A Hybrid Watermarking Scheme for Increasing Watermark Capacity and Security

R. A. El-Sheikh
Electronics and Communications Engineering Department
Faculty of Engineering
Mansoura University
Mansoura 35516 Egypt

F. Khalifa
Electronics and Communications Engineering Department
Faculty of Engineering
Mansoura University
Mansoura 35516 Egypt

M. A. Mohammed
Electronics and Communications Engineering Department
Faculty of Engineering
Mansoura University
Mansoura 35516 Egypt

ABSTRACT
Imperceptible and robust watermarking schemes have been vastly used recently as powerful tools to guard the copyright protection, rightful ownership, and content authentication. This paper introduces a secure hybrid digital image watermarking algorithm based on bi-dimensional empirical mode decomposition (BEMD); redundant discrete wavelet transform (RDWT); discrete cosine transform (DCT) and singular value decomposition (SVD). A watermark is scrambled by Arnold transform to boost up its secrecy and robustness. The main purpose of this scheme is to increase the embedding watermark capacity and encryption while keeping it robust against different types of attacks. The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) are two most common quantities used to estimate the strength of watermark image encryption algorithms/ciphers with reference to differential attacks. A high NPCR/UACI score is usually explicated as a high resistance to differential attacks, as well as higher PSNR evaluation metrics. Experimental using PSNR, WDR, MSE, NC and BCR metrics on different host images (Lena, Barbara, and Boat) and the cameraman as the watermark image show that the presented scheme is rich in terms of imperceptibility, capacity, security and robustness. This has been also highlighted by comparing its performance against other state-of-the-art schemes.

Keywords
Robust watermarking, BEMD, NPCR, UACI, Redundant Discrete wavelet transform (RDWT).

1. INTRODUCTION
Since that moment when technology and wireless networks have begun to grow widely around the world a question seemed to arise about how to secure multimedia digital content such as ownership identification, content authentication, copyright protection and tamper detection. From all data hiding techniques (cryptography, watermarking, and steganography), watermarking is the best solution to deal with these tasks. Digital watermarking is simply the process of embedding some information into a multimedia element, such as image, video or audio that can be extracted later on to prove the authenticated owner of the media. Watermarking may be fragile, semi-fragile, or robust, non-blind, semi-blind or blind, visible or invisible etc. Imperceptibility, robustness, capacity, and security are the basic necessities for a secure watermarking scheme. Imperceptible means cover image and watermarked image should be the same. Robustness means that the watermark algorithm should be resistant to geometric attacks (e.g., filtering, scaling, noise addition, translation, rotation, cropping). Security implies protection against noxious attacks [1, 2], and capacity simply refers to how much data can be embedded in the original image.

Watermarking algorithms can be grouped in two categories: spatial domain, and frequency (or transform) domain [1, 3]. Transform domain methods (e.g., DWT, DCT, SVD) have good imperceptibility and more robust. Spatial domain techniques are less robust against various geometric attacks, but high data hiding capacity [2].

In literature, a tremendous number of research work in watermarking field has been investigated. For example,

El-Assy et al. [1] presented a hybrid digital watermarking technique using advantages of four algorithms BEMD, DWT, DCT, and SVD. In their framework, the watermark is embedded into the 2nd IMF and the SVD is applied on the mid frequency band of the DCT block. This watermarking scheme is robust against some attacks such as: Gaussian blur, median filter, rotation, cropping, JPEG compression, contrast, sharpening, and histogram equalization, etc. Rahman et al. [4] presented an image watermarking scheme based on DWT, DCT, and SVD. The host image re-arranged by zigzag order, then DWT is applied to the re-arranged matrix. DCT is applied on the high frequency bands (LH, HL, HH). Finally, SVD is applied on the high frequency components to embed the watermark. This algorithm fails to some attacks (compression, cropping, and Gaussian noise). Khan, et al. [5] proposed a hybrid scheme based on DWT, DCT, and SVD. They decomposed the host image into four bands using DWT and apply DCT on HH then map the DCT coefficients in a zigzag order into four quadrants. Finally, the SVD is applied to each quadrant. Their algorithm demonstrated more robustness and invisibility against some of geometric attacks. Chaturvedi et al. [6] decompose original image into 1-level sub bands using DWT, the lowest level (LL) has been selected for watermark embedding as it contains maximum energy. Gaur et al. [2] presented a new hybrid technique based on RDWT, DCT, and SVD using Arnold transform and zigzag sequence to make their algorithm more secure. They decomposed the input image using RDWT into four sub bands and the DCT is applied on high frequency sub-band. Finally, they applied the SVD on of mid, high frequency sub-bands of DCT coefficients to embed the data. This technique is secure against various geometric. Lagzian et al. [17] proposed a scheme based on RDWT-SVD using advantage of RDWT over DWT. The RDWT is applied to host image and the SVD is applied on LL. Finally, singular value of the LL watermark sub band is embedded in the singular value of an image. However, the algorithm is not robust against geometrical attacks.

Biad et al. [8] presented a watermarking scheme based on the bi-dimensional empirical mode decomposition (BEMD). The BEMD is applied to host image to obtain (IMF1, IMF2, IMF3, R1) and the DWT is applied on R1. Then, SVD is applied to the HL sub-band to embed the watermark. The scheme in [8] is more robust against JPEG compression, noise addition and filtering. The use of the BEMD has been approved for common image processing. Zhou, et al. [9] proposed hybrid watermarking algorithm based on DWT and SVD. They decomposed the host image into four bands using the DWT, decompose (LH, HL) into another four sub bands, then apply the SVD to (LH2, HL2) and embed the same watermark data after encryption with a certain key by modifying the singular values. However, this algorithm is not robust to all types of attacks.

The previous research work has its own limitations. To partially overcome the individual limitations of those schemes, this paper introduces a new robust digital image watermarking scheme using gray scale image as cover and watermark. This pipeline utilizes BEMD, RDWT, DCT, and SVD schemes in an effort that each technique compensates the defect in others. Also, the proposed algorithm incorporates RDWT instead of DWT to exploit the shift invariant property of over DWT. In this scheme, a watermark is embedded in the singular values of the DCT block in high frequency bands of RDWT which selected from second IMF. The Proposed algorithm has also been analyzed with RDWT-SVD,

RDWT-DCT-SVD, DWT-SVD, DWT-DCT-SVD,

DWT-DCT, BEMD-DWT-SVD; BEMD-DWT-DCT-SVD based techniques by applying various geometric attacks. Although, this schema has not improved the results significantly from BEMD-DWT-DCT-SVD paper whose resistance to image processing attacks was higher than others, it increased the capacity of the embedded watermark. Also, this algorithm has provided the embedded data area with encryption using Arnold scramble method to make it more secure, imperceptible and robust, which are the main purposes of the suggested work.

The rest of this paper is organized as follows. The transform techniques used for watermarking are described in Section 2. The embedding and extraction steps of the proposed scheme are given in Section 3. In Section 4, description of the metrics that used to evaluate the performance of the proposed technique is fully described.

Experimental results, the comparison with the previous algorithms, and the discussion of the presented results are presented in Section 5. Finally, the conclusions of the research work are given in Section 6.

2. METHODS

Here, a non-blind, hybrid, and robust digital image watermarking is introduced. The proposed technique combines multiple algorithm utilizes the idea that each algorithm compensates the drawback of others. The proposed pipeline consists of BEMD, RDWT, DCT and SVD techniques with Arnold scramble to improve the robustness against different kind of attacks. Since this algorithm is a hybrid technique utilizing multiple algorithms, details of those algorithms are given below.

2.1 Bi-dimensional Empirical Mode Decomposition

The BEMD is similar to one-dimensional (1-D) EMD; however, the surface envelope interpolation and the extrema detection are more complicated. The EMD method is a time domain analysis method it is used for the non-stationary and nonlinear data. With which any complicated data can be decomposed into a small and finite number of intrinsic mode functions using the sifting and iteration process according to Huang method [1, 8]. The author has expressed a set of intrinsic mode functions by Eq.1.

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

where X(t) is the input signal decomposed into *n* intrinsic mode functions (IMFs) and a residue.

One of the most important features in the EMD method is that the basic functions are derived directly from the signal itself In contrast to Fourier analysis; the basic functions are represented by sum of sines and cosines. So, the EMD is more adaptive.

2.2 Redundant Discrete Wavelet Transform

The DWT is one of the most popular transform methods used in image processing application because of its spatio-frequency localization property. It has been observed that down-sampling attains shift variant even for a slight shift in the whole cover image. That occurs because of the down sampling of its bands. Due to the major changing in the wavelet coefficients of the image, erroneous extraction of the original and watermark image data occurs. This is the weakness point in DWT. The researchers have proposed RDWT techniques to overcome this obstacle. For this, RDWT based techniques become more robust than DWT based techniques. In RDWT the size of the sub band at the same decomposition level is the same as the host image but decreased in DWT. RDWT analysis and synthesis equations can be expressed as the following equations [7, 10]:

Analysis equations

$$\mathbf{C_j[K] = C_{j+1}[K] + h_j[-K]} \quad (2)$$

$$\mathbf{d_j[K] = C_{j+1}[K] + g_j[-K]} \quad (3)$$

Synthesis equation

$$\mathbf{C_{j+1}[K] = 1/2(C_j[K] * h_k[K] + d_j[K] * g_i[K])} \quad (4)$$

Fig.1 and Fig.2 represents the one dimensional RDWT and one dimensional DWT respectively and their inverse transform [2].

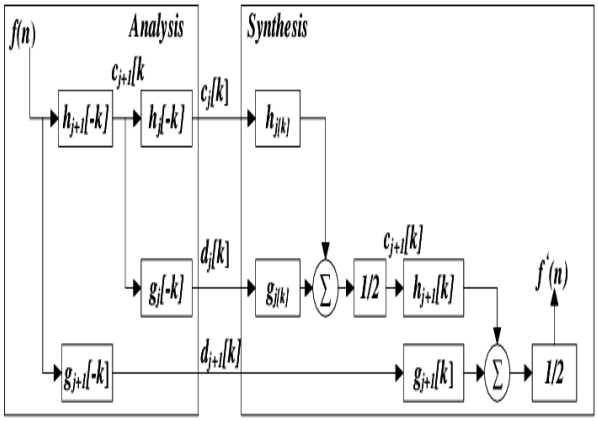

Fig 1: Analysis and synthesis filters of 1-D RDWT

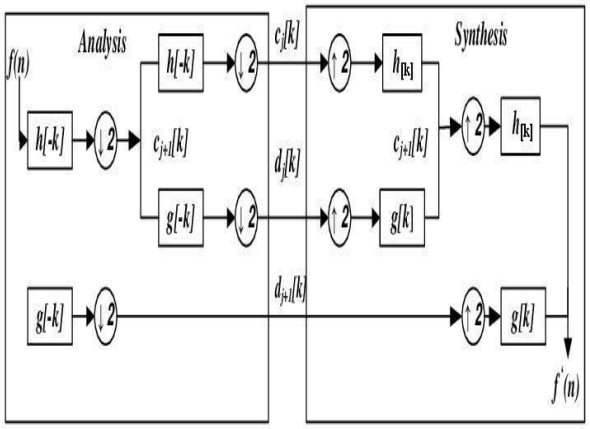

Fig 2: Analysis and synthesis filter banks of 1-D DWT

where * means convolution, ↑2 means up sampling and ↓2 means down sampling at each iteration in DWT. Down sampling decreased the size of each sub band and increased the decomposition level. RDWT is ignoring both the up and down sampling of coefficients. At the end of each level the output coefficient two times that of the input. All of the above illustrates that RDWT based digital image processing techniques is more robust than DWT based techniques due to directionality, shift invariant, and spatio-frequency localization property [2,10]. This was the primary reason to use this technique in the embedding algorithm.

2.3 Discrete Cosine Transform

The DCT is a method used for converting a signal into primary frequency components and points to an image as a sum of sinusoidal of different frequencies and magnitudes. It splits the spectral areas of the image into low, medium and high frequency sub-bands according to their energy as shown in Fig.3 [1, 2]. The 1-D DCT is useful in processing 1-D signal such as speech waveforms, but the 2-D DCT is used in image compression. DCT-based watermarking is based on 2 facts; the 1st fact is that the low-frequency sub-bands which contains the most important visual parts of the image which called DC value and the rest is AC values of the image has most of the signal energy, The 2nd fact is that high frequency components of the image are usually ousted by noise attack and compression. The DCT has been used in standard JPEG image compression because of its good performance, but it is computationally more expensive and difficult to implement [5].

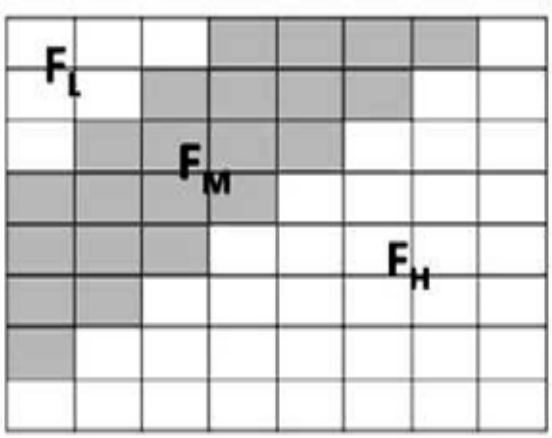

Fig 3: DCT Region

2.4 Singular Value Decomposition

The SVD is a mathematical tool that belongs to the orthogonal transforms category used to analyze matrices and it's also used in various applications like noise reduction, image compression, image hiding and image watermarking. In this method a certain matrix can be decomposed into three matrices of either the same or different dimensions under some conditions. In SVD the maximum available energy is compressed into the minimum number of coefficients, due to that it is quite used in digital image watermarking algorithms. In SVD any n x n matrix A is defined as $A=USV^t$ where U, V are left and right orthogonal matrices and S (Diagonal elements) which called singular values. The singular values do not affect the visual perception because of the good stability property. It is important to know that each singular value represents the luminance of an image while the pair of the singular vectors allocates the geometric characteristics of the image layer [2,8]. Singular values are less affected when image processing is performed. This is due to the fact that bigger singular values do not only ensure the most energy of an image, but also withstand attacks. For that reason, the matrix S has been used as a choice for embedding a robust watermark [7].

2.5 Arnold Scrambling Transform

For security realization and to improve the robustness, scrambling transformation is utilized in the watermark images before embedding into the host image. Scrambling transformation is one of the various technologies which used in encryption systems; after applying Arnold transform the relationship between pixels in the image will be destroyed and distributed everywhere in the carrier evenly. This will make the algorithm more robust. Due to the transformation a watermark that is meaningful will become a meaningless, chaotic image. Thus, any attacker won't be able to recover the watermark without knowing the scrambling algorithm and keys even if he extracted it from the embedding system. Arnold transformation is defined in equation [3]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \qquad (5)$$

where (x, y) state the pixel coordinates of the original space, while (x', y') state the pixel coordinates after a certain number of iterations, N is the size of the square image, also known as a step number. The initial state of the original image can be retrieved after a certain number of iterations according to the previous formula. Arnold transformation is cyclical. So the image will not be restored if the number of iterations and cycle is unknown. Therefore, in the Arnold transformation cycle and iterations can be considered as a private key [2, 11, 12].

3. PROPOSED ALGORTHIMS

Overall, a step-by-step algorithm of the embedding and extraction schemes are described in the following algorithms

3.1 a Watermark Embedding

a) Read the original image (I), then encrypt image using Arnold scramble (A).

b) Apply BEMD on the A vector to decompose it into three IMF's and a residue.

c) Apply RDWT to the second IMF to decompose it into four sub-bands (LL, LH, HL and HH).

d) DCT is applied on the four sub-bands (LL, HL, LH and

HH) and get DCT coefficient matrices D1, D2, D3, and D4.

e) Apply SVD on D2, D3 and D4 to get S1, S2, and S3.

f) RDWT is applied on the watermark image to decompose it into four sub-bands of the same size (LL, HL, LH, and HH).

g) Apply Arnold scramble on the DCT Coefficients that applied on all sub-bands of RDWT of watermark and get (Aw) matrix for the sub-bands.

h) Modify the scrambled coefficients of A_{wi} with S1, S2, S3 as the following equation [4]:

$$\mathbf{S_{ii} = S_i + con * A_{wi}} \tag{6}$$

i) Apply SVD after Embedding watermark.

j) Apply inverse SVD and inverse DCT, then apply inverse RDWT to get second IMF*.

k) Apply inverse Arnold scramble to get watermarked image WI.

3.1.b Watermark Extraction

l) Scramble watermarked image using Arnold map and get (Ar*) matrix.

m) Apply BEMD on (Ar*) matrix to decompose it into the intrinsic mode functions (IMFs).

n) Apply RDWT on the second IMF to decompose it into four sub-bands LL, HL, LH and HH.

o) DCT is applied to the four sub bands and get four coefficient matrices d1, d2, d3, d4.

p) SVD is applied on d1, d2, d3 to get the singular values Se1, Se2, Se3.

q) Apply inverse SVD to get iS1, iS2, iS3 matrices.

r) Modify the previous matrices using the following Eq. [5]:

$$\mathbf{S_w = \frac{(iS_i - S_i)}{con}} \tag{7}$$

s) Apply inverse Arnold scramble to $\mathbf{S_w}$ matrix.

t) Inverse DCT and inverse RDWT is applied to get Extracted watermark.

Robustness and imperceptibility are usually two common matrices used to evaluate the watermarking algorithms.

4. PERFORMANCE METRICS

Robustness and imperceptibility are usually two common metrics used to evaluate the watermarking algorithms. In this paper, different metrics have been used for evaluation. Details of those metrics are given below.

4.1 Robustness Measures

To check the robustness of the watermark algorithm against several types of attacks, such as geometric, filtering and noise attacks such as (Gaussian, Salt & Pepper) etc. the bit-correct ratio (BCR) and the normalized correlation coefficient (NC) have been used [1, 2]. Figure (5) shows the results of applying different attacks to the watermarked image.

i. The bit correct ratio (BCR)

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

ii. Correlation Coefficients (NC)

$$\mathbf{NC = \frac{\sum_i \sum_j W_n(i,j) * W_n'(i,j)}{\sum_i \sum_j |W_n(i,j)|^2}} \tag{9}$$

where (W, W`) are the original watermark and extracted watermark respectively. The unity value given exact matching between the extracted watermark and the original watermark images, NC of about 0.7 or above is counted passable [8].

4.2 Imperceptibility Measures

Peak signal to noise ratio, the mean square error, and watermark to document ratio are the metrics that will be used for the capacity measures or imperceptibility as they will compare the amount of distortion inserted into a cover image by a watermarking algorithm [1, 10].

i. Peak Signal-to-Noise Ratio

The PSNR in decibels (dB) can be represented by the given formula:

$$\mathbf{PSNR = 20 x Log\, MAX / \sqrt{MSE}} \tag{10}$$

ii. Mean Square Error

$$\mathbf{MSE = \frac{1}{MxN} \sum_{j=1}^{N} x(i,j) - x'(i,j)^2} \tag{11}$$

iii. Watermark-to-Document Ratio (WDR)

$$\mathbf{WDR = 10 x \log \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (X(i,j) - X'(i,j))^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} x^2(i,j)}} \tag{12}$$

where MAX is the utmost value can a pixel take of the image; M and N represent the image dimensions; x(i, j) the original image's pixel value; X'(i, j) are the watermarked image's value of pixel.

4.3 Security analysis

A perfect encryption algorithm should withstand against familiar attacks, such as statistical, differential, and the other types of attacks. Some image that is indistinguishable from a real random image may be considered as an ideally encrypted one because the opponent cannot detect the local relations between plain text and cipher text. In general, any attacker will be able to detect a reliable relationship between the plain image and the cipher-image if he changes only one pixel (e.g., make a trivial change) of the encrypted image and notice that the result is changed. Thus, the attack which causes a severe change in the cipher-image with respect to confusion and diffusion due to one minor modification in the plain image would become very incompetent and virtually worthless.

To the best of the author's knowledge, Chen and Mao presented the unified average changing intensity (UACI) and the number of pixels change rate (NPCR) in 2004 [11, 13].

Since then, NPCR and UACI become most security analyses in the image encryption area. The UACI and the NPCR are the two common measures used to test the effect of changing one-pixel on the whole image encrypted to evaluate the encryption strength of the proposed algorithm [11, 14]. Let us assume that two cipher images at the grid (i, j) are indicated as $\mathbf{E^1(i,j)}$ and $\mathbf{E^2(i,j)}$ before and after changing only one pixel in the plain image, respectively; and a bipolar array with the same size as the image, A, is specified in Eq. (13). Then the NPCR is defined in Eq. (14), and UACI can be mathematically defined by Eq. (15), where T represents the total number of pixels in the cipher-text, F represents the largest pixel value, convenient with the format of the cipher text image.

$$A(i,j)=\begin{cases}0, & \text{if } E^1(i,j)=E^2(i,j)\\ 1, & \text{if } E^1(i,j)\neq E^2(i,j)\end{cases} \tag{13}$$

$$\mathbf{NPCR}=\sum_{i\,j}\frac{\mathbf{A(i,j)}}{\mathbf{T}}\mathbf{x100\%} \tag{14}$$

$$\mathbf{UACI}=\sum_{i\,j}\frac{\left|\mathbf{E^1(i,j)-E^2(i,j)}\right|}{\mathbf{F.T}}\mathbf{x100\%} \tag{15}$$

The range of NPCR is [0, 1]. So, if all pixel values in $\mathbf{E^2}$ are varied compared to those in $\mathbf{E^1}$ this means that $\mathbf{N(E^1,E^2)=1}$ and if all pixels in $\mathbf{E^2}$ still the same values as in $\mathbf{E^1}$ it means that $\mathbf{N(E^1,E^2)=0}$. The UACI focuses on the average variation between two cipher-text images, while NPCR concentrates on the total number of pixels that changes value in differential attacks [11, 14].

5. RESULTS AND DISCUSSION

The proposed algorithm has been developed and executed using MATLAB 2016, and a laptop that has RAM4GB, Processor: Intel(R) Core (TM) 2 Quad (Q6600) 2.40 GHz, and OS: Windows 7.1.

In this paper, different grayscale (Lena, Barbara, Boat) images as the original image and the grayscale cameraman image as the watermark image are used. All images' sizes were 512x512 pixels.

Fig 4: The cover (a) and watermark (b) images

The proposed watermarking algorithm was tested with and without attacks. The latter includes Gaussian blur, Gamma correction, Gaussian noise, median filter, salt& pepper, JPEG compression, sharpening, rotation, cropping, contrast adjustment, and histogram equalization. The effected watermarked images and the best extracted watermark image will be seen clearly by the human eyes as shown in figures 6 and 7.

To highlight the advantage of our pipeline, we compare its performance against state-of-the-art watermarking algorithms. The evaluation of our method and the compared one is based on the metrics described in Section 3. Tables 1 through 5, summarizing the quantitative comparison between the results obtained using the proposed algorithm and other.

All results are represented as the mean ± standard deviation values of some metrics that were processed on the three host images (Lena, Barbara, Boat) to ensure the efficiency of suggested algorithm.

In particular, Tables 1, 2 , and 3 document that the proposed scheme has a good response in terms of visual quality between the host image and watermarked images with and without attack based on using PSNR, WDR, and MSE evaluation metrics, respectively.

Furthermore, Table 4 and 5 show bit correct ratio (BCR) and normalized correlation (NC) values between the embedded and the extracted watermark. As demonstrated in the Tables, NC values of the proposed approach are higher than 0.999 for almost all types of attacks. Additionally, Table 6 and Table 7 show the encryption strength of the proposed watermarking scheme using NPCR is higher than 99.9% and the UACI is in the range of 33%, respectively. Due to this, it will very hard for any attacker to tamper or manipulate the secret watermark. All the previous work indicates to robustness and imperceptibility of the proposed watermarking scheme against different type of attacks.

6. CONCLUSIONS

In this paper, an encrypted, non-blind, combined digital watermarking technique based on BEMD-RDWT-DCT-SVD is presented. The cover image and the watermarked image are scrambled by Arnold transform to fulfill higher embedding security. Without knowing the scrambling scheme and key; it will be extremely hard for any attacker to recover the images even if he extracted the watermarking from the watermarked image. The performance of the proposed algorithm was examined after applying it to different gray-scale images and compared it with other eight stare-of-the-art techniques. Although, the proposed algorithm did not improve the results of this scheme significantly over the algorithm in [1], which has the highest robustness, our scheme highly increased the amount of embedding data while keeping the imperceptibility and the robustness against different types of attacks. Additionally, our scheme had shown an increased embedding watermarking security.

Original Image

Watermarked image- No attack

Watermarked image Gaussian blur

Watermarked image-Gaussian attack

Watermarked image-Histogram

Watermarked image-Gama correlation

Watermarked image-Cropping

Watermarked image-Salt & Paper

Watermarked image-Sharping

Watermarked image-Rotation

Watermarked image-JPEG compression

Watermarked image-JPEG 70% compression

Watermarked image-Median filter

Fig 6: Examples of watermarked images with different types of attack

Original Watermark

Watermark-No attack

Watermark-Gaussian blur

Watermark-Gaussian attack

Watermark-Histogram

Watermark-Gama correlation

Watermark-Cropping

Watermark-Salt & Paper

Watermark-Sharping

Watermark-Rotation

Watermark-JPEG compression

Watermark-JPEG 70% compression

s

Watermark-Median filter

Fig 7: Extracted watermarked image from the noisy attacked image in Figure 6

Table 1. Performance results in terms of PSNR

Attacks	Zhou et al. [9]	Chaturvedi et al. [6]	Rahman et al. [4]	Khan et al. [5]	Biad et al. [8]	El-Assy et al. [1]	Lagzian et al. [7]	Gaur et al. [2]	Proposed
No attack	45.58374 0.0000	51.77007 0.067602	37.16714 1.264639265	36.272905 1.032573636	42.69321 0.0000	51.77007 0.067601943	37.64934 0.002046859	46.47245 4.158842	44.17673 0.188536

Gaussian noise	20.10231 0.052291	20.11012 0.060715	20.032705 0.059092036	20.02119 0.0403006	20.058925 0.0436866	20.11012 0.0607148	20.02619 0.0366976	20.04194 0.018995	20.11448 0.303002
Salt & pepper(0.01)	25.44817 0.055324	25.32419 0.161373	25.04387 0.1863403	24.95602 0.1666097	25.2415 0.147377	25.32419 0.161373	25.15142 0.1512382	25.45409 0.163312	25.2182 0.379696
Sharping	30.64797 3.378098	38.21347 3.509766	27.202295 2.255940344	27.478655 2.5392602	30.2303 3.105632	38.21347 3.5097659	30.31909 2.9853122	34.26788 2.98083	32.47916 2.29125
Histogram equalization	19.12239 1.94327	19.02479 1.774191	19.88921 1.9574474	19.87809 0.96864	19.95858 1.9364166	19.02479 1.774191	19.11873 1.966222	19.11198 1.605205	16.96423 3.510848
Median (5x5)	27.15744 4.061594	32.86469 2.46006	26.944995 4.04770631	26.7152 4.3967391	27.141425 4.0361945	32.86469 2.4600598	26.85353 3.7613982	31.11175 3.31772	28.84802 2.744292
Rotation 10°	12.42861 0.26093	12.60225 0.215689	12.208455 0.2729516	12.191935 0.1365033	12.306235 0.2606244	12.60225 0.215689	12.34156 0.2634996	12.37897 0.21538	12.17816 0.27146
Cropping 40%	12.13974 0.262471	12.42205 0.336828	12.06459 0.198952375	12.05174 0.399616135	12.21467 0.2624476	12.42205 0.3368281	12.01311 0.2312644	11.87269 0.178644	11.95084 0.411807
Jpg compression (70%)	34.8207 1.22815	41.5029 3.187982	33.797585 1.5349971	33.474115 0.988266	35.205385 1.0416652	41.5029 3.187982	33.17657 0.7730995	36.79877 1.732786	36.59832 1.082323
Jpg compression	35.37085 1.110247	25.29261 12.67823	34.021965 1.35286469	33.75909 0.8209979	35.716855 0.95350078	25.29261 12.678232	33.60395 0.6665615	37.24537 1.738181	37.15508 0.997403
Gaussian Blur (5x5)	24.87858 2.234688	27.10234 1.994402	24.77238 2.28247199	24.698075 2.5080431	24.819085 2.2287271	27.10234 1.994402	24.68523 2.127762	27.03425 1.86801	24.84966 1.414528
Gamma correction (0.84)	25.37684 0.161696	25.26943 0.153526	25.18481 0.197312	25.21185 0.1045399	25.26322 0.1569925	25.26943 0.1535257	23.82702 0.1192696	25.35504 0.688757	25.34561 0.632216

Table 2. Performance results in terms of WDR

Attacks	**Zhou et al. [9]**	**Chaturvedi et al. [6]**	**Rahman et al. [4]**	**Khan et al. [5]**	**Biad et al. [8]**	**El-Assy et al. [1]**	**Lagzian et al. [7]**	**Gaur et al. [2]**	**Proposed**
No attack	-42.4435 0.632324	-45.2686 0.454543	-31.15608 1.897769215	-34.545675 2.967827352	-36.9214 0.273382674	-45.26855 0.454542946	-31.99463 0.442124917	-45.64818 5.759723	-38.7124 4.10544
Gaussian noise	-15.6285 0.933637	-15.6439 0.75943	-14.83084 0.9267071	-14.82451 0.9212038	-14.287115 0.2823134	-15.64392 0.7594296	-14.18471 0.8381287	-14.04442 0.720994	-14.0376 2.899405
Salt & pepper(0.01)	-21.0117 0.837282	-20.4209 0.840733	-19.976005 0.78641657	-20.03408 0.52314583	-19.46969 0.4204351	-20.42089 0.84073269	-19.38046 1.04704294	-19.71576 0.930377	-19.7105 3.593201

Sharping	-29.2912 1.090458	-35.9172 5.505407	-24.80748 1.2081052	-26.633415 1.92009076	-24.45849 3.2500879	-35.91721 5.5054073	-26.99795 3.67797624	-29.61942 3.63617	-27.5674 3.432799
Histogram equalization	-14.1901 1.541398	-13.359 1.235428	-14.514055 1.532960942	-14.580305 0.47672022	-14.186765 1.66307177	-13.35898 1.23542815	-14.17386 1.59122423	-14.23071 1.290695	-11.9361 6.619431
Median (5x5)	-26.1559 1.287824	-30.6854 4.560642	-25.78205 1.140448685	-25.96345 0.476720224	-21.369615 4.160105621	-30.6854 4.560642431	-23.4002 4.308541368	-26.20959 3.878885	-23.9962 3.584547
Rotation 10o	-8.08765 1.626518	-7.7494 2.137948	-7.78421 1.621431069	-7.806775 0.202587454	-6.53442 0.533714766	-7.7494 2.137948278	-7.97556 2.216175098	-8.05454 1.832279	-7.67818 2.480611
Cropping 40%	-10.0202 3.096172	-8.29729 4.387418	-8.96847 3.009849517	-8.95743 0.981380857	-6.44286 0.252357435	-8.29729 4.387418044	-9.96736 3.776328127	-9.96734 3.182119	-8.17951 3.6411
Jpg Compression (70%)	-31.1138 1.577786	-38.0672 4.565861	-29.646975 0.336614917	-31.202915 2.385454918	-29.433575 1.074115684	-38.06722 4.565861315	-28.62433 0.835637055	-31.09981 1.75948	-30.7019 3.16995`5
Jpg compression	-31.576 1.660217	-29.6108 13.06587	-29.75566 0.442204842	-31.4792 2.483290416	-29.945045 0.962238841	-29.61077 13.06587087	-28.86693 0.677836837	-31.55968 1.717551	-31.1209 3.201036
Gaussian Blur (5x5)	-23.2342 1.806594	-21.3416 5.048185	-21.64973 1.880280377	-21.626195 1.678480442	-19.047275 2.360468095	-21.34163 5.048185218	-22.72396 3.609306551	-23.21829 3.191405	-20.2273 3.404201
Gamma correction (0.84)	-21.5524 1.564776	-21.43 1.146671	-20.13881 1.588729119	-20.30147 1.620754549	-19.49141 0.39733153	-21.43003 1.146670863	-17.93974 1.181166727	-18.9721 1.514697	-18.9099 3.282176

Table 3. Performance results in terms of MSE

Attacks	Zhou et al. [9]	Chaturvedi et al. [6]	Rahman et al. [4]	Khan et al. [5]	Biad et al. [8]	El-Assy et al. [1]	Lagzian et al. [7]	Gaur et al. [2]	Proposed
No attack	0.00003 0.0000	0.000007 0.000002	0.00023991 0.000057	0.00024 0.000006	0.00005379 0.00000	0.00000665 0.000002	0.00017182 0.00000008	0.00002253 0.000007	000038 00000177
Gaussian noise	0.00977 0.000118	0.00975 0.000138	0.0099237 0.000132783	0.009955 0.000009	0.00986559 0.00001	0.00974962 0.00013799	0.00993987 0.0000084	0.00990389 0.000004	0.00974 0.000626
Salt & pepper(0.01)	0.00285 0.0000036	0.00293 0.000106	0.00313379 0.00013386	0.003195 0.0001179	0.002991655 0.00001	0.00293 0.000105955	0.00305392 0.00010456	0.00284833 0.000112	0.003007 0.000287

			5				2		
Sharping	0.00086 0.000834	0.000151 0.000251	0.00215972 0.00106217	0.00204 0.001109234	0.001199495 0.00076091	0.00015089 0.00025143	0.00092916 0.000772519	0.00037429 0.000678	0.000565 0.000554
Histogram equalization	0.01224 0.006045	0.01252 0.006267	0.01046337 0.00623931	0.010475 0.002309596	0.010288195 0.006066853	0.01252 0.006266577	0.01224975 0.0061392	0.01226879 0.005011	0.020118 0.023204
Median (5x5)	0.00192 0.002158	0.000517 0.000499	0.00296571 0.00222765	0.00292 0.00234481	0.002827175 0.002130408	0.00051705 0.000498843	0.0020637 0.002131548	0.00077415 0.00178	0.001304 0.00149
Rotation 10°	0.05717 0.00343	0.054926 0.002626	0.06021457 0.00288614	0.06037 0.001848711	0.058824425 0.003421828	0.05492567 0.002625833	0.05832357 0.003529482	0.05782331 0.002889	0.06056 0.003665
Cropping 40%	0.0611 0.00363	0.057253 0.004178	0.06218967 0.000146095	0.062605 0.005725263	0.0601598 0.003622743	0.05725251 0.00417756	0.06290562 0.003298679	0.06497264 0.002539	0.063814 0.006174
Jpg compression (70%)	0.00033 0.000008	0.0000071 0.00001	0.00044002 0.000146095	0.00045 0.000008	0.000308705 0.000007	0.00007075 0.00001	0.00048122 0.0000075	0.00020899 0.000131	0.000219 0.0000064
Jpg compression	0.00029 0.00006	0.002956 0.039059	0.00040836 0.0001275	0.00042 0.00007	0.000272835 0.00006	0.00295623 0.039059234	0.00043612 0.000006	0.00018857 0.000119	0.000193 0.00005
Gaussian Blur (5x5)	0.00325 0.001792	0.001949 0.001227	0.00380322 0.0018518	0.0038 0.002010075	0.00374043 0.001789	0.00194879 0.0012271	0.00339998 0.0017963	0.00197959 0.001523	0.003274 0.001139
Gamma correction (0.84)	0.0029 0.000105	0.002972 0.000101	0.00303346 0.000138218	0.00301 0.000007	0.0029766 0.00010512	0.00297206 0.000101281	0.00414284 0.000113	0.00291404 0.00055	0.00292 0.000386

Table 4. Performance results in terms of NC

Attacks	Zhou et al. [9]	Chaturvedi et al. [6]	Rahman et al. [4]	Khan et al. [5]	Biad et al. [8]	El-Assy et al. [1]	Lagzian et al. [7]	Gaur et al. [2]	Proposed
No attack	1.0000 0.0000	0.99717 0.002394	0.99947 0.000612	0.99947 0.000612	1.0000 0.0000	0.99717 0.002394	0.99909 0.000404	0.98554 0.006329	0.99944 0.000006
Gaussian noise	2.84898 0.271898	0.91905 0.115272	1.000655 0.001969	1.0006 0.00194	1.0000 0.0000	0.91905 0.115272	1.06896 0.01686	1.01929 0.02211	0.99944 0.000006
Salt & pepper(0.01)	1.63999 0.132825	0.931 0.092994	0.999905 0.00111429	0.99992 0.0011231	1.0000 0.0000	0.931 0.092994	0.94996 0.007643	0.99934 0.020957	0.99946 0.0000067
Sharping	2.82584 0.757077	1.03095 0.072401	1.000095 0.00131348	1.00014 0.00112305	1.0000 0.0000	 0.0724012	1.14068 0.0414025	0.99207 0.078224	0.99944 0.0000066

Histogram equalization	2.57925 1.011572	3.04294 5.902391	0.999965 0.00109701	0.99985 0.00134616	1.0000 0.0000	3.04294 5.90239054	5.8087 1.062073943	0.99492 2.047579	0.99945 0.0000067
Median (5x5)	-1.05234 0.738096	0.11895 0.568467	0.99879 0.0001531	0.998715 0.0010187	1.0000 0.0000	0.11895 0.568467076	0.90699 0.0315056	0.98009 0.043826	0.99945 0.0000071
Rotation 10^{o}	-0.38964 0.257278	-26.5439 9.662153	0.998925 0.0000015	0.998895 0.0000057	1.0000 0.0000	-26.54392 9.662153093	0.89744 0.0897426	0.98392 0.044843	0.99946 0.000008
Cropping 40%	-0.34382 0.356776	-1.21324 8.936317	0.998905 0.000004	0.99881 0.00013454	1.0000 0.0000	-1.21324 8.936317022	1.47591 1.7248406	0.98669 1.049537	0.99944 6.09E-05
Jpg compression (70%)	0.71106 0.103983	1.01118 0.058961	0.999185 0.00029445	0.999235 0.00032716	1.0000 0.0000	1.01118 0.058960506	1.00043 0.0039735	0.98511 0.007451	0.99944 0.000006
Jpg compression	0.75501 0.084783	-0.00212 0.930882	0.999245 0.00036373	0.99928 0.00038553	1.0000 0.0000	-0.00212 0.93088183	0.99796 0.00353533	0.98516 0.007722	0.99944 0.000006
Gaussian Blur (5x5)	-1.63844 0.856765	0.16728 0.782763	0.99867 0.0002801	0.998605 0.0003308	1.0000 0.0000	0.16728 0.782763117	0.79287 0.07323531	0.97668 0.119397	0.99944 0.000007
Gamma correction (0.84)	0.87584 0.090654	4.3417 0.797779	0.99945 0.00059758	0.99943 0.00058924	1.0000 0.0000	4.3417 0.797779167	3.82474 0.07864517	0.98502 1.369244	0.99944 0.000006

Table 5. Performance results in terms of BCR

Attacks	**Zhou et al. [9]**	**Chaturvedi et al. [6]**	**Rahman et al. [4]**	**Khan et al. [5]**	**Biad et al. [8]**	**El-Assy et al. [1]**	**Lagzian et al. [7]**	**Gaur et al. [2]**	**Proposed**
No attack	100.00 0.0000	16.68549 48.24589	96.31653 2.1266524	98.158265 2.1266524	99.85428 0.168263	16.68549 48.245894	99.73831 0.3628546	98.56796 0.477794	98.5588 0.036218
Gaussian noise	76.82648 1.371476	13.00354 21.97792	92.39578 2.260573878	93.563845 2.931065757	100.00 0.0000	13.00354 21.977922	67.57393 0.7113244	98.24409 14.24751	98.2212 0.02839
Salt & pepper(0.01)	77.3819 1.913213	13.30261 22.38459	95.15305 1.809098443	96.29078 2.1263503	99.958805 0.042395	13.30261 22.384594	76.828 1.2267942	98.20213 10.04864	98.1789 0.124501
Sharping	88.21716 0.205953	16.87775 21.41213	93.80302 3.05588695	96.31119 1.9284337	99.96338 0.0422851	16.87775 21.412133	82.25975 3.539307	98.48061 9.207403	98.3887 0.060693
Histogram equalization	89.32495 0.739572	13.39417 22.74529	90.4644 5.6654457	93.740845 5.8250152	100.00 0.0000	13.39417 22.74529	82.13844 4.05156756	98.45505 8.629038	98.4459 0.042438
Median (5x5)	23.75488	13.30109	95.79468	96.97418	99.51782	13.30109	61.8248	98.58589	98.58551

	5.205823	20.98925	1.597435414	0.43960415	1.74047E-14	20.98925162	4.23014192	18.21462	0.0536
Rotation 10°	35.57281 5.787853	12.45117 21.99427	96.46263 1.86758	96.4077 1.8282139	100.00 0.0000	12.45117 21.99427165	56.08292 1.697367737	98.48404 19.7465	98.473 0.079042
Cropping 40%	29.36554 5.70518	12.64343 21.51871	95.48416 1.82327412	96.529195 1.37045821	99.51782 0.2475505	12.64343 21.51870987	62.52174 13.71263942	98.60954 15.44739	98.5794 0.021566
Jpg compression (70%)	68.23883 8.281702	15.70435 22.42193	96.59119 1.4586561	97.9578 1.472567545	99.674225 0.0731848	15.70435 22.42192996	98.5363 0.18325391	98.5775 0.019696	98.5729 0.053397
Jpg compression	69.47784 9.662108	12.72278 25.56947	96.56677 1.5893022	98.015405 1.5868599	99.7467 0.040374165	12.72278 25.56946573	98.50845 0.13070275	98.57941 0.087136	98.5706 0.045952
Gaussian Blur (5x5)	20.59937 3.156307	12.81738 21.69116	95.08934 1.7780292	96.590425 0.3855967	99.51782 1.74047E-14	12.81738 21.69115933	53.74985 3.25284407	98.60802 2 1.73951	98.60802 0.032978
Gamma correction (0.84)	83.47778 12.27867	14.0686 22.27925	96.79298 1.904018	98.41938 1.7662686	99.6727 0.227175422	14.0686 22.27924757	59.2453 0.005196152	98.57101 18.53832	98.5706 0.036461

Table 6. Performance results in terms of NPCR/UACI

PER %	Gaur et al [2]	Proposed
NPCR	99.4854	99.6487
UACI	23.03	37.1609

7. REFERENCES

[1] A. M. El-Assy, M. A. Mohamed, M. E. A. Abou-El-Seoud, "Improved BEMD-DWT-DCT-SVD Robust Watermarking Technique for Still Images", *International Journal of Computer Applications*, Vol.150, No.9, pp 13-20, 2016.

[2] Q. Zheng, N. Yen, C. C. Tung, H. H. Liu, "The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis", *The Royal Society*, 1996

[3] L. Gahalod, "A Review on Digital Image Watermarking using 3-Level Discrete Wavelet Transform", *IJSRSET, 4099 Themed Section: Engineering and Technology*, Vol. 4, Issue 1, Print ISSN: 2395-1990, Online ISSN : 2394-9301, pp 930-936, 2018.

[4] M. Rahman, "A DWT, DCT and SVD Based Watermarking Technique to Protect the Image Piracy", *International Journal of Managing Public Sector Information and Communication Technologies*, Vol. 4, No. 2, pp 21-32, 2013.

[5] M. I. Khan, M. Rahman, I. H. Sarker, "Digital Watermarking for Image Authentication Based on Combined DCT, DWT and SVD Transformation", *Department of Computer Science and Engineering, Chittagong University of Engineering and Technology*, Chittagong-4349.

[6] N. Chaturvedi, Dr. S. J. Basha, "Comparison of Digital Image watermarking Methods DWT & DWT-DCT on the Basis of PSNR", *International Journal of Innovative Research in Science, Engineering and Technology*, Vol. 1, Issue 2, pp 147-153, 2012.

[7] S. Gaur, V. K. Srivastava, "A RDWT and Block-SVD based Dual Watermarking Scheme for Digital Images", International Journal of Advanced Computer Science and Applications, Vol. 8, No. 4, pp 2011-2019, 2017.

[8] S. Lagzian, M. Soryani, M. Fathy, "A New Robust Watermarking Scheme Based on RDWT-SVD", *International Journal of Intelligent Information Processing*, Vol. 2, No. 1, no1-33, 2011.

[9] S. A. Biad, T. Bouden, M. Nibouche, E. Elbasi, "A Bi-Dimensional Empirical Mode Decomposition Based Watermarking Scheme", *The International Arab Journal of Information Technology*, Vol. 12, No.1, pp 24-31, 2015.

[10] S. Gaur, V. K. Srivastava, "A Hybrid RDWT-DCT and SVD Based Digital Image Watermarking Scheme Using

Arnold Transform", *4th International Conference on Signal Processing and Integrated Networks* (SPIN), pp 399-404, 2017.

[11] F. Wu, J. Li, "The Text Image Watermarking Using Arnold Scrambling and DFT", *Computer Modeling & New Technologies*, 18(11) 477-481, 2014.

[12] I. M. G. Alwan, E. M. Jamel, "Digital Image Watermarking Using Arnold Scrambling and Berkeley Wavelet Transform", *Al-Khwarizmi Engineering Journal*, Vol. 12, No 2, pp 124-133, 2016.

[13] X. Zhou, J. Ma, W. Du, "SoW: A hybrid DWT-SVD based Secured Image Watermarking", *International Conference on Sensor Network Security Technology and Privacy Communication System* (SNS & PCS), pp 197-200, 2013.

[14] Y. Mao, G. Chen, S. Lian, "A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps", *International Journal of Bifurcation and Chaos*, Vol. 14, No. 10, pp 3613-3624, 2003.

[15] Y. Wu, J. Noonan, S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption", *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications* (JSAT), pp 31-38, 2011.