

A Hybrid Digital Watermarking Approach Using Wavelets and LSB

V. Ashok Kumar¹, C. Dharmaraj², Ch. Srinivasa Rao³

¹Department of Electronics and Communication Engineering, AITAM Tekkali, A.P., India

²Department of Electronics and Communication Engineering, GITAM University, A.P., India

³Department of Electronics and Communication Engineering, JNTUK Vizianagaram, A.P., India

Article Info

Article history:

Received Oct 25, 2016

Revised Jun 5, 2017

Accepted Sep 11, 2017

Keywords:

Alphabet pattern

DCT

DWT

Pell's cat map

Water mark

ABSTRACT

The present paper proposed a novel approach called Wavelet based Least Significant Bit Watermarking (WLSBWM) for high authentication, security and copyright protection. Alphabet Pattern (AP) approach is used to generate shuffled image in the first stage and Pell's Cat Map (PCM) is used for providing more security and strong protection from attacks. PCM applied on each 5×5 sub images. A wavelet concept is used to reduce the dimensionality of the image until it equals to the size of the watermark image. Discrete Cosign Transform is applied in the first stage; later N level Discrete Wavelet Transform (DWT) is applied for reducing up to the size of the watermark image. The water mark image is inserted in LH_n Sub band of the wavelet image using LSB concept. Simulation results show that the proposed technique produces better PSNR and similarity measure. The experimental results indicate that the present approach is more reliable and secure efficient. The robustness of the proposed scheme is evaluated against various image-processing attacks.

Copyright © 2017 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

V.Ashok Kumar,
Department of Electronics and Communication Engineering,
Aditya Institute Of Technology And Management,
Tekkali, Andhra Pradesh, India 532201.
Email: venkuash123@rediffmail.com

1. INTRODUCTION

In recent years, increase in use of the widespread internet has allowed the authors to distribute their content in digital form. Digital watermarking is the one of main richest research topic in the field of image processing and it has great attention for research community. Compare to audio and video, image watermarking is more dedicated and popular because of many practical applications such as Authentication of content and objects, Content identification and management, copy right protection and so on. The content includes audio, video, digital repositories, libraries or web publishing.

Watermarking is a process that inserts image/text called a watermark into another image and resultant image called watermarked image [1]. In order to be successful, the watermark should be unnoticeable and strong to deliberate or impulsive changes of the image. It should be robust against common image processing operations such as filtering, cropping, blurring, resizing etc; and common image compression techniques [2].

2. RELATED WORK

Basically, the watermarking can be classified into two major categories such as blind and non-blind watermarking approaches. In blind approach, original image is not required for extraction of watermark

image where as in non-blind approach, original image is required. The present approach uses the blind technique. So many approaches are available in this category such as Wavelet technology, block based approach, LSB based approach, and edge based techniques [3, 4, 5, 6]. In a preferred watermarking system, the watermark should be robust to content preserving attacks including geometric deformations and image processing operations [7, 8, 9, 10, 11]. Typically, the following features are considered for deriving an optimal image watermarking system: Perceptual Transparency, Robustness, Data Rate, Security, Verification and reliability. The present paper considers all these features in designing digital watermarking technique in efficiency and effective manner.

The authors [12, 13] embedded the watermark in those regions that are invariant to geometric attacks to avoid synchronization errors. The well-known patch work watermarking methods [14, 15] inserted a message by supposing that two sets randomly selected pixels are Gaussian distributed with zero mean. The patch method is sensitive to de-synchronization operations because the watermark is highly related to the position of those marked patches. Histogram based watermarking schemes are also exploited as due to reference for reversible watermarking and also for audio watermarking in the literature [16, 17, 18, 19]. In the literature watermarking methods based on Gaussian kernel filter and the histogram shape invariance are reported to enhance the robustness [20, 21].

Watermarking is applied in frequency domain by applying transforms like Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) or Discrete Wavelet transform (DWT) [21,22]. Recently, the researches for more secure watermarking techniques have revealed the fact that the content of the images could be used to improve the invisibility and the robustness of a watermarking scheme [24]. Sumalatha and Vijayakumar proposed content authentication schemes called Block based Content Checksum Watermarking method (BCCW) [25] and Local Edge Based Content Hash method [26] for efficient tamper detection. The novelties of these methods are hierarchical in nature and they show very high perceptual quality of embedded image. The BCCW method overcomes the drawbacks of Walton's [27] and Chang et.al. [28] Schemes, by embedding the checksum computed on the block B_i into the 2×2 sub block which has the maximum average compared to other sub blocks of the block.

FethiBelkhouche and UvaisQidwai [29] used one dimensional chaotic map. It has been shown that the method is used for binary image encryption with the possibility of using several keys such as the initial state, the external parameters and the number of iterations. It is also shown that the sensitivity to initial state plays an important role in chaotic encryption. Huang-PeiXiao, Guo-jiZang [30] proposed scheme using two chaotic systems based on the thought of higher secrecy of multi-system. One of the chaotic systems is used to generate a chaotic sequence. Podesser, Schmidt and Uhl [31] proposed a selective encryption algorithm for the uncompressed (raster) images, which is quite opposite from the first method proposed by Droogenbroeck and Benedett [32]. More recently, a reined hierarchical scheme of digital watermarking was obtained by Tassa [33] from subtler properties of Birkhoff polynomial interpolation. In [34], a method using Lagrange interpolation formula is proposed to estimate and recover the lost data. Shereenet.al [35] proposed a model called A New Profile Learning Model for sytem based learingtechnique which is used for authotication of the ownership.

Content authentication applications [36] where any tiny changes to the content are not satisfactory, the embedding distortion has to be rewarded perfectly. Many digital watermarking schemes proposed in the literature for still images and videos are mainly used in applications. In all these applications, apart from copyright protection, illegal copy protection, proof of ownership problems, identification of manipulations, there is a growing need for the authentication of the digital content.

3. MOTIVATION

The most essential properties of any digital watermarking techniques are robustness, security, imperceptibility, complexity, and verification. Robustness is the property where the watermark can be identified even after standard operations such as filtering, adding noise, scaling, lossy compression, color correction, or geometric modifications. Security is defined as the embedded watermark that cannot be removed away from trustworthy detection by embattled attacks. Imperceptibility means the watermark cannot be seen by the Human Visual System (HVS). Complexity is defined as the effort and time essential for watermark embedding and recovery. Finally, verification is a process in which there is a confidential key or public key function. The present paper considers all these properties in designing digital watermarking techniques.

According to the different properties of watermarking, it is applied in various fields like Ownership Assertion, Broadcast Monitoring, Copyright Protection, Fingerprinting, ID Card Security, Content labeling, Copy Control Fraud and Tamper Detection, Content Authentication, Integrity Verification, Usage control, Medical Safety and Content protection. Sometimes, several applications are combined in one watermarking

scheme. However, it is impossible to put all the applications in one scheme because different applications demand different properties of watermarking system to different extent. Depending on the watermarking applications and purpose, different properties or requirements of watermarking also arise and result in various design issues.

To overcome the disadvantages, the present paper proposes a method called Wavelet based Least Significant Bit Watermarking (WLSBWM) integrates the alphabet pattern approach for generating the shuffled image, wavelet concept to reduce the dimensionality, Pell's cap map for protection from attacks and LSB approach is used to insert the watermark image. The present approach is simple technique to insert the image and provides high protection from attacks. The novelty of the proposed approach is that double protection is provided for watermarked image so that it protect from attacks. The rest of the paper is organized as follows. Proposed WLSBWM described in section 4 and results are discussed in section 5. Attacks on the proposed method are discussed in section 6 and finally conclusions are given in section 7.

4. PROPOSED METHOD

In order to provide copyright protection for the identification of ownership, the present paper provides a hybrid technique to insert and extract the watermark in effective and efficient manner. The proposed WLSBWM method consists of 8 simple steps for inserting the watermark image and 8 steps for extracting the watermark image. The block diagram of the inserting water mark image is shown in Figure 1. The watermark insertion algorithm is described below.

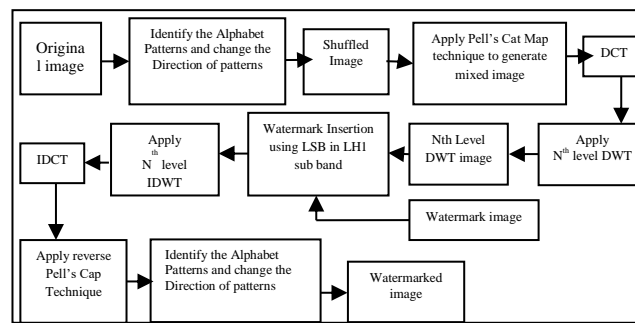


Figure 1. block diagram of the WLSBWM method

A. Watermark insertion algorithm

Step 1: Identify the Alphabet pattern: In insertion algorithm step one, for providing the security to protect from attacks the present approach converts the original image into shuffled image. The present paper uses the Alphabet patterns to generate the shuffled image. The generation of shuffled image has two sub tasks i.e. identify the Alphabet patterns on each 3×3 and change the direction of the pixel values in reverse direction. The present paper uses 'T' pattern, 'E' pattern, and 'U' patterns. The 3×3 window consists of 9 pixels. The pixel values are indicated by $P_1, P_2, P_3 \dots P_9$. The 3×3 window is shown in Figure 2.

P_1	P_2	P_3
P_4	P_5	P_6
P_7	P_8	P_9

Figure 2. 3×3 window

In a given window, if the pixels values of P_1, P_2, P_3, P_5 , and P_8 are same then treats the 3×3 window forms the 'T' pattern. If 'T' pattern existed in 3×3 window then change the direction of the pixel positions to form inverted T pattern. The figure 3 depicts the inverted 'T' pattern. If the pixel positions shown in figure 4 which are highlighted has same values then 3×3 window forms the E pattern and change the pixel position according to figure 4(b). In the same way if the 3×3 window form U pattern, change the positions of the pixels according to figure 5b. The same procedure is applied for remaining 3×3 windows in the entire image the resultant image is treated as shuffled image

P ₁	P ₂	P ₃	P ₇	P ₈	P ₉
P ₄	P ₅	P ₆	P ₄	P ₅	P ₆
P ₇	P ₈	P ₉	P ₁	P ₂	P ₃

Figure 3. (a) T Pattern (b) Inverted T pattern

P ₁	P ₂	P ₃	P ₃	P ₈	P ₁
P ₄	P ₅	P ₆	P ₆	P ₅	P ₄
P ₇	P ₈	P ₉	P ₉	P ₂	P ₇

Figure 4: (a) E Pattern (b) Inverted E pattern

P ₁	P ₂	P ₃	P ₇	P ₈	P ₉
P ₄	P ₅	P ₆	P ₄	P ₅	P ₆
P ₇	P ₈	P ₉	P ₁	P ₂	P ₃

Figure 5. (a) U Pattern (b) Inverted U pattern

Step 2: Pell's Cat Map (PCM):

For providing further security and authentication, Pell's Cat Map (PCM) [37] is employed on the 5×5 non overlapped blocks of shuffled image.

A discrete mapping using the matrix $P = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$ with determinant -1 is still area preserving but also orientation reversing. As it turns out the matrix P will generate numbers in the Pell's and half-companion Pell sequences, so P together with the modulo N operation will henceforth be denoted Pell'scatmap as shown in equation (1)

$$T_p : Z_N \times Z_N \Rightarrow Z_N \times Z_N \quad (1)$$

$$\text{Where } T_p \left(\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \right) = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\text{mod } N)$$

Step 3: Apply DCT on mixed image before inserting the watermark image.

DCT has been extensively used in image watermarking because of high energy compaction competence and respectable robustness. Generally, from spatial domain to frequency domain conversion Discrete Cosine Transform (DCT) is used [38, 39]. It also delivers suitable trade-off between Human Visual System (HVS) model and the image misrepresentation degree [40, 41]. DCT watermarking can be classified into two categories: Global DCT watermarking and Block-based DCT watermarking [42, 43]. The DCT computation is performed on the entire image in Global DCT [41], whereas the DCT computation is performed separately on each non-overlapping blocks[44, 45] to get low-frequency, mid-frequency and high-frequency sub-bands[43]. Generally, the watermark is inserted into a mid-frequency sub-band, which provides protection from watermarking attacks and it is well-matched with HVS model [46, 47]. Given an image f of size $M \times N$, the forward and inverse DCTs are shown in equations (2) and (3) [48]. The present paper utilizes and applies DCT on mixed image.

$$F(u, v) = c(u)c(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \cos \left[\frac{\Pi(2x+1)u}{2M} \right] \cos \left[\frac{\Pi(2y+1)v}{2N} \right] \quad (2)$$

$$f(x, y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} c(u)c(v) F(u, v) \cos \left[\frac{\Pi(2x+1)u}{2M} \right] \cos \left[\frac{\Pi(2y+1)v}{2N} \right] \quad (3)$$

Where $u=0 \dots M-1, v=0 \dots N-1$ and

$$c(u) = \begin{cases} \sqrt{\frac{1}{M}}, u=0 \\ \sqrt{\frac{2}{M}}, u=1 \dots M-1 \end{cases} \quad c(v) = \begin{cases} \sqrt{\frac{1}{N}}, v=0 \\ \sqrt{\frac{2}{N}}, v=1 \dots N-1 \end{cases}$$

Step 4: Apply N level DWT on DCT image:

In frequency domain, another reliable transformation technique is Discrete Wavelet Transform (DWT). DWT is a mathematical tool for disintegrating an image hierarchic [39]. It divides the image into four sub-bands which are lower resolution approximation image (LL), horizontal (HL), vertical (LH) and diagonal (HH) detail sub-bands [37]. This process of division can be repeated several times to compute multi-level wavelet decomposition. Based on HVS model, the LL sub-band is not suitable for the watermark embedding, because it contains important data about the image and causes image distortion. HH sub-band is not suitable because of less hearty against image processing operations such as lossy compression [45]. Thus, the suitable sub-bands for watermark embedding are the mid-frequency sub-bands LH and HL[46, 48]. Figure.6 illustrates decomposition of an image using 2D wavelet transform after 3 levels of decomposition.

LL3	HL3	HL2	HL1
LH3	HH3		
LH2		HH2	
LH1			HH1

Figure 6. Third level wavelet transform

Apply N^{th} level DWT on DCT image to insert the watermark, N level depends on the Size of the original image and water mark image. Suppose the size of the image 256×256 and the watermark image size is 64×64 the 2 level DWT is applied. If the size of the original image is 512×512 then 3 levels of the DWT applied on original image.

Step 5: Embedding the watermark:

Find the Size of the Watermark image and Converts the watermark image into a vector of zeros and ones. The condition for inserting the watermark is the size of the LH_n is equal to size of the watermark image. Where n is the n^{th} level DWT. The LSB of the each value in LH_n sub-band is replaced with the corresponding watermark image bit value. The new LH_n sub band is called the watermark sub band image

Step 6 Apply N^{th} inverse DWT: Apply nth level Inverse DWT on watermark sub-band image and IDCT is also applied.

Step 7: The reverse of step 3, inverse PCM is applied on the shuffled watermarked image.

Step 8: The reverse of step one, Identify the Alphabet patterns on each 3×3 of shuffled watermarked image and change the direction of the pixel values in reverse direction to obtain a shuffled image. The resultant image is called watermarked image.

B. Water mark extraction algorithm

The block diagram of the water mark extraction is shown in Figure 7. The proposed method Wavelet based LSB Watermark Extraction (WLSBWME) consists of 8 steps as illustrated below.

Step 1: In step one, Identify the Alphabet patterns on each 3×3 sub-window of the watermarked and change the direction of the pixel values in reverse direction to obtain a shuffled watermarked image.

Step 2: Apply Pell's Cat Map (PCM) on the each 5×5 sub-window of shuffled image.

Step 3: Convert the watermark image into a vector of zeros and ones and find the Size of the Watermark image

Step 4 & 5: Apply DCT on watermarked shuffled image and get watermarked shuffled DCT Image

Step 6: Apply N level DWT on DCT image to extract the watermark image.

Step 7: After N^{th} DWT is applied on image, stores the LH1 values into S.

Step 8: extract the LSB of the each values in S, store the values inTemp which is equal size of the S. The Temp is the watermark image.

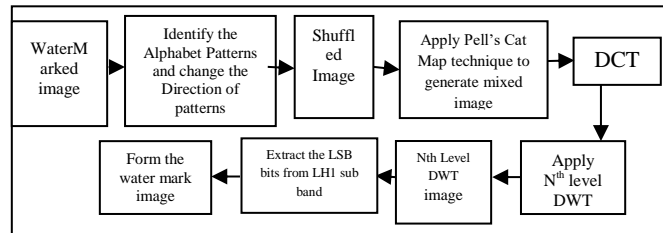


Figure 7: block diagram of the water mark extraction process

5. RESULTS AND DISCUSSION

The proposed WLSBWM method is experimented over 30 images of size 256×256. The images used in this approach are shown in figure 8. The present method is tested with two different watermark images. i.e. 'AITAM' and 'GITAM' logos of size 64×64 and shown in figure 9(a) and 9(b) respectively. The proposed method tested with Matlab software on i3 processor and 4GB RAM. The resultant watermarked images after inserting the watermark image logos of 'GITAM' and 'AITAM' are shown in Figure 10 and 11 respectively

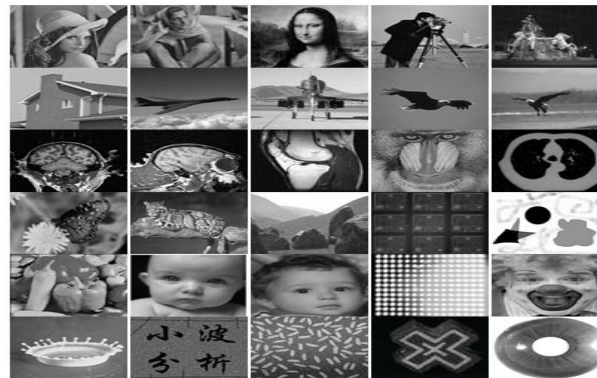


Figure 8: Images used in this experiment (i) Lena, (ii) Barbara, (iii) Monalisa, (iv) Cameraman, (v) Terraux, (vi) House, (vii) Airplane, (viii) Jetplane, (ix) Eagle-1, (x) Eagle-2, (xi) MRI-1, (xii) MRI-2, (xiii) MRI-3, (xiv) Mandrill, (xv) CT-1, (xvi) Butterfly, (xvii) Cheetah, (xviii) Landscape, (xix) Chips, (xx) Paint, (xxi) Peppers, (xxii) Baby-1, (xxiii) Baby-2, (xxiv) circles, (xxv) Joker, (xxvi) Milkdrop, (xxvii) Character, (xxviii) Seed, (xxix) Tile, (xxx) Iris.



Figure 9: watermark images (a) Logo of GITAM and (b) logo of AITAM



Figure 10. Watermarked images: a) Monalisa b) Eagle-1 c) Cameraman d) Baby-2 e) MRI-1 f) Landscape g) Jetplane h) House i) Joker k) Cheetah when insert the watermark logo of 'GITAM'

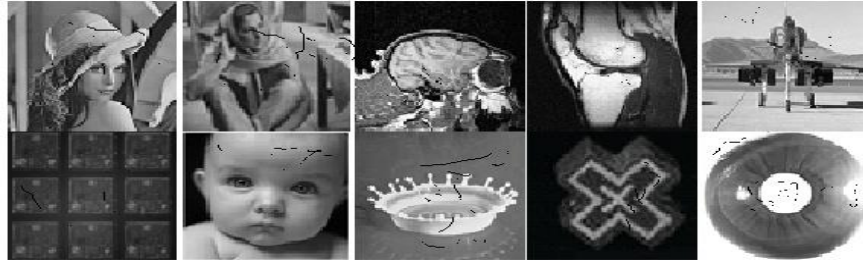


Figure 11. Watermarked images: a)Lena b)Barbara c)MRI-2 d)MRI-3 e)Jetpalne f)Chips g)Babu-1 h)Milkdropi i)Joker k)Cheetah when insert the watermark logo of 'AITAM'

To find the effectiveness of the proposed method, the present paper used two popular and effective criteria called Normalized Correlation Coefficient (NCC) and Peak Signal Noise Ratio (PSNR) for evaluating the performance of the proposed watermarking algorithm.

The quality of the watermark or the frangibility of the algorithm is assessed by the similarity measurement NCC between the referenced watermark W and the extracted watermark W^* as given in Equation 4.

$$NCC = \frac{\sum_{i=0}^{N-1} W(i)XW^*(i)}{\sum_{i=0}^{N-1} (W(i))^2} \quad (4)$$

Where, N is number of pixels, $w(i)$ and $w^*(i)$ are the original watermark and the extracted watermark. In the above equation $\rho = 1$ indicates perfect correlation, while an extremely low value reveals that the watermarks are dissimilar. If NCC value ranges from 0.65 to 1.0 then one can say that the image preserves high quality after inserting the watermark.

The present method also calculates, the difference between the original image and the watermarked image by Peak Signal Noise Ratio (PSNR). The bigger PSNR is, the smaller is the difference, and PSNR is defined through given Equation (5).

$$PSNR = 10 \log \left(\frac{255^2}{MSE} \right) \quad (5)$$

Where mean squared error (MSE) is evaluated using Equation (6)

$$MSE = \frac{\sum_{i=1}^M \sum_{j=1}^N (X_{ij} - X'_{ij})^2}{MN} \quad (6)$$

Where M and N are respectively the length and the width of the host image; X_{ij} denotes the gray level of the original image pixel; X'_{ij} denotes the gray level of the watermarked image pixel.

Table 1 and 2 shows the PSNR and NCC values for all the 30 images when two watermark images are used. From the Table 1 and 2, it is clearly evident that all the images shows high PSNR and NCC values which indicates high robustness and high quality of image after watermark insertion.

Table 1. PSNR and NCC values of the proposed method when insert the logo of 'GITAM'

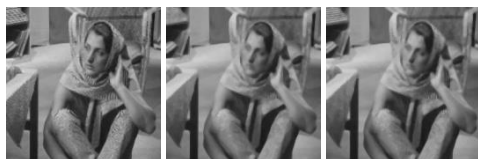
S.No	Image	PSNR	NCC
1	Lena	49.19	0.985
2	Barbara	51.66	1
3	Monalisa	54.19	0.995
4	Cameraman	50.61	0.997
5	Terraux	49.36	0.987
6	House	49.1	1
7	Airplane	49.85	0.985
8	Jetplane	52.02	0.993
9	Eagle-1	51.17	0.995
10	Eagle-2	50.63	0.955
11	MRI-1	50.23	0.965
12	MRI-2	51.21	0.975
13	MRI-3	51.8	0.965
14	Mandrill	49.62	0.985
15	CT-1	49.08	0.985
16	Butterfly	49.02	0.983
17	Cheetah	49.83	1
18	Landscape	50.57	0.959
19	Chips	51.31	0.975
20	Paint	48.55	0.993
21	Peppers	48.47	1
22	Baby-1	48.94	1
23	Baby-2	51.75	0.995
24	circles	49.37	0.987
25	Joker	49.83	0.975
26	Milkdrop	50.57	0.961
27	Character	49.85	0.983
28	Seeds	52.02	0.955
29	Tile	51.17	0.969
30	Iris	50.63	0.972

Table 2. PSNR and NCC values of the proposed method when insert the logo of 'AITAM'

S.No	Image	PSNR	NCC
1	Lena	49.74	0.975
2	Barbara	52.21	1
3	Monalisa	54.74	0.985
4	Cameraman	51.16	0.985
5	Terraux	49.91	0.983
6	House	49.65	1
7	Airplane	50.4	0.975
8	Jetplane	52.57	0.985
9	Eagle-1	51.72	0.986
10	Eagle-2	51.18	0.945
11	MRI-1	50.78	0.945
12	MRI-2	51.76	1
13	MRI-3	52.35	0.957
14	Mandrill	50.17	0.965
15	CT-1	49.63	0.979
16	Butterfly	49.57	0.975
17	Cheetah	50.38	1
18	Landscape	51.12	0.945
19	Chips	51.86	0.964
20	Paint	49.1	0.985
21	Peppers	49.02	0.992
22	Baby-1	49.49	1
23	Baby-2	52.3	0.98
24	circles	49.92	0.975
25	Joker	50.38	0.975
26	Milkdrop	51.12	0.965
27	Character	50.4	1
28	Seeds	52.57	0.965
29	Tile	51.72	0.955
30	Iris	51.18	0.967

6. PROPOSED WLSBWM METHOD WITH ATTACKS

To find the effectiveness of the proposed **WLSBWM** method, find the two parameters values when attacks on the image. Watermarking techniques are usually tested against various robustness criteria. The proposed watermarking technique is tested by using the different geometric attacks and transformations on Barbara, Monalisa, MR-1 and Eagle-1. The resultant watermarked 'Barbara' with different attacks like salt and pepper noise, rotation, median filter, cropping, Gaussian noise, compression, Grey level blurring, Motion blurring and Sharpening are shown in Figure 12 (a) to 12(i).



12(a) Attacked images when using 3×3, 5×5 and 7×7 masks in Median filter



12(b) Attacked images when 5%, 10%, 15% Cropping



12(c) Attacked images when Rotation (20, 40, 60)



12(d) Attacked images when 10%, 15%, 20% Salt and pepper noise added



12(e) Attacked images when 10%, 15%, 20% Gaussian noise added



12(f) Attacked images when 90%, 80%, 70% JPEG compression applied



12(g) Attacked images with 5%, 10%, 15% Gaussian blurring



12(h) Attacked images with 5%, 10%, 15% Motion blurring



12(i) Attacked images when 5%, 10%, 15% Sharpening attack

Figure 12(a-i). Attacked Watermarked Barbara images

The PSNR and NCC values, for the binary logo of 'GITAM' and 'AITAM' with different attacks on Barbara, Monalisa, MR-1 and eagle-1 images are listed out in Table 3 and 4.

Table 3: PSNR and NCC values with various attacks of the Proposed method when insert logo 'GITAM'

Type of Attack	Barbara		Monalisa		MR-1		Eagle-1	
	PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC
Median filter (3×3)	48.31	0.901	46.83	0.902	47.7	0.903	49.07	0.897
Median filter (5×5)	44.21	0.851	45.51	0.832	44.66	0.833	44.79	0.837
Median filter (7×7)	41.65	0.761	40.99	0.732	40.49	0.743	40.59	0.747
Cropping 5%	46.65	0.871	48.15	0.872	46.62	0.873	49.06	0.867
Cropping 10%	43.28	0.841	43.86	0.802	44.17	0.803	43.93	0.807
Cropping 15%	40.65	0.751	41.19	0.732	40.83	0.733	40.62	0.737
Rotate 2°	48.76	0.921	47.75	0.922	46.65	0.923	49.77	0.917
Rotate 4°	45.5	0.861	44.91	0.752	43.75	0.813	44.98	0.817
Rotate 6°	42.09	0.781	40.86	0.712	40.18	0.733	41.77	0.717
Salt and Pepper Noise 10%	48.43	0.941	48.82	0.902	49.44	0.903	47.94	0.897
Salt and Pepper Noise 15%	45.18	0.871	43.74	0.832	44.08	0.813	45.23	0.827
Salt and Pepper Noise 20%	39.95	0.791	41.31	0.742	38.99	0.743	44.08	0.747
Gaussian noise 10%	48.65	0.901	47.84	0.922	48.81	0.893	48.99	0.927
Gaussian noise 15%	44.45	0.851	44.93	0.872	45.09	0.813	44.43	0.807
Gaussian noise 20%	40.99	0.791	41.69	0.752	41.38	0.763	41.24	0.727
JPEG Compression 90%	49.87	0.931	48.88	0.902	47.93	0.923	49.33	0.887
JPEG Compression 80%	45.29	0.841	46.21	0.792	43.83	0.833	44.75	0.817
JPEG Compression 70%	41.09	0.751	39.85	0.722	40.76	0.763	39.72	0.747
Gaussian Blur 5%	47.62	0.921	48.96	0.902	48.99	0.903	47.34	0.897
Gaussian Blur 10%	44.31	0.841	42.75	0.832	44.36	0.843	42.79	0.807
Gaussian Blur 15%	39.22	0.751	40.17	0.732	40.24	0.773	40.43	0.717
Motion blurring 5%	47.31	0.921	47.95	0.872	47.95	0.883	47.96	0.877
Motion blurring 10%	42.83	0.801	43.87	0.822	44.07	0.793	44.24	0.787
Motion blurring 15%	39.1	0.741	40.14	0.712	39.99	0.743	40.71	0.717
Sharpening 5%	49.24	0.921	48.78	0.862	50.22	0.883	46.76	0.887
Sharpening 10%	45.18	0.831	44.19	0.832	44.81	0.833	43.16	0.807
Sharpening 15%	41.22	0.761	40.18	0.742	40.59	0.703	40.13	0.737
Average	44.48	0.841	44.46	0.815	44.32	0.821	44.59	0.813

Table 4: PSNR and NCC values with various attacks of the Proposed method when insert logo 'AITAM'

Type of Attack	Barbara		Monalisa		MR-1		Eagle-1	
	PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC
Median filter (3×3)	48.98	0.903	47.9	0.892	47.51	0.906	47.76	0.897
Median filter (5×5)	45.51	0.833	44.2	0.852	44.84	0.826	44.85	0.817
Median filter (7×7)	41.07	0.763	41.99	0.772	41.17	0.756	41.23	0.737
Cropping 5%	48.9	0.883	46.67	0.882	46.76	0.886	46.88	0.867
Cropping 10%	43.81	0.823	43.19	0.842	43.88	0.806	44.22	0.787
Cropping 15%	40.91	0.753	41.36	0.762	40.68	0.746	40.89	0.737
Rotate 2°	49.91	0.903	48.87	0.912	46.88	0.916	46.94	0.907
Rotate 4°	45.02	0.813	45.48	0.862	44.15	0.806	44.09	0.807
Rotate 6°	41.8	0.733	42.09	0.792	39.87	0.736	39.78	0.717
Salt and Pepper Noise 10%	47.87	0.903	47.91	0.922	49.08	0.906	48.89	0.887
Salt and Pepper Noise 15%	44.91	0.843	45.18	0.862	43.64	0.796	44.15	0.807
Salt and Pepper Noise 20%	43.81	0.773	39.76	0.812	38.82	0.746	38.99	0.737
Gaussian noise 10%	49.07	0.913	48.7	0.902	48.65	0.906	48.892	0.887
Gaussian noise 15%	43.72	0.803	43.91	0.862	44.56	0.826	45.15	0.797
Gaussian noise 20%	40.62	0.723	41.01	0.802	40.71	0.776	41.43	0.747
JPEG Compression 90%	48.79	0.903	49.78	0.922	48.08	0.926	47.87	0.917
JPEG Compression 80%	44.67	0.833	45.15	0.842	43.76	0.846	43.77	0.827
JPEG Compression 70%	40.36	0.763	40.9	0.762	40.71	0.776	41.4	0.767
Gaussian Blur 5%	47.52	0.913	47.68	0.912	48.97	0.906	49.08	0.897
Gaussian Blur 10%	42.87	0.823	44.28	0.842	43.87	0.836	44.33	0.837
Gaussian Blur 15%	40.08	0.733	38.83	0.762	39.82	0.776	39.68	0.777
Motion blurring 5%	47.8	0.893	47.29	0.912	47.98	0.896	47.86	0.877
Motion blurring 10%	43.74	0.803	43.14	0.802	43.75	0.806	44.18	0.797
Motion blurring 15%	41.07	0.733	38.91	0.742	39.86	0.746	39.73	0.737
Sharpening 5%	46.85	0.893	49.26	0.912	50.23	0.886	50.28	0.887
Sharpening 10%	42.72	0.803	44.69	0.832	44.76	0.836	44.75	0.827
Sharpening 15%	40.06	0.753	41.18	0.772	40.76	0.716	40.66	0.707
Average	44.53	0.823	44.42	0.842	44.21	0.826	44.36	0.814

The table 3 and 4 clearly indicate the robustness and quality of the image is not degraded for all attacks by the proposed method.

From the above results observe that the proposed method gives good results and got reasonable values of PSNR and NCC values when various attacks on watermark image. The proposed method is tested when two watermark images are inserted in 30 different images. From the above study, observe that the proposed method is most suitable for inserting the watermark image.

Comparison of the proposed method with other existing methods:

To evaluate the efficiency, the proposed method is compared with the existing watermarking approaches [46,47, 48]. The method proposed by Zhu Yuefeng et.al [46] inserts and extracts the water mark image using dual transformation and self-recovery approach. This approach analyzes inserting positions by using DC coefficient and inserts the water mark image into original image. Saravjit Kaur [47] proposed water marking technique based on DWT. The insertion and extraction of the watermark image in the grey scale images are accomplished by transform methods. Thirugnanam et.al. [48] Proposed a technique using DWT and Independent Component Analysis (ICA). The performance results of the proposed WLSBWM method and other existing methods are listed in table 5. Table 5 clearly indicates the WLSBWM method outperforms the other existing methods. The graphical representation of the performance of the WLSBWM method and other existing method is shown in Figure 13.

Table 5. Performance results of the proposed WLSBWM method with the existing methods in terms of PSNR

S.No	Test Images	Zhu Yuefeng Method	Saravjit Kaur Method	Thirugnanam. Method	Proposed WLSBWM
1	Lena	39.63	40.67	39.98	49.74
2	Mandrill	37.2	38.64	34.45	50.17
3	Peppers	36.54	42.12	36.56	49.02
4	House	37.89	40.19	34.95	49.65
5	Barbara	36.45	41.12	41.62	52.21
6	Milkdrop	37.64	40.61	39.14	51.12
7	Airplane	33.12	40.23	41.15	50.4
8	Cameraman	35.69	39.95	40.32	51.16

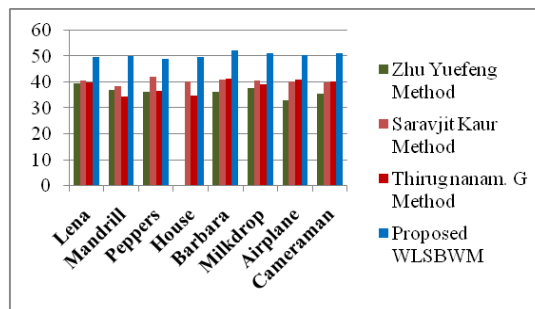


Figure 13. Graphical Representation of the proposed WLSBWM with the existing methods.

7. CONCLUSIONS

The present paper derived a hybrid scheme called WLSB for embedding the watermark. The proposed scheme uses three stages for embedding the watermark. In the first stage, shuffled image is generated by using alphabet patterns and PCM for protection from attacks. In the second stage, the DCT is applied and then N level DWT is applied until size of the LH1 sub band size matches with water mark image. Insert the watermark bits into LSB of the LH1 sub band values row by row and column by column. The proposed scheme guarantees high authentication. The present approach is simple and reliable and provides more security. The extraction process is also handy with simple steps. The experimental results on various images with various attacks show that the proposed technique provide good image quality and robustness when compared to other methods.

REFERENCES

- [1] Watermarking Technique for Protecting Digital Images", 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), Volume: 7, year 2010 pp. 226 – 233.
- [2] Saied AmirgholipourKasmani, AhmadrezaNaghsh-Nilchi, "A New Robust Digital ImageWatermarking Technique Based On Joint DWT-DCT Transformation", IEEE 3rd InternationalConference on Convergence and Hybrid Information Technology Vol. 2, year 2008, pages 539-544.
- [3] Sukanti B. Mardolkar, and NayanaShenvi "Joint Dwt-Dct Based Blind And Robust Digital Watermarking Approach For Copyright Protection", International Journal Of Pure And Applied Research In Engineering And Technology, Volume 4, issue:9 2016 pp: 218-226
- [4] A.F.ElGamal, N.A.Mosa and W.K.ElSaid, "Block-based Watermarking for Color Images using DCT and DWT", International Journal of Computer Applications, Volume 66– No.15, March 2013, pp: 33-40
- [5] GurpreetKaur, andKamaljit Kaur, "Implementing LSB on Image Watermarking Using Text and Image", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.
- [6] P. Ramesh Kumar and K.L.Sailaja, "Watermarking Algorithm Using Sobel Edge Detection", Int. J. Advanced Networking and Applications, Volume: 02, Issue: 05, Pages: 861-867, 2011.
- [7] Bhowmik.D, Abhayaratne.C (2009), "A frame work for evaluating wavelet based watermarking for scalable coded digital item adaptation attacks", in Proc. SPIE Wavelet Applications in Industrial Processing VI, Vol.7248,P.72480M
- [8] Lang Zhai (2011), "Researches on digital image watermarking algorithm in DWT domain with chaotic encryption", Inf. English Department, Jilin Bus & Technol. Coll., Changchun, China, Pages(s):3321-3324, August.
- [9] Mei Jiansheng, Li Sukang, Tan Xiaomei (2009), A Digital Watermarking Algorithm Based On DCT and DWT, Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, May 22-24, pp. 104-107.
- [10] DeepayanBhowmik, CharithAbhayaratne (2009), "A framework for evaluating wavelet based watermarking for scalable coded digital item adaptation attacks", Proc. SPIE 7248, Wavelet Applications in Industrial Processing VI, 72480M (January 27); doi:10.1117/12. 816307
- [11] RatnaBhargavi V, Ranjan K. Senapati, "Bright Lesion Detection in Color Fundus Images Based on Texture Features", Bulletin of Electrical Engineering and Informatics, March 2016 Vol. 5, No. 1, March 2016, pp. 92~100,
- [12] Lu. C. S, Sun. S. W, Hsu. C. Y, Chang. P. C (2006), "Media hash-dependent image watermarking resilient against both geometric attacks and estimation attacks based on false positive-oriented detection", IEEE Trans. Multimedia, vol. 8, no. 4, pp. 668–685, August.
- [13] Seo. J. S and Yoo.C. D (2006), "Image watermarking based on invariant regions of scale-space representation," in IEEE Trans. Signal Process., vol. 54, no. 4, pp. 1537–1549, April.
- [14] Yeo. I. K and Kim. H. J (2003), "Generalized patchwork algorithm for image watermarking", Multimedia System, vol. 9, no. 3, pp. 261–265.

- [15] Lin. C. H, Chan. D. Y, Su. H, Hsieh. W. S (2006), "Histogram-oriented watermarking algorithm: Colour image watermarking scheme robust against geometric attacks and signal processing", in Proc. IEE Vis. Image Signal Process., vol. 153, no. 4, August.
- [16] Lee. S, Suh. Y, and Ho. Y (2004), "Lossless data hiding based on histogram modification of difference images," in Proc. 2004 Pacific-Rim Conf. Multimedia, vol. 3, pp. 340–347.
- [17] Ni. Z, Shi. Y, Ansari. N, Su. W (2006), "Reversible data hiding", in IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–363, March.
- [18] Xiang. S, Huang. J (2007), "Histogram-based audio watermarking against time-scale modification and cropping attacks", IEEE Trans. Multimedia, vol. 9, no. 7, pp. 1357–11372, November.
- [19] Xiang. S, Huang. J, Yang. R (2006), "Time-scale invariant audio watermarking based on the statistical features in time domain", in Proc. 8th International Workshop Information Hiding, vol. LNCS-4437, pp. 93–108.
- [20] Coskun. B, Sankur. B, Memon. N (2006), "Spatio-temporal transform based video hashing," IEEE Trans. Multimedia, vol. 8, no. 6, pp. 1190–1208, December.
- [21] Xiang. S, Kim. H. J, Huang. J (2007), "Histogram-based image hashing robust against geometric deformations", in Proc. 9th ACM Multimedia Security Workshop, Sep., pp. 121–128.
- [22] Lang Zhai (2011), "Researches on digital image watermarking algorithm in DWT domain with chaotic encryption", Inf. English Department, Jilin Bus & Technol. Coll., Changchun, China, Pages(s):3321-3324, August.
- [23] DeepayanBhowmik, CharithAbhayaratne (2009), "A framework for evaluating wavelet based watermarking for scalable coded digital item adaptation attacks", Proc. SPIE 7248, Wavelet Applications in Industrial Processing VI, 72480M (January 27); doi:10.1117/12. 816307.
- [24] Qi. X, Qi. J (2007), "A robust content-based digital image watermarking scheme", Signal Processing, Elsevier, Vol. 87, Issue 6, Pp. 1264-1280.
- [25] Sumalatha L., et.al (2012), "A Simple Block Based Content Watermarking Scheme for Image Authentication and Tamper Detection", in International Journal of Soft Computing and Engineering (IJSCE), Vol. 2(4).
- [26] Sumalatha. L, Venkata Krishna. V, Vijaya Kumar. V (2012), "Local Content Based Image Authentication for Tamper Localization", in International Journal of Image, Graphics and Signal Proc., Vol.9, pp: 30-36.
- [27] Walton. S (1995), "Information authentication for a slippery new age", Dr. Dobbs J., Vol.20 (4), pp:18–26
- [28] Chang C.C., Hu Y.S (2006), "A watermarking-based image ownership and tampering authentication scheme", Pattern Recognition Letter, Vol.27 (5), pp: 39-446
- [29] FethiBelkhouche and UvaisQidwai (2003), "Binary image encoding using 1D chaotic maps", IEEE International Conference on Image Processing (ICIP'2003), volume I, pages 205–208.
- [30] GuoshengGu, Guoqiang Han (2006), "An Enhanced Chaos Based Image Encryption Algorithm", in IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06).
- [31] Podesser. M, Schmidt.H.P and Uhl. A (2002), "Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments", 5th Nordic Signal Processing Symposium, on board Hurtigruten, Norway, October 4-7
- [32] Pranab Kumar Dhar, Mohammad Ibrahim Khan, Jong Myon Kim (2010), "A New Audio Watermarking System using Discrete Fourier Transform for Copyright Protection", IJCSNS International Journal of Computer Science and Network Security, Vol. 10 Number 6, June.
- [33] Tassa. T (2004), "Hierarchical Threshold Secret Sharing", in Proceeding of the Theory of Cryptography Conference, MIT, Cambridge MA, USA, February 2004, LNCS 2951, Springer-Verlag, 473–490.
- [34] Ting. G.C.W (2006), "Ambiguity Attacks on the GanicEskicioglu Robust DWT-SVD Image Watermarking Scheme", proceedings of Information Security and Cryptology (ICISC 2005), Seoul, Korea, LNCS 3935, Springer Berlin/Heidelberg, Germany, pp. 378–389.
- [35] Shereen H. Ali, Ali I. El Desouky, Ahmed I. Saleh "A New Profile Learning Model for Recommendation System based on Machine Learning Technique", Indonesian Journal of Electrical Engineering and Informatics (IJEEL) Vol. 4, No. 1, March 2016, pp. 81~92
- [36] Tian. J (2003), "Reversible data embedding using a difference expansion", IEEE Transactions on Circuits and Systems for Video Technology, Vol.13, No.8, Pp.890-896.
- [37] Pell's cap Chen Y-L. et al. (2013), A maximum entropy-based chaotic time-variant fragile watermarking scheme for image tampering detection, Entropy, Vol 15 pp 3170-3185
- [38] Lin, S. D, Shie, S. C., and Guo, J. Y., "Improving the robustness of DCT-based image watermarking against JPEG compression", Journal of Computer Standards & Interfaces, vol.32, pp. 54-60, 2010.
- [39] Jose, S., Roy, R. C., and Shashidharan, S., "Robust Image Watermarking based on DCT-DWT-SVD Method", International Journal of Computer Applications, vol.58, no.21, pp. 0975-8887, November 2012.
- [40] Xijin, W., Linxiu, F., "The Application Research of MD5 Encryption Algorithm in DCT Digital Watermarking", International conference on Solid State Devices and Materials Science, Journal of Physics Procedia, vol.25, pp.1264-1269, 2012.
- [41] Tao, B., Dickinson, B., "ADAPTIVE WATERMARKING IN THE DCT DOMAIN", IEEE International Conference on Acoustics, Speech, and Signal Processing, pp. 21-24, 1997.
- [42] Potdar, V. M., Han, S., and Chang, E., "A Survey of Digital Image Watermarking Techniques", 3rd IEEE International Conference on Industrial Informatics (INDIN), pp. 709-716, 2005.

- [43] Eswaraiiah, R., Edara, S. A., and Reddy, E. S., "Color Image watermarking Scheme using DWT and DCT Coefficients of R, G and B Color Components", International Journal of Computer Applications, vol.50, no.8, pp. 0975-8887, July 2012.35
- [44] Kashyap, N., SINHA, G. R., "Image Watermarking Using 3-Level Discrete Wavelet Transform", I.J.Modern Education and Computer Science, vol.3, pp. 50-56, 2012.
- [45] Pardhan and rath, " Digital Watermarking technique using DWT and Cross Choas", Journal of processing technology, vol:6, pp:897-904, 2010
- [46] Zhu Yuefeng and Lin Li "Digital Image Watermarking Algorithms Based On Dual Transform Domain And Self-Recovery", International Journal On Smart Sensing And Intelligent Systems Vol. 8, No. 1, March 2015.
- [47] Saravjit Kaur and Research Scholar, "A Digital Image Watermarking Technique Based on DWT", International Journal of Computer &IT, {Pages1-8, 2015.
- [48] Thirugnanam.G, Arulselvi.S, "Robust Digital Image Watermarking Scheme Based on DWT and ICA," Global Journal of Computer Science and Technology, Vol.10, 2010.

BIOGRAPHIES OF AUTHORS



Mr.V.Ashok Kumar is currently working as Associate Professor of ECE Department, Aditya Institute of Technology and Management, Tekkali, A.P., India. He received M.Tech from College of Engineering JNTUK, Kakinada. He obtained B.E. from Hindustan College of Engineering, Madras University, Chennai, Tamilnadu. Currently pursuing Ph.D in GITAM Institute of Technology GITAM UniversityVisakhapatnam, AP, India. He Published research papers in National Journals and Conference as well. Areas of interests include Microprocessors and Image processing.



Dr.DharmaRaj.C. is currently working as Professor of ECE Department and Vice Principal, GITAM Institute of Technology GITAM UniversityVisakhapatnam, AP, India. He obtained his Ph.D from GITAM Institute of Technology GITAM UniversityVisakhapatnam, AP, India. He received M.E. degree from the Osmania University, Hyderabad, Telangana. Areas of interests includes Electronic Devices and Circuits, Satellite Communication, And Microwave Engineering. He Published research papers in National and International Journals and Conferences as well.



Dr.Ch.Srinivasa Rao is presently working as Professor of ECE Department, JNTU College of Engineering Vizianagaram, AP, India. He obtained his Ph.D from University College of Engineering, JNTUK, Kakinada, A.P, India. He received M.Tech. degree from the same Univeristy. Areas of interests includes Signal and Image Processing. He Published research papers in National and International Journals and Conferences as well.