensional Empirical Mode Decomposition (BEMD); discrete wavelet transform (DWT); discrete cosine transform (DCT), and singular value decomposition (SVD). The results obtained from the experimentation showed that the algorithm has excellent robustness against different attacks, e.g. jpeg compression, additive Gaussian noise, cropping, rotation, and Gamma correction. The resulting PSNR achieved up to 60.1629 dB in case of free attacks. In addition, the results of proposed algorithm have been compared with many new related algorithms, published in trusted journals to prove that proposed technique is the best.

## Keywords

Bidimensional Empirical Mode Decomposition (BEMD) discrete wavelet transform (DWT), discrete cosine transform (DCT) and singular value decomposition (SVD).

## 1. INTRODUCTION

In recent years the usage of internet has increased tremendously, the growth of the technology has simplified sharing of the digital images, videos or any other legal document. So, illegal reproduction of data has also emerged with this extraordinary revolution and is raising questions and concerns about ownership rights. The problem of unauthorized access can be solved by adding digital watermarking to the image. Watermarking (data hiding) [1, 2] is the process of embedding data into a multimedia element such as image, audio or video. Watermarking may be visible or invisible, blind or non-blind, fragile, robust or semi-fragile etc. The watermark may be any text, image or logo of the distributor which acts as the ownership information of the valid or authorized distributor in order to guarantee the ownership and the integrity. The basic requirements for a secure watermarking scheme are imperceptibility, robustness, capacity and security.

Digital image watermarking are mainly grouped into two classes: transform domains [3, 4], and spatial domains [1, 5]. The following works were carried out by specific persons in the area of digital watermarking search: Eskicioglu [6] proposed watermarking algorithms based on DWT and SVD, the Authors decomposing the host image using DWT into four bands, then apply the SVD to each band, and embed the same watermark data by modifying the singular values. Modification in all frequencies allows the development of a watermarking this scheme is not robust to all types of attacks. Sverdllov et al [7] presented a new hybrid watermarking

scheme based on DCT and SVD. ,the Authors applying the DCT to the host image, then map the DCT coefficients in a zigzag order into four quadrants, and apply the SVD to each quadrant. These four quadrants represent frequency bands from the lowest to the highest. The singular values in each quadrant are modified by the singular values of the DCT-transformed watermark. Khan et al [8], presented a hybrid digital image watermarking based on DWT, DCT, and SVD in a zigzag order. the Authors decomposing the host image using DWT into four bands, and select high frequency band(HH) to apply DCT, then map the DCT coefficients in a zigzag order into four quadrants, that represent low, mid and high bands. Finally, apply the SVD to each quadrant; this algorithm gives more invisibility and robustness against some attacks. Such as geometric attack. Hu, et al [3], presented image watermarking scheme based on DWT, DCT, and SVD is proposed. The DWT is applied to the host image to obtain a low-frequency (LL) sub band next; the DCT is applied to the LL sub band to obtain the frequency components. Finally, SVD is applied on the obtained frequency components to embed the watermark. This algorithm fails to resist two ambiguity attacks. In the first one, using the singular vectors of any fake watermark in the extracting process, the attacker can always claim that this watermark is the embedded one, hence, proves his ownership of the watermarked image. In the second attack, any watermarked image is publicly available which can be re-watermarked by an attacker's watermark. Later, this attacker one can claim that the embedded watermark is his one; Loukhaoukha, et al, had proven that this algorithm should not be used for proof of ownership, transaction tracking and data authentication [9].

By observing all the papers, a new robust digital watermarking technique have been proposed for gray scale image as cover and watermark using advantages of four algorithms BEMD, DWT, DCT, and SVD. In the proposed method, watermark is embedded into the singular values of the mid frequency band of the DCT block in high frequency band of DWT which selected from second IMF. The Proposed technique has also been analyzed and compared with DWT, DCT-SVD, DWT-SVD, DWT-DCT-SVD based techniques by applying various image attacks and subsequently measuring the results and proved to be better.

The paper is organized as follows: Section 2 describes the Transforms used for Watermarking. Section 3 explains the steps for the proposed algorithm. Section 4discusses the results which are compared with similar previous algorithms and Section 5 concludes the research work

## 2. TRANSFORMED WATERMARKING

## Decomposition (BEMD)

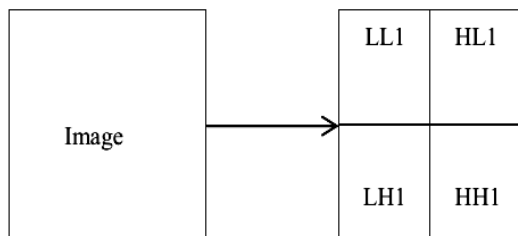
The iteration process and sifting process of BEMD is the same with EMD. The EMD method is a time-domain analysis method especially suited to nonlinear and non-stationary data. The core idea is to find the intrinsic multi-scale vibrations in the input signals. Based on the method of Huang [10], the author obtained a set of intrinsic mode functions as expressed by Eq.1

$$X(t) = \sum_{i=1}^n IMF_i + R_n \quad (1)$$

where  $X(t)$  is the input signal and  $R_n$  is the residue,  $X(t)$  is decomposed into  $n$  intrinsic mode functions (IMFs) and a residue. Image can be regarded as a 2D matrix signal  $f(x, y)$  [11].

## 2.2 Discrete Wavelet Transform (DWT)

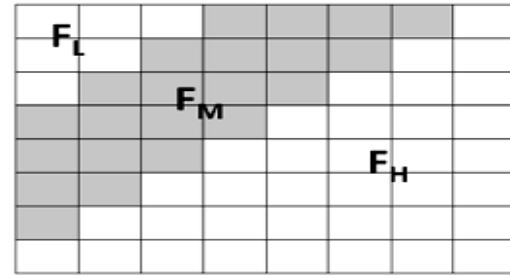
Wavelet transform decomposes an image into a set of four sub band which can be reassembled to reconstruct the original image without error. Dwt apply 2-D filters in each dimension. The input image have been divided by this filters into four non-overlapping multi-resolution sub bands, a lower resolution approximation image LL1, horizontal LH1, vertical LH1 and diagonal HH1 detail components as shown in Fig.1. Most signal information of original image is in the low frequency district. While the level detail, the upright detail and the diagonal detail of the original image is in LH, HL and HH frequency district respectively. According to the character of HVS, human eyes are sensitive to the change of smooth district of image, but not sensitive to the tiny change of edge, profile and streak. Therefore, to increase imperceptibility the author embeds the watermark in the higher level sub [12].



**Fig 1: Single level DWT**

## 2.3 Discrete Cosine Transform (DCT)

The DCT have been used to convert a signal into elementary frequency components. this transform DCT is a way to separate the spectral regions of the image according to their energy as shown in Fig.2. DCT-based watermarking is based on two facts. The first fact is the most important visual parts of the image lie into low-frequencies Sub-band which has much of the signal energy, the second fact is that high frequency components of the image are usually removed through compression and noise attacks [13].



**Fig 2: Definition of DCT Region**

## 2.4 Singular Value decomposition (SVD)

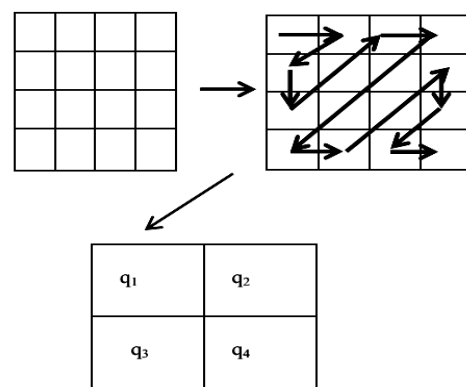
SVD is an effective numerical method used to decompose the matrix into three matrices that are of the same size as the original matrix. Then SVD of original matrix  $A$  is defined as  $A=USV^T$  where  $U$  and  $V$  are orthogonal matrices and  $S$  is Diagonal elements which called singular values, the author used these  $S$  values to embed and extract the image [14].

### 3. PROPOSED ALGORITHM

The proposed watermarking scheme is combined BEMD, DWT, DCT and SVD techniques to develop a new hybrid non-blind image watermarking scheme that is resistant to a variety of attacks. The proposed scheme is given by the following algorithm.

### 3.1 Watermark Embedding

- BEMD is applied to the host image to decompose it into the intrinsic mode functions (IMFs).
- Apply DWT on second IMF to decompose it into four sub-bands LL, LH, HL and HH.
- Apply DCT to HH band and get DCT coefficient matrix  $h$ .
- Map DCT coefficient matrix  $h$  into four quadrants  $q_1, q_2, q_3$  and  $q_4$  by using zigzag scanning.
- Apply SVD to each quadrant  $q_1, q_2, q_3$  and  $q_4$  to get  $S_1, S_2, S_3$  and  $S_4$  (as seen in Fig.3).



**Fig 3: zigzag scanning**

- f. EMD is applied to the watermark image to decompose it into the intrinsic mode functions (IMFs).
- g. Apply DWT on second IMF to decompose it into four sub-bands LL; LH; HL, and HH.

- h. Apply DCT to HH band and get DCT coefficient matrix w.
- i. Apply SVD matrix w to get Sw.
- j. Modify S<sub>1</sub>, S<sub>2</sub>, S<sub>3</sub> and S<sub>4</sub> by using equation
$$S_{ii} = S_i + con * Sw \quad (2)$$
- k. Mapping coefficients from zigzag scanning to original position matrix H\*.
- l. Apply inverse DCT to H\* to produce HH\*.
- m. Apply inverse DWT to LL, HL, LH and HH\* to get second (IMF\*).
- n. Apply inverse EMD to get watermarked image WI.

### 3.2 Watermark Extraction

- a. BEMD is applied to the watermarked image to decompose it in to the intrinsic mode functions (IMFs).
- b. Apply DWT on second IMF to decompose it into four sub-bands LL, LH, HL and HH.
- c. Apply DCT to HH band and get DCT coefficient matrix h.
- d. Map DCT coefficient matrix h into four quadrants q1, q2, q3 and q4 by using zigzag scanning.
- e. Modify S1, S2, S3 and S4 by using equation
$$Sw = \frac{S_{ii} - S_i}{con} \quad (3)$$
- f. Re-construct SVD matrix for each quadrant q1, q2, q3 and q4.
- g. Apply inverse DCT, inverse DWT and inverse EMD to each quadrant.

## 4. EXPERIMENTS AND RESULTS

The proposed algorithm has been implemented and executed using MATLAB 9 software on laptop which has Processor: Intel Core i5-3230M, RAM: 6GB, and OS: Windows 8.1.

### 4.1 Digital Images Dataset

The proposed watermarking algorithm is tested with the 512×512, grayscale, Windows Bitmap (BMP), 8 bit per pixel, Lena image as a host image and 256×256, grayscale, Joint Photographic Experts Group (JPEG), 8 bit per pixel, cameraman image as watermark image.

### 4.2 Performance Evaluation Metrics:

Watermarking algorithms are usually evaluated with respect to two metrics: imperceptibility and robustness.



Fig 4: Host image Lena.



Fig 5: watermark image

#### 4.2.1 Capacity Measures or imperceptibility

Imperceptions means that watermark should not be noticeable to the viewer and also should not produce any distortion in the host image [15]. An important way of evaluating watermarking algorithms is to compare the amount of distortion introduced into a host image by a watermarking algorithm. To evaluate it, the mean square error, peak signal to noise ratio, and watermark to document ratio have been used [16, 17].

##### i. Mean Square Error

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (X(i, j) - X'(i, j))^2 \quad (4)$$

##### ii. Peak Signal-to-Noise Ratio

PSNR in decibels (dB) is represented as shown:

$$PSNR = 20 \times \log_{10} \left( \frac{MAX}{\sqrt{MSE}} \right) \quad (5)$$

##### iii. Watermark-to-Document Ratio (WDR)

$$WDR = 10 \times \log_{10} \frac{\sum_{i=1}^M \sum_{j=1}^N (X(i, j) - X'(i, j))^2}{\sum_{i=1}^M \sum_{j=1}^N X^2(i, j)} \quad (6)$$

where (M, N) are the image dimensions;  $X(i, j)$  is the pixel value of the original image;  $X'(i, j)$  is the pixel value of the watermarked image, and MAX is the maximum pixel value of the image.

#### 4.2.2 Robustness Measures

Robustness means the ability of the watermark to withstand for different types attacks, such as geometric transformations, filtering and noise attacks etc. To evaluate it, the normalized correlation coefficient and the bit-correct ratio (BCR) have been used [16, 18].

##### i. Correlation Coefficients

$$NC = \frac{\sum_j \sum_i W_n(i, j) * \hat{W}_n(i, j)}{\sum_i \sum_j |W_n(i, j)|^2} \quad (7)$$

##### ii. The bit correct ratio (BCR)

$$BCR = \frac{100}{l} \sum_{n=0}^{l-1} \begin{cases} 1 & W_n' = W_n \\ 0 & W_n' \neq W_n \end{cases} \quad (8)$$

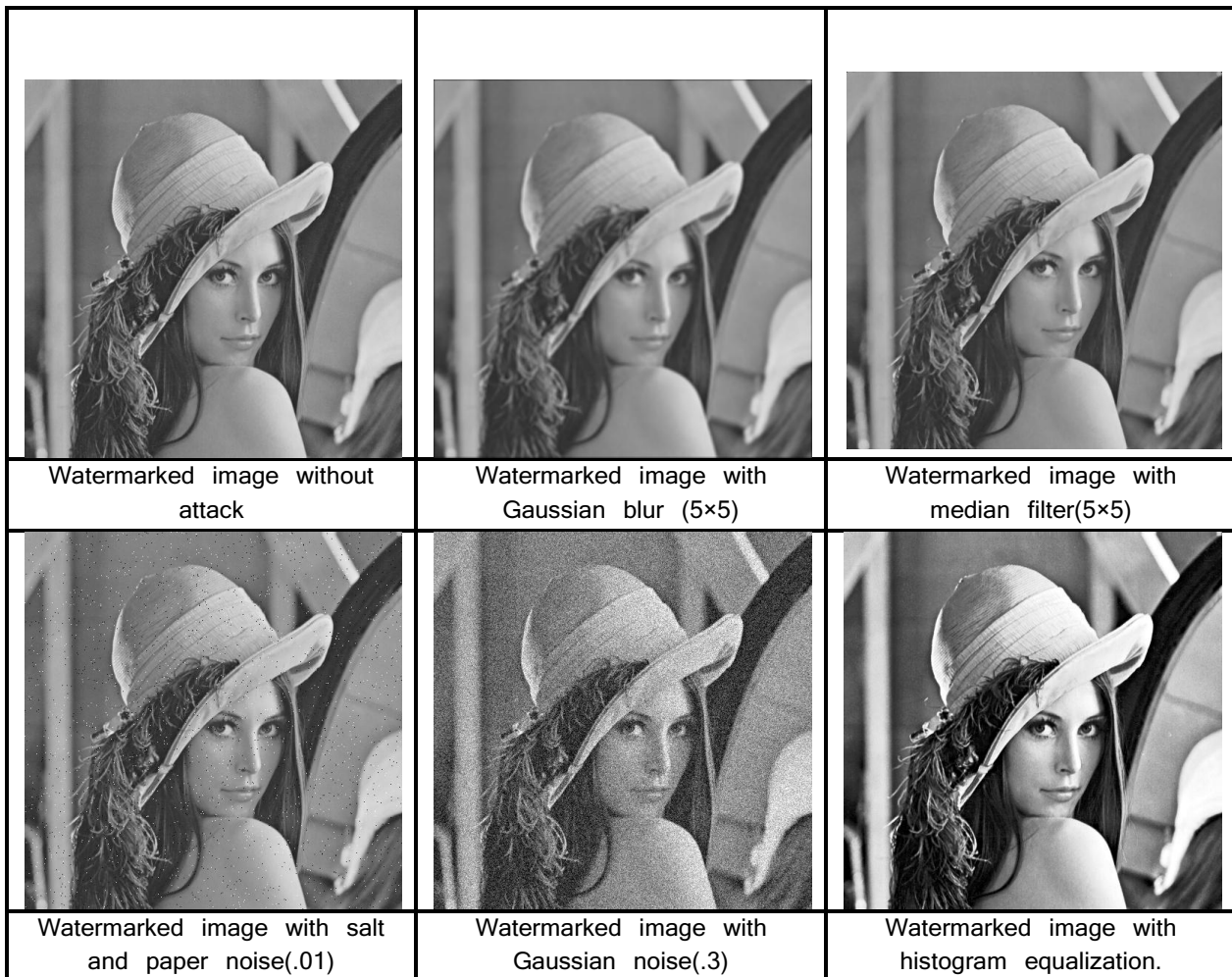
Where  $l$  is the watermark length;  $W_n$  Corresponds to the nth bit of the embedded watermark, and  $W_n'$  corresponds to the nth bit of the recovered watermark.

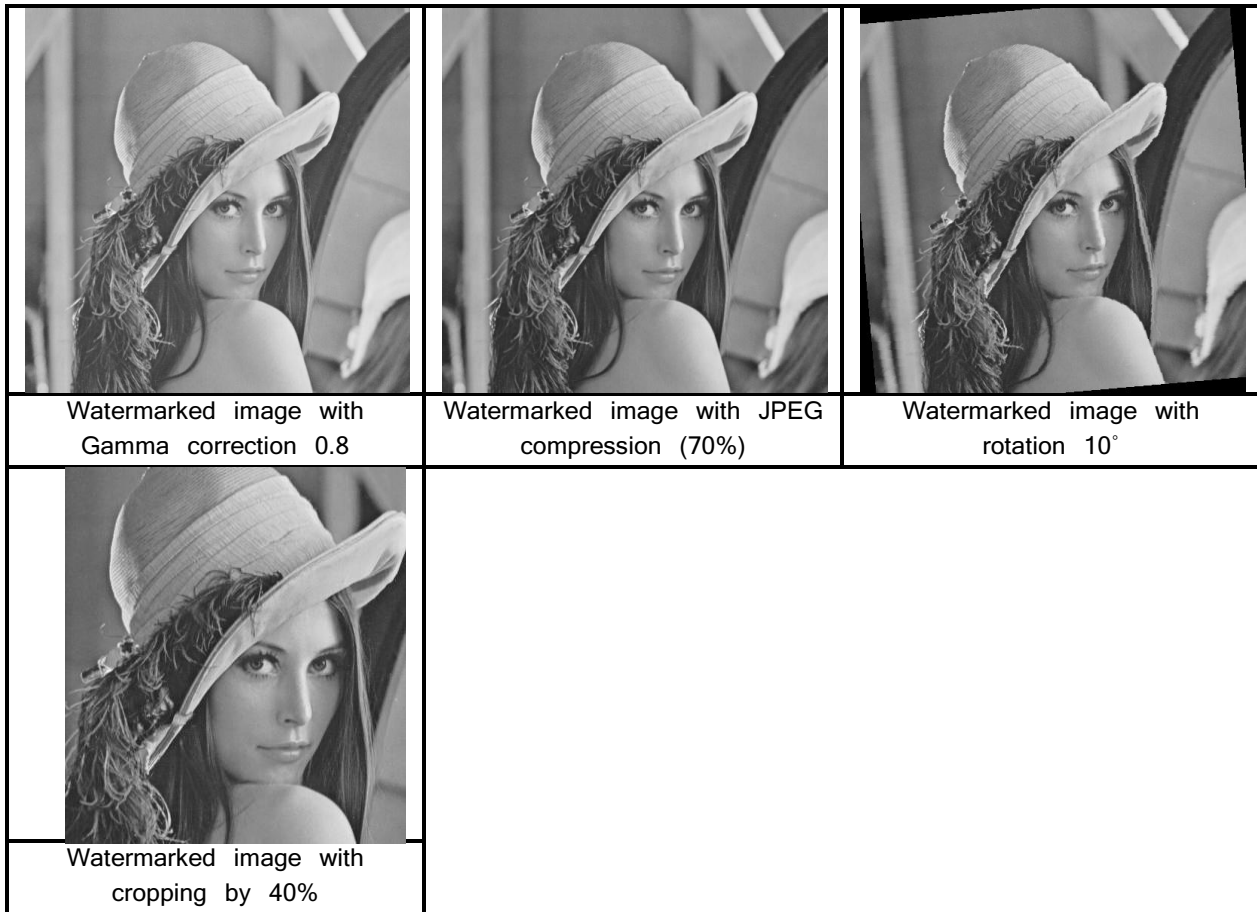
### 4.3 Experiments and results

The proposed watermarking scheme was tested without and with attacks like: Gaussian blur, Gaussian noise, median filter, JPEG compression, sharpening, rotation, cropping, contrast adjustment, and histogram equalization.

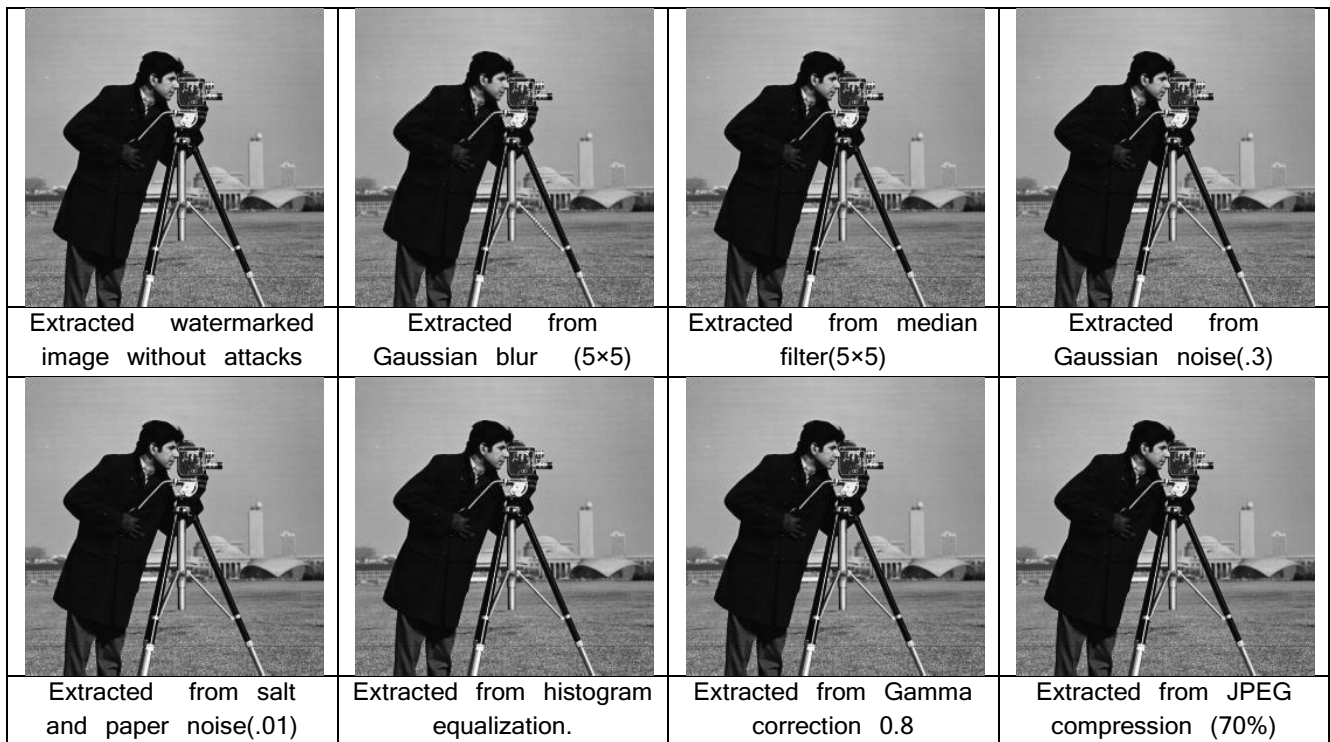
In figure 6 and figure 7 the human eyes will see the effect of noises on watermarked images and the best extracted watermark image from four quadrants q1, q2, q3 and q4 after applying the attacks on watermarked image. The Gaussian blur, Gaussian noise, and JPEG compression attacks have been resisted when Watermark embedded in the LL band (B1), The sharpening, cropping, Gamma correction, histogram equalization, and gamma correction attacks have been resisted when Watermark embedded in the HH band (B4), The Rotation attack has been resisted when Watermark embedded in the LH band (B2)

As you will see in table 1; 2; 3; 4, and 5 the results of proposed algorithm have been compared with those obtained from other watermarking scheme [6-8, 19]. Table. 2 and Table.5 show normalized correlation (NC) and bit correct ratio (BCR) values between the actual watermark and extracted watermark from attacked watermarked image. Table.1, Table.3, Table.4 show the PSNR, MSE, WDR values of the host image and watermarked images with and without attack. A comparison indicates that the proposed watermarking scheme more imperceptibility and robust against different kinds of noise which gives NC value 1 for almost type of attacks and good PSNR, MSE, WDR and BCR values





**Fig 6: shows different types of noisy attacked image**



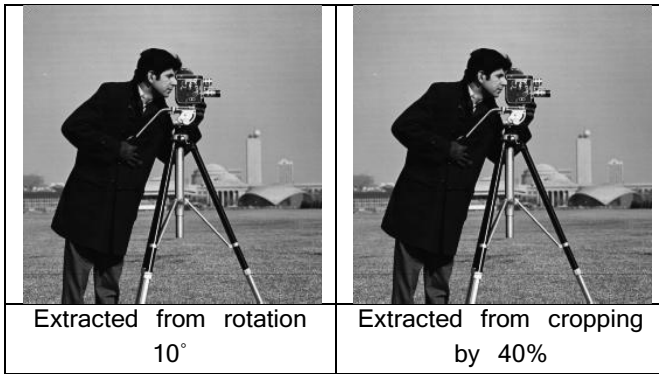


Fig 7: shows the extracted watermarked image from corresponding noisy attacked image

Table 1. Performance results in terms of PSNR

Attacks	Taoaand et al[19]	Sverdllov et al [7]	Ganic & Eskicioglu [6]	Khan et al [8]	Proposed
no attack	25.30558	23.3465785	35.13337126	46.95630406	60.1629
Gaussian noise(.3)	18.73769	18.3463352	19.64892076	19.75410542	20.76117552
Gaussian blur(5×5)	23.76955	22.7405456	28.60624198	28.6172194	28.61241029
Median(5×5)	25.06159	23.2723588	35.26316918	36.10192796	37.1834241
Salt and pepper noise (.01)	22.28095	21.2141854	24.81219223	25.15197639	25.24946064
Histogram Equalization	17.30584	18.0458	17.97187824	18.1253	19.12608388
Gamma correction 0.8	19.72367	17.9745	22.59161184	22.7966	24.79675591
Jpg compression	25.30254	23.3592	35.05785504	46.2929	49.30600308
Jpg compression (70%)	25.079	23.2308	36.97020805	37.8373	38.85970988
Cropping by 40%	7.73048	7.77342	7.803051	7.8056630	8.012634
Rotation 10°	12.2653	11.6	12.464989	12.4650	13.02654

Table 2. Performance results in terms of maximum NC

Attacks	Taoaand et al[19]	Sverdllov et al [7]	Ganic & Eskicioglu [6]	Khan et al [8]	Proposed
no attack	1	1	0.999202951	1	1
Gaussian noise(.3)	0.726898	0.9541332	0.985161922	0.989373417	1
Gaussian blur (5×5)	0.921751	0.94087959	0.999263307	0.998987557	1
Median(5×5)	0.978992	0.99590108	0.999391021	0.99946952	1
Salt and pepper noise (.01)	0.877382	0.99315087	0.995857768	0.998070789	1
Histogram Equalization	0.7943	0.7943	0.997564213	0.9993	1
Gamma correction 0.8	0.966461	0.9694	0.999272879	1	1
Jpg compression	0.999875	1	0.999190114	1	1
Jpg compression (70%)	1	1	0.999202951	1	1
Cropping by 40%	0.726898	0.9541332	0.985161922	0.989373417	.99958742136
Rotation 10°	0.921751	0.94087959	0.999263307	0.998987557	1

Table 3. Performance results in terms of WDR

Attacks	Taoaand et al[19]	Sverdllov et al [7]	Ganic & Eskicioglu [6]	Khan et al [8]	Proposed
no attack	-19.9335	-17.974502	-29.7612944	-41.58422717	-54.7908
Gaussian noise(.3)	-13.3656	-12.974258	-14.2768439	-14.38202854	-14.46687075
Gaussian blur (5×5)	-18.3975	-17.368469	-23.2341651	-23.24514251	-23.34510078
Median(5×5)	-19.6895	-17.900282	-29.8910923	-30.72985108	-30.8853
Salt and pepper noise (.01)	-16.9089	-15.842109	-19.4401154	-19.7798995	-19.97738376
Histogram Equalization	-11.9338	-12.6737	-12.5998014	-12.7532	-13.854007
Gamma correction 0.8	-14.3516	-12.6024	-17.219535	-17.4245	-17.42467903
Jpg compression	-19.9305	-17.9871	-29.6857782	-40.9208	-45.9339262
Jpg compression (70%)	-19.7069	-17.8587	-31.5981312	-32.4653	-33.46593242
Cropping by 40%	-2.3584	-2.3987	-2.4309748	-2.43358620	-2.9687
Rotation 10°	-6.8932	-6.98567	-7.0929128	-7.0928864	-7.9876

**Table 4. Performance results in terms of MSE**

Attacks	Taoaand et al [19]	Sverdllov et al [7]	Ganic & Eskicioglu [6]	Khan et al [8]	Proposed
no attack	1.80E+02	2.82E+02	18.70926733	1.229598999	0.0588
Gaussian noise(.3)	8.16E+02	8.93E+02	6.61E+02	6.46E+02	6.25E+02
Gaussian blur (5×5)	2.56E+02	3.25E+02	84.09490973	83.88261617	81.97555393
Median(5×5)	1.90E+02	2.87E+02	18.15837533	14.96928684	14.96600037
Salt and pepper noise (.01)	3.61E+02	4.61E+02	2.01E+02	1.86E+02	1.84E+02
Histogram Equalization	1.13E+03	956.7924	9.73E+02	939.431	9.12E+02
Gamma correction 0.8	6.50E+02	972.6184	3.36E+02	320.4314	3.12E+02
Jpg compression	1.80E+02	281.498	19.03743362	1.4325	1.331419373
Jpg compression (70%)	1.89E+02	289.9468	12.25668716	10.0383	9.03674698
Cropping by 40%	1.0288338e+04	1.023269e+04	1.01178e+04	1.01117762e+4	1.00115862e+4
Rotation 10°	3.6213e+003	3.5469e+003	3.4585e+03	3.4586e+003	3.4469e+003

**Table 5. Performance results in terms of BCR**

Attacks	Taoaand et al [19]	Sverdllov et al [7]	Ganic & Eskicioglu [6]	Khan et al [8]	Proposed
no attack	0.030518	1.9638	0	9.7351	0
Gaussian noise(.3)	0.030518	0	0	0	0
Gaussian blur (5×5)	0.001526	0	0	0	0
Median (5×5)	0.19989	0	0	0	0
Salt and pepper noise (.01)	1.313782	0	0	0	0
Histogram Equalization	0.012207	0	0	0	0
Gamma correction 0.8	0	0	0	0	0
Jpg compression	1.159668	0	0	0	0
Jpg compression (70%)	0.1663	0	0	0	0
Cropping by 40%	0.64086	0	0	0	0
Rotation 10°	0.0031	0	0	0	0

## 5. CONCLUSIONS

In this paper, a combined digital watermarking technique based on BEMD-DWT-DCT-SVD had been presented. The performance of this proposed techniques had been investigated and discussed in comparison with four different related techniques. The robustness of the proposed technique was tested against a set of different categories of attacks. The combination of these transforms in the proposed technique had improved the watermarking imperceptibility and makes it robust against nine different types of attacks, e.g. jpeg compression; salt and pepper noise and image cropping. The proposed technique had shown a great improvement in handling cropping attacks as well as rotation attacks.

## 6. REFERENCES

- [1] C.I. Podilchuk and E.J. Delp. 2001. Digital Watermarking: Algorithms and Applications. IEEE Signal Processing Magazine Journal, vol. 18, no. 4, pp. 33-46, (July 2001).
- [2] I.J. Cox, M.L. Miller, and J.A. Bloom. 2002. Digital Watermarking. Morgan Kaufmann.
- [3] W.C. Hu, W.H. Chen, and C.Y. Yang. 2012. Robust image watermarking based on discrete wavelet transform, discrete cosine transform and singular value decomposition. Journal of Electronic Imaging, vol. 21, no. 3, p. 033005, (July 2012).
- [4] P. Taoaand and A.M. Eskicioglu. 2004. A robust multiple watermarking scheme in the Discrete Wavelet Transform domain. Internet Multimedia Management Systems Proceedings of the SPIE, vol. 5601, pp. 133-144.
- [5] M. Mondal and D. Barik. 2012. Spatial Domain Robust Watermarking Scheme for Color Image. International Journal of Advanced Computer Science, vol. 2, no. 1, pp. 24–27, (January 2012).
- [6] E. Ganic and A.M. Eskicioglu. 2004. Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies. Proceedings of the 2004 multimedia and security workshop on Multimedia and Security. pp. 166-174, (September 2004).
- [7] A. Sverdllov, S. Dexter, A.M. Eskicioglu. 2005. Robust DCT-SVD Domain Image Watermarking For Copyright Protection: Embedding Data In All Frequencies. Proceedings of the 13th European Signal Processing Conference (EUSIPCO2005). Antalya. Turkey.(September 2005).
- [8] M.I. Khan, M.M. Rahman and M. I. H. Sarker. 2013. Digital Watermarking for Image Authentication based on Combined DCT, DWT, and SVD Transformation. International Journal of Computer Science, Vol. 10. No. 5, pp. 223–230.
- [9] K. Loukhaoukha, A. Refaey, K. Zebbiche, and M. Nabti. 2015. On the Security of Robust Image Watermarking Algorithm based on Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition. International Journal of Applied Mathematics and Information Sciences, Vol. 9, no. 3, pp. 1159-1166-81, (May 2015).
- [10] K. Amolins, Y. Zhang and P. Dare. 2007. Wavelet based image fusion techniques—An introduction, review and

- comparison. ISPRS J. Photogramm. Remote Sens., vol. 62, no. 4, pp. 249-263.
- [11] W. Dong, X. Li, X. Lin, and Z. Li. 2024. A Bidimensional Empirical Mode Decomposition Method for Fusion of Multispectral and Panchromatic Remote Sensing Images. *remote sensing*, vol. 6, no. 9, pp. 8446-8467.
- [12] H. Olkkonen. 2011. Discrete wavelet transforms - algorithms and applications. InTech. (August 2011).
- [13] K.R. Roa and P. Yip. 1990. Discrete Cosine Transform: Algorithms, Advantages, Applications "Academic Press, Boston.
- [14] K. Baker. 2005. Singular Value Decomposition Tutorial, (March 29, 2005)
- [15] T. Ramashri and S.N. Reddy. 2009. Robust Image Watermarking Algorithm Using Decimal Sequences. *International Journal of Wireless Networks and Communications*, vol. 1, pp. 1–8.
- [16] A. Al-Haj and A. Abu-Errub. 2008. Performance Optimization of Discrete Wavelets Transform Based Image Watermarking Using Genetic Algorithms. *Journal of Computer Science*. vol. 4, no. 10, pp. 834-841.
- [17] J.J. Eggers and B. Girod. 2001. Quantizaion effects on digital watermarks. *Signal Processing*, vol. 81, no. 2, pp. 239– 263, (February 2001).
- [18] J.S. Pan, H.C. Huang, and F.H. Wang. 2001. Genetic Watermarking Techniques. Fifth Int'l Conf. on Knowledge-Based Intelligent Information Engineering System & Allied Technologies.
- [19] P. Taoaand and A.M. Eskicioglu. 2004. A robust multiple watermarking scheme in the Discrete Wavelet Transform domain. *Internet Multimedia Management Systems Proceedings of the SPIE*, vol.5601, pp. 133-144.