

# Attestation Performance on Digital Watermarking

B.Priyanka, D.Pramodh Krishna, and E.Purushottam

Student of Computer science Engineering, Sri Vidyanikethan engineering college, Tirupati, India  
 Faculty of Computer science Engineering, Sri Vidyanikethan engineering college, Tirupati, India  
 Student of Computer science Engineering, Sri Vidyanikethan engineering college, Tirupati, India

## Summary

In this study, we propose a digital watermarking scheme, which performs operations like embedding, attack and detection of watermarks. Watermarks are embedded for authentication of images. In this paper, both visible and invisible watermarks are proposed. Invisible watermark is performed by LSB (least significant bit) and visible watermark is performed by DCT (Discrete cosine transform) which results a watermarked image. Later, we add noise to the watermark image which in turn means an attack on the image. JPEG compression is also done on the image as a form of attack. Finally, we de-noise the image and extract the watermark.

### Keywords:

*digital watermark, Least significant bit, Discrete cosine transform, JPEG compression, watermarked image, authentication, attack, de-noise, embed watermark, detect watermark, extract watermark.*

## 1. Introduction

Internet is a platform for the transformation of tons of images and data in digital media. The data that is distributed can be duplicated, morphed. Among many authentication methods watermark is one such to authenticate the data that is transferred. Many researches are carrying out on this particular field.

A watermark is a form of text or image that is embedded in to the paper for its evidence of authenticity. The extension of this concept is Digital watermarking. Watermarks are of two kinds: visible and invisible. This paper, implement both visible and invisible watermarks in an image. Watermark must be robust to various kinds of attacks. The invisible watermarking technique is implemented by least significant bit method. Here an attack is also shown by adding some noise to the watermark image i.e by compressing and decompressing using JPEG compression technique. Later, the noise is removed. Information hiding has become a serious concern in digital world especially in when people transfer secret message. Even though, there are encryption and decryption techniques as traditional ones but they are not risk handlers to the extent. The process of information hiding is done by three methods

1. **cryptography**: It is the process of sending a secret in the form of text message. To know the message the authorized person must decipher it.

2. **steganography**: It is the process of hiding or embedding a text or image inside the image, a part from sender and receiver one is aware of the secret. The attacker can even think of the existence of secret.

3. **watermarking**: It is related to steganography but, in watermarking technique the information that is hidden is usually related to the cover object. It is used for content authentication and copyright protection.

During the date back 13<sup>th</sup> century watermarks are used to indicate the paper brand and then by the end of 18<sup>th</sup> century watermarks began to use as anti-counterfeiting measures on money. Finally, in 1995 digital watermarking era has begun and many researches are carried out on digital watermarking which led to the huge discovery of algorithms and techniques.

Digital watermarking is defined as the digital signal that is embedded in audio, video or image with some information related to those and which cannot be eliminated easily.

The process to embed a watermark is done in three steps:

1. **embedding watermark**: In this algorithm it accepts the data to be embedded and produces watermark signal.

2. **attack on image**: The watermark signal is transmitted and during transformation the attacker may or may not modify the image. If there is a modification then it is said to be an attack.

3. **detection of watermark**: This algorithm is applied when the attacked signal to extract watermark from it. If the signal undergoes any modification then the information is also carried in the copy. If suppose, the signal doesn't undergo any modification the watermark is present and it can be extracted.

The following is the block diagram for the watermarking technique. We first embed the watermark in to the original or cover image and make it a watermarked image and then after transformation we extract the watermark and check whether it has been undergone any sort of manipulations or attacks. Finally, we extract the watermark from the image to prove its authenticity.

To avoid illegal access to the watermark a secret key as shown in the figure is used during the embedding process and extraction process of watermark.

Watermarking techniques are used for copyright protection, broadcast monitoring, authentication, tamper detection and digital finger printing, content protection, content labeling.

## 2. Review on watermarking

Watermarking techniques are classified as two types:

1. **visible watermarking**: These watermarks are visible in the form of text message or any logo. By these we identify the ownership of the image.

$$V_w = (1-\gamma)V + \gamma * W$$

$V_w$  = Watermarked Image

$\alpha$  = constant;

$$0 \leq \gamma \leq 1, IV$$

$\gamma=0$  No watermark,

if  $\gamma=1$  watermark present

$V$  =original image ; $W$  =watermark

2. **Invisible watermark**: These watermarks are invisible and cannot be perceived by human eye. It is used to protect image form being copied in turn it provides authentication to the image. Invisible watermarks are of 3 kinds:

**Robust**: As the names mentioned it is strong and overcomes several processing attacks. For example: filtering, compression

**Fragile**: It is distorted under slight changes. **Semi fragile**: It breaks under the changes performed by the user i.e exceeding specific threshold.

## 3. Embedding techniques in watermarking

A watermark can be embedded in three ways using Spread spectrum it is obtained by additive modification and it is robust which has low information capacity due to host interference. Secondly, quantization it is done by quantizing. Compared to spread spectrum it is less robust which can carry large data since it is having a little interference from host signal. Third embedding method amplitude modification, it is done in spatial domain which is similar to spread spectrum.

Embedding a watermark in to an image involves many techniques like spatial domain and frequency domain.

**Spatial domain watermarking** modifies the pixels of selected subsets of an image, which even includes the flipping of lower order bit in each pixel. This technique is not applicable to filtering.

**LSB (Least Significant Bit Coding)**: It is one of the earliest methods which can be applied to any form of watermarking. In this the LSB of the carrier signal is

substituted in the watermark. These are embedded in a sequence manner which acts as a key. So, while retrieve it back the same sequence order must be followed. During encoding of watermark it first selects a subsets of pixels on which the watermark is embedded. It embeds the information on the LSBs of the pixels. As it is a simple coding technique so the robust of watermark is very low. So, the watermark retrieved here is noise component.

**Predictive Coding** : it is proposed by Matsui and Tanaka [8] for gray scale images. In this method it exploits the correlation between adjacent pixels. A set of pixels are chosen to embed watermark and through the difference between the adjacency of the pixels the alternate pixels are replaced. It can improved by adding constants to all differences. By this a cipher key is created. It enables the retrieval of the embedded watermark. This coding technique gives much more robustness compared to the LSB coding technique

**Correlation-Based**: In this a pseudo random noise with a pattern is added to an image.

$$F_w(y, z) = F(y, z) + l * W(y, z) \text{ where,}$$

$F_w(y, z)$  = Watermarked image.

$F(x, y)$  = Original image

$l$  = gain factor

**Patchwork Technique**: In this patch watermarking technique, an image is divided in to two subsets and an operation is chosen and applied to these two subsets in an opposite direction. For example: If  $x[i]$  is the value of the sample at  $I$  in subset 'A' which is increased and  $y^{i+}$  is the value of the sample in the subset 'B' whose value is decreased, then the result in difference between the two subsets is

$$\sum(x[i]-y[i]) = 2M \text{ for watermarked images} \\ = 0 \text{ otherwise}$$

Where  $1 \leq M \leq \infty$

**Frequency domain watermarking** is based on discrete cosine transform technique(DCT).

**Discrete cosine transform technique**: It converts a sequence of data points in the spatial domain to sum of sine and cosine waveforms which are with different amplitudes in frequency domain. It transforms in a linear fashion which maps n-dimensional vector to n-coefficients. This linear combination of basis vectors weighted to n coefficients results in the original vector. These basis vectors are sinusoidal which can be represented by sinus shaped waves. The popular member of this class is Discrete Fourier Transformation(DFT).In DCT we use real numbers where as in DFT we use complex numbers. This can be considered as the difference between DCT and DFT. There are one-dimensional and two-dimensional DCTs

**One-dimensional DCT**:

The following is the formula for DCT in one dimensional form

$$F(u) = C(u) \sum f(x) \cos[\pi(2x+1)u/2N]$$

Where  $u=0,1,\dots,N-1$

$C(u)=\text{SQRT}(1/N)$  when  $u=0$

$C(u)=\text{SQRT}(2/N)$  when  $u \neq 0$

Two-dimensional DCT:

The following is the formula for DCT in one dimensional form

$$F(u,v)=C(u)C(v)\sum\sum(x,y)\cos[\pi(2x+1)u/2N]\cos[\pi(2y+1)y/2N]$$

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

$C(u),C(v)=\text{SQRT}[1/N]$  when  $u, v=0$   $C(u),C(v)=\text{SQRT}[2/N]$  when  $u,v \neq 0$

The following are the examples of DCT(discrete cosine transform).

75	76	75	75	69	66	77	71
73	74	73	74	63	64	68	69
69	68	71	72	67	58	48	41
59	55	56	52	47	40	24	9
51	50	45	41	33	22	7	-5
43	37	32	24	15	5	-6	-25
29	21	9	-2	-10	-21	-44	-69
9	-4	-17	-35	-52	-61	-57	-35

Example for 8X8 DCT

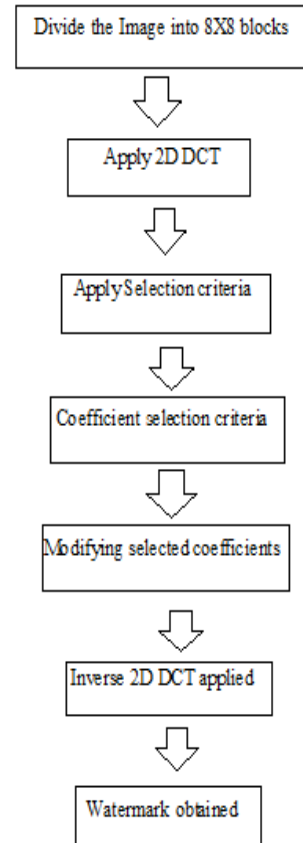
After Discrete Cosine Transform the following values are obtained.

251	118	-13	6	-2	6	-1	0
279	-68	-8	-7	-1	4	-4	-1
-51	-14	34	-14	5	0	-1	0
27	5	-10	8	-7	4	-5	1
-22	-7	14	-9	4	-2	1	1
-3	15	-18	15	-6	2	-1	2
7	-9	6	-6	4	0	0	2
3	7	-9	3	0	-2	-1	0

After 2D-DCT for 8X8 block

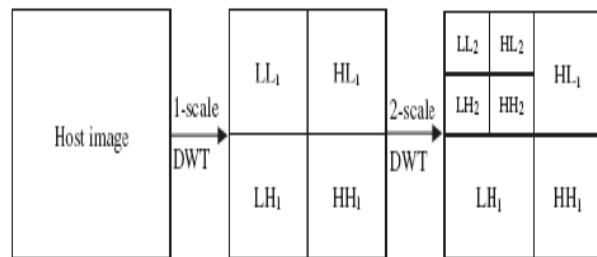
The following are the Steps explaining the example:

- 1.Divide the image in to 8x8 non-overlapping blocks.
- 2.Apply forward DCT to each block.
- 3.Apply selection criteria, followed by coefficient selection criteria.
- 4.Watermark is embedded by modifying the coefficients that are selected.
- 5.Finally, the watermarked image is obtained by applying Inverse DCT.



Block diagram for DCT

*Wavelet transform watermarking* In this the image is divided in to four side bands. The Fourier transform is an analysis of global frequency content in the signal. This can be done by using the Short Time Fourier Transform. The wavelet transform technique divides the image into four sidebands a low resolution approximation of the tile component and the component horizontal, vertical and diagonal Frequency characteristics.



Wavelet based transforms

*Simple watermarking* as the name represents it is simple. It inserts a logo or text message in the image to protect

from ownership authentication. The following is the image representing simple watermark.



Simple watermark image

### 4. Proposed method

In our proposed method firstly we implement two forms of watermarking techniques. One is visible watermarking and the other is invisible watermarking. Secondly, we add noises to the images and also perform compressing and decompressing techniques in the form of attacks. Thirdly, we remove the noises and compared watermark image with the original image.

#### I. Invisible watermark using LSB

- 1.An image A is selected form set of standard images and let it be the base image on which a watermark is embedded.
- 2.An image B is selected from set of standard images which is a watermark image that is added to the base image.
- 3.The MSB(Most Significant Bit) of watermark image B is read and written on the LSB(Least Significant Bit) of image A.
- 4.Thus, image A is said to be watermarked with image B results in image C.
- 5.So, the result image C therefore will contain the image A LSBs replaced by MSBs of image B.
- 6.This LSB technique is a form of spatial domain technique.

**Algorithm:**

- Step 1:** select a standard image to be used as a base image I.
- Step 2:** select a standard image to be used as a watermark image W
- Step 3:** read the images and display them.

**Step 4:** change the size of the images to double, so that they store the results of operations that are performed in them.

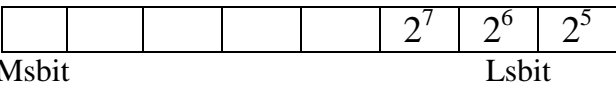
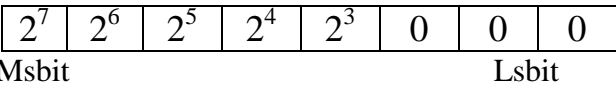
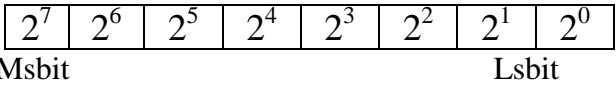
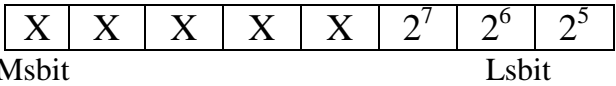
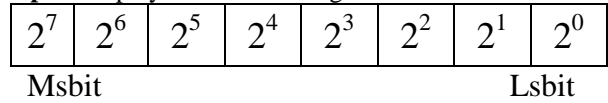
**Step 5:** Assign the no. of bits of the watermark image that is replaced by the base image.

**Step 6:** Shift the watermark image 8 bits right

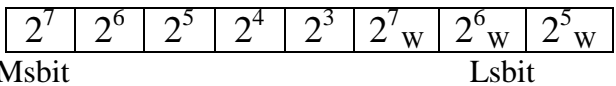
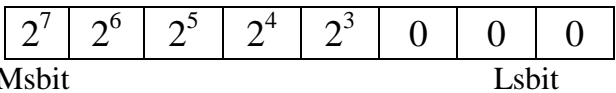
**Step 7:** least significant bits of the base signal is made zero.

**Step 8:** add message image and cover image

**Step 9:** Display watermark image.



+



#### II. Visible watermarking

- 1.An image A is selected form set of standard images and let it be the base image on which a watermark is embedded.
- 2.An image B is selected from set of standard images which is a watermark image that is added to the base image.
3. Concatenate both the images A and B to get watermark image E.
4. The result image E will now contain base image A and watermark image B.
5. It is a visible watermark technique.

**Algorithm:**

- Step 1:** select a standard image to be used as a base image I

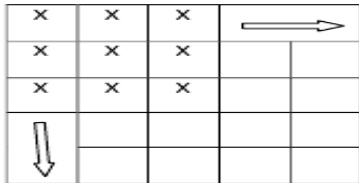
**Step 2:** select a standard image to be used as a watermark image W

**Step 3:** read the images and display them.

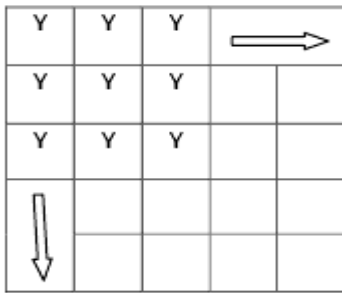
**Step 4:** change the size of the images to double, so that they store the results of operations that are performed in them.

**Step 5:** concatenate the images

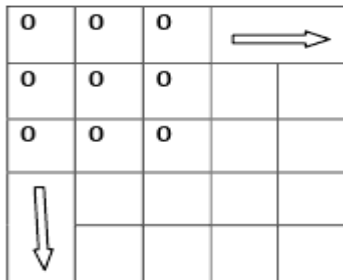
**Step 6:** display the watermark image.



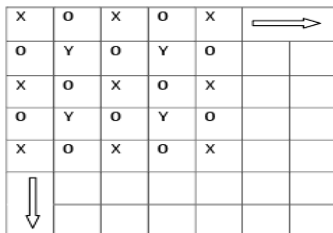
(i)



(ii)



(iii)



(iv)

**III. Adding noise and compressing the visible watermark image**

1. Noise is added to the concatenate image E

2. The noise is in the order of random matrix [512x512].

3. The resultant image is noisy image F.

4. Once the noise is added to the image, the program waits for the JPEG compression

5. Once it done with the compression, the program is informed by pressing enter key and it proceed by removing the noise.

6. JPEG Compression is done by running the .exe file [19]

7. The watermarked image added with noise F. The size of the original image is 257KB, after JPEG compression the size of the image is 92.2 KB

**Algorithm:**

**Step 1:** Read the visible image and initialize the noise as a random matrix.

**Step 2:** add noise to the image

**Step 3:** change the size of the image to double, so that they store the results of operations that are performed in them.

**Step 4:** display the image with noise added to it.

**Step 5:** Save watermarked image with the noise added to it is compressed using JPEG compressing technique.

**IV. Denoising**

1. JPEG compressed image is denoised now.

2. Run the program by reading the JPEG compression noise and remove the noise from it.

3. The result image is G

**V. Seperation of watermark**

1. Finally, the base image A and the watermark image B are separated from the recovered concatenated watermarked image G

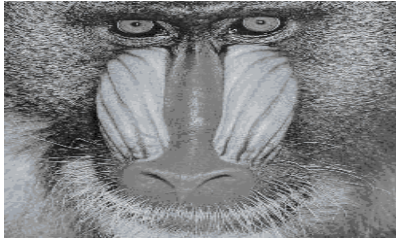
2. The images are in JPEG format compared to the original images. Therefore their sizes are less.

**5. Experimental results**

The tool that is used for the execution of this algorithm was in Matlab. Our aim is to replace the LSB of the base image with the MSB of the watermark. The images are read by the user. The user enters the name of the images, both the base and the watermark along with their extension i.e format of the image that is saved. Both these images will be read and stored by the tool i.e Matlab. The tool displays these images to the user with respective titles. Then the image size is doubled by using program. This is done by the tool to provide double data-type space for the images. The reason for doing so, is to provide decimal storage for the subsequent additional operations. Next, assign the number of most significant bits of the watermark which will be used to overwrite on the least significant bit spaces of the base signal. The watermark signal bits are shifted to the right by the specified bits.



Base image A



Watermark image B



Invisible watermarked image



Visible watermarked image

For the concatenation of two images. The base image and the watermark image is read. A zero matrix of 512X512 is defined. By placing the indexes of the base image in

alternate indexes of the zero matrixes the base image is written in the zero matrixes. Similarly, the watermark is placed in the remaining spaces. We defined the zero matrixes as 512X512, since the base and watermark images are 256X256. Later concatenated image is then displayed and stored as visible watermarked image. The following are the experimental results of the concatenated image.

The following are the experimental results shown performed in matlab.



Base image A



Watermark image B



Concatenated image E

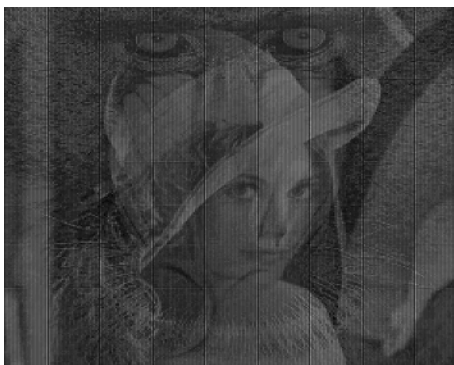
Later, the concatenated image is added noise. This is done by a program with a random matrix noisy of 512X512 dimension. This matrix is used as noise in the coming steps. The resultant watermarked is added with noise and



it is displayed. The following are the images of added noises and JPEG compression.



Concatenated watermarking with Noise added to it E



JPEG compressed watermarking image with noise size 98.2KB

After adding noise to the watermarked image, the program waits for the user to trigger it to continue executing the remaining part of the program i.e Once the compression is done, the user inform the program to continue execution. Now reads the JPEG image which was obtained from the JPEG decompression. Thus the resultant image noise and it is read. Next the noise is removed by subtracting the noise matrix from noise image and the recovered image is stored i.e Recovered watermarked image.

The tool used for the execution of this algorithm is Matlab. Finally, the images are separated from the concatenated recovered watermarked image. Thus, the original base and watermark images are recovered.



Watermarked Image, after compression and noise removal



Recovered base image of size 19KB



Recovered watermark image of size 20.2 KB

The following are the results obtained

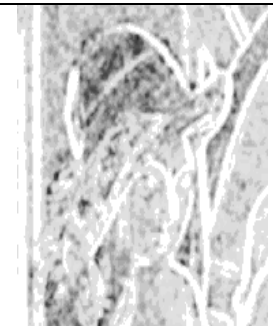
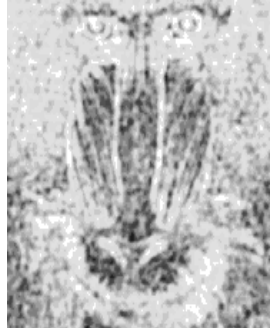
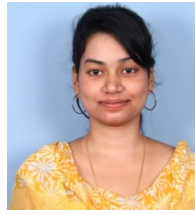
Image	Format	MAPS
Initial Lena image Size 65KB	Bitmap	
Recovered Lena Size 19KB	JPEG	

Image	Format	MAPS
Initial Baboon image Size 65KB	Bitmap	
Recovered Baboon image Size 20.2KB	JPEG	

## 6. Conclusion

Using Matlab, two forms of watermarking techniques have been implemented. One is invisible and the other being visible. Noise is added to the images in the form of attack. The images are compressed and decompressed which is another form of attack. The noise is later removed and the base and watermark images are separated from the watermarked image. Finally, the results are shown in table.



**B.Priyanka** received the B.E. in computer science engineering from Mahatma Gandhi institute of technology in 2011 affiliated by JNTU-H. Presently, she is pursuing her M.Tech[computer science] in Sri vidyaniketan engineering college, A.Rangampet, Tirupati, India. Her research interest includes Image processing, visual cryptography, steganography.



**D.Pramodh Krishna** received the B.E. and M.E. degrees, from Jawaharlal Nehru technological Univ. Hyderabad in 2003. Presently, he is working as an faculty(computer science Dept.) in Sri vidyaniketan engineering college, Tirupati, India. He published many papers in data mining. His research interest includes Data mining, computer networks, Image processing.



**E.Purushottam** received the MSc.(Computers) from S.V University in 2011. Pursuing M.Tech (Computer Network and Information Security) from JNTUA Univ. His research interest includes Cloud computing, Networks, Image Processing, Cryptography, Data Mining.