Image Watermarking Using LSB Technique

Preeti Gaur [1], Neeraj Manglani [2]

Research Scholar [1], Asst. Professor [2]

Jagannath University, Jaipur

gaurpreeti24@gmail.com[1], neeraj.maglani@Jagannathuniversity.org[2]

Abstract- Along with the increasing availability of multimedia applications the growth of the Internet has spawned a number of copyright issues. Digital watermarking is one of the areas that this growth has fueled. It is the common technique of embedding a splash of information in the unique file, such that a changed file is obtained. The splash of information, thus included, serves one of different uses, such as sensing tampering, reassuring integrity or identifying piracy. The Watermarking approaches are diverse and can be broadly classified based on their visibility, robustness, or fragility. Their uses are also adaptable, as they can be applied to images, text, video or audio. In this paper, we have shown N – significant bit watermarking and the results showing the best possible watermarking. In this paper the implementation of watermarking is done by using MATLAB software. MATLAB is a superior dialect for specialized registering. It contains features of visualization, processing, and programming in a user friendly environment where issues and arrangements are communicated in the recognizable numerical documentation

Keywords: Watermarking, Encryption, Decryption, MATLAB, PSNR

1. INTRODUCTION

In open networks, to securely transmit data Encryption and Decryption is used. To protect confidential image data from unauthorized access as each type of data has its own features, different techniques should be used. The principle goal of designing any encryption and decryption algorithm is to hide the original message and send the non readable text message to the receiver so that secret message communication can take place over the web. An algorithm strength depends on the difficulty of cracking the original message. Data encryption is widely used to ensure security however; most of the available encryption algorithm is used for text data.

Encryption is the process to convert original image data in to some other anonymous structure using a key which is not identified by anyone. Decryption defines the recovery of original data from the encrypted thing.

1.1 Goals of Encryption/Decryption

Confidentiality: In the computer the Information is transmitted should be accessed only by the authorized party.

Authentication: In this the identity of the sender is to be checked by the system from the information received by any system whether the information is arriving from an authorized person or a false identity.

Integrity: In this only the authorized party is allowed to modify the transmitted information. No one else in between the sender and receiver are allowed to alter the given message.

Non Repudiation: It ensures that neither the sender, nor the receiver of message can deny the transmission of messages.

Access Control: In this only the authorized parties are permit to access the given information.

1.2 WATERMARKING [3]

1.2.1 Watermark

A watermark is a visible embedded overlay on a digital photo consisting of text, a logo, or a copyright notice. The purpose of a watermark is to identify the work and discourage its unauthorized use.

1.2.2 Digital watermark

A digital watermark added to a photo, is more or less visible information in the form of a text or some other photo/image that has been added to the original photo. The added information can be more or less transparent to make it either easy or hard to notice the watermark.

1.2.3 Digital Watermarking

Digital Watermarking technique is used to hide a small amount of digital data in a digital signal in such a way that it can't be detected by viewer. A digital watermark is of two types-

1. Visible Digital Watermarking
2. Invisible Digital Watermarking

A **visible watermark** is a visible semi-transparent text or image overlaid on the original image. It allows the original image to be viewed, but it still provides copyright protection by marking the image as its owner's property. *Visible* watermarks are more robust against image transformation especially if we use a semi-transparent watermark placed over whole image. Thus they are preferable for strong copyright protection of intellectual property that's in digital format.

An **invisible watermark** is an embedded image which cannot be perceived with human's eyes. Only electronic devices or specialized software can extract the hidden information to identify the copyright owner. Invisible watermarks are used to mark a specialized digital content like text, images or even audio content to prove its authenticity.

Typical applications of digital watermarking can include broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, device control legacy enhancement and content description.

1.3 Digital watermarking life-cycle phases

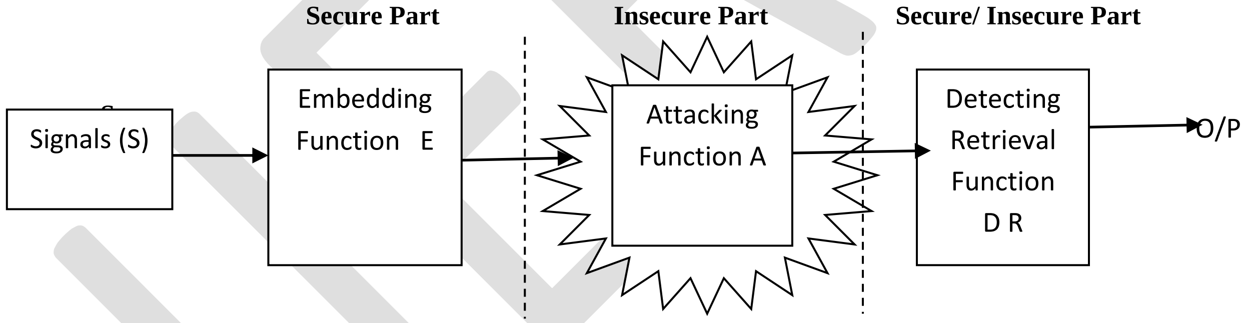


Figure 1 Digital Watermarking life cycle

Digital watermark life-cycle phases include embedding-, attacking, and detection retrieval functions. In a signal the embedded information is called a digital watermark. Digital watermark can be defined as the difference between the cover signal and the watermarked signal. The signal where the watermark is to be embedded is called the *host* signal. We can divide a watermarking system into three distinct steps **embedding**, **attack**, and **detection**.

In **embedding step**, the data and the host to be entrenched are accepted by the algorithm, and it produces a watermarked signal.

After this the watermarked digital signal is stored or transmitted, mostly transmitted to another person. If modification is done by this person then, it is known as an **attack**. Whilst the alteration may not be malicious. In attack, the third parties may try to eliminate the digital watermark through alteration. Examples of different possible modifications are, cropping an image or video or intentionally adding noise, lousy compression of the data in which resolution is diminished.

Detection (extraction) is an algorithm which is applied to the attacked signal to attempt to take out the watermark from it. If the signal was original during transmission, then the watermark still is present and it may be extracted.

In **robust digital watermarking** applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong.

In **fragile digital watermarking**, if any change is made to the signal then the extraction algorithm should be fail.
In general any watermarking algorithm consist of three parts –

- Watermark
- The encoder
- The decoder

1.4 Types of Watermarking

Watermarking techniques can be divided into four categories according to the type of document to be watermarked:

- Text Watermarking
- Image Watermarking
- Audio Watermarking
- Video Watermarking

In other way, the digital watermarks can be divided into three different types as follows:

- Visible watermark
- Invisible-Robust watermark
- Invisible-Fragile watermark

In Visible watermarking watermark is visible to a casual viewer on a careful inspection.

The invisible-robust watermark is embedded or applied in such a way that changes made to the pixel value are perceptually not noticed and it can be recovered only with appropriate decoding mechanism.

The invisible-fragile watermark is applied or embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark. [1]

1.5 Watermarking Techniques [2]

Frequency Domain Watermarking

This technique is very much similar to spatial domain watermarking in which the values of chosen frequencies can be changed. The watermark signal is applied to lower frequencies for the reason that high frequencies will be lost by solidity or scaling,

Spread Spectrum

Spread spectrum technique can be used for both frequency domain and spatial domain. In this method the watermark extraction is achievable without using the original unmarked image.

Spatial Domain Techniques

In this technique

- ✓ Watermark is applied in pixel province.
- ✓ During watermark embedding no transforms are applied to the host signal.
- ✓ In the pixel domain the combination with the host domain is based on easy operations.
- ✓ The watermark can be detected by correlating the anticipated model with the received signal.
- ✓ This technique is performed by changing values of pixel color samples of a video frame.
- ✓ LSB algorithm uses Spatial Domain Technique**.**

1.6 Watermarking using LSB [2]

What is LSB?

- ✓ It stands for Least Significant Bit.
- ✓ It is the byte or octet in that position of a multi byte number which has the least potential value

- ✓ The least significant bit (LSB) gives the unit value and it shows the bit position in a binary integer.
- ✓ It determines whether the number is odd or even.
- ✓ The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right.
- ✓ It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position.
- ✓ If the number changes even slightly then the least significant bits have the useful property of changing rapidly.
- ✓ It is easy to understand
- ✓ Simple to implement

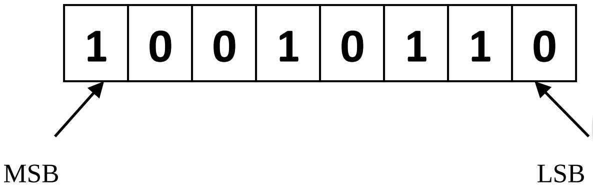


Figure 2 Binary representations of decimal 150

- ✓It shows the binary representation of decimal 150. Here LSB represents a value of 0. The MSB is an 8-bit binary number which represents a value of 128 decimal.

Least Significant Bit Modification

In Least Significant Bit method watermark embedding embed the watermark into the least significant bits of the cover object. It is the simplest method of watermarking. LSB substitution has many drawbacks say undesirable noise, cropping, or lossy compression etc.

In this the impact of watermark is negligible on the cover object. As the hacker came to know about the algorithm, he can easily modified the embedded watermark without any problem. As it is not possible for a hacker to view the watermark.

PSNR

The full form of PSNR is Peak signal-to-noise ratio. It shows the ratio between the most feasible power of a signal and the power of corrupting noise which affects the reliability of its illustration. PSNR is usually expressed in terms of the logarithmic decibel scale as many signals have very large dynamic variety.

It is mostly used to calculate the quality of rebuilding of lossy compression codecs e.g., for image compression. In this the original data is used as a signal, and the noise is the error introduced by compression. Even though a higher PSNR usually indicates that the rebuilding is of higher excellence, but in some cases it is not necessary. It is easily defined with the help of mean squared error (MSE).

Given a noise –free mxn monochrome image I and its noisy approximation K, MSE is defined as:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR (in dB) is defined as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

Where

MAX_I = maximum possible pixel value of the image.

$MAX_{I\,=}$ 255, When the pixels are represented using 8 bits per sample.

$MAX_{I\,=}$ 2^B-1, when samples are represented using linear PCM with B bits per sample.
m = Numbers of rows of pixels of the images
i = Index of that row
n = Number of columns of pixels of the image
j = index of that column

In lossy image and video compression the values for the PSNR are in between 30 and 50 dB, where the bit depth is 8 bits. The value of PSNR is between 60 and 80 dB for 16-bit data.

In the absence of noise, the two images I and K are identical, and thus the MSE is zero. In this case the PSNR is infinite or undefined.

2. DESIGN AND IMPLEMENTATION

Proposed Method

In this method the message image is encrypted with the cover image by using Watermarking using LSB technique and after encryption it is decrypted using the same technique to get cover image and message image in their original form. In this we use spatial domain method LSB for security of images, which is easy, simple and more effective method.

In this method the significant bit goes from 1 to 8 and then finding the related PSNR and MSE we can find the most efficient way of image watermarking.

Step1: We take a cover image and a message image which is to be watermarked

Step2: We take the significant bit ‘n’ that ranges from 1 to 8 and change the bit values of the images with respect to the value of ‘n’

Step3: We watermark the changed cover image with the message image and thus the message image get hidden called the steganographed image and also find the PSNR and MSE with respect to the original cover image

Step4: We extract the message image from the steganographed image called extracted image and find its PSNR and MSE with respect to the original message image

This concept is shown in figure.

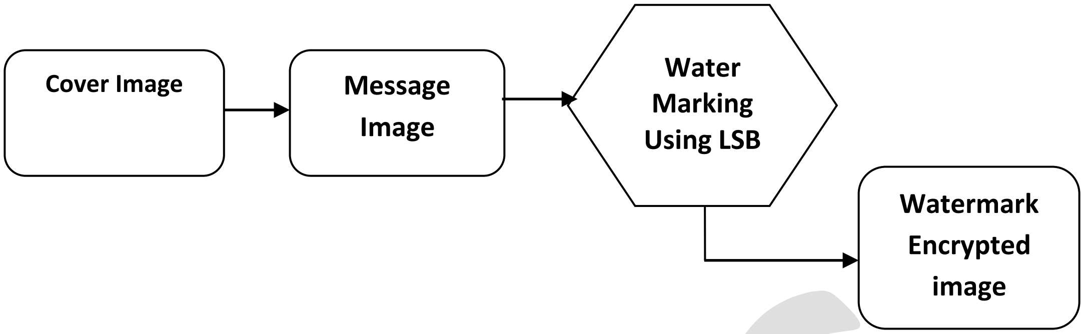


Figure 3 Encryption using Water marking

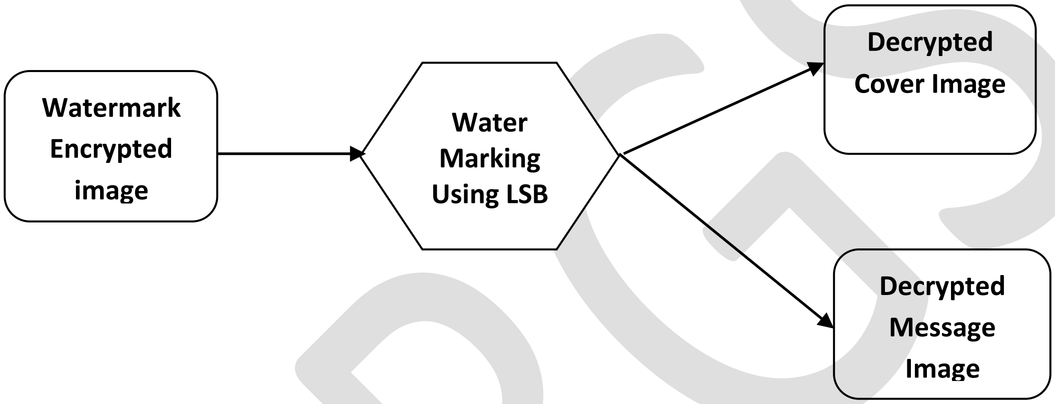


Figure 4 Decryption Using Watermarking

Proposed Algorithm [4]

Digital Watermarking Encryption Algorithm

1. Begin
2. Check the length of the watermark text to know how many copies will be embedded in the first LSB and if it will embed in the second LSB.
3. Embedding the length of the watermark text in the first LSB.
4. Convert the watermark text from characters to bits.
5. Inverse the watermark bit.
6. Check the coordinate of X, if it is odd, the algorithm will add 1 to X, and if it is even, the algorithm will subtract 1 from X.
7. Embed the watermark bit in the first LSB.
8. Go to 4 until finishing the entire watermark.
9. Go to 4 if we need to embed another copy of the watermark text.
10. Save the Image as bitmap image
11. End

Digital Watermarking Decryption Algorithm

1. Begin
2. Get the length of the watermark text from the first LSB.
3. The user can choose which copy he wants if there is more than one copy.
4. Check the coordinate of X, if it is odd, the algorithm will add 1 to X, and if it is even, the algorithm will subtract 1 from X.
5. Get the bit from the first LSB.
6. Converse the bit and save it in array.
7. Go to 3 until finishing all the watermark text.

8. Convert the array to characters.
9. End

Implementation

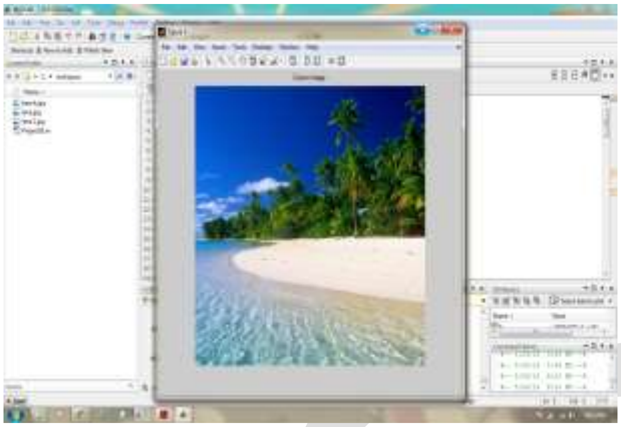


Figure 5 Cover Image

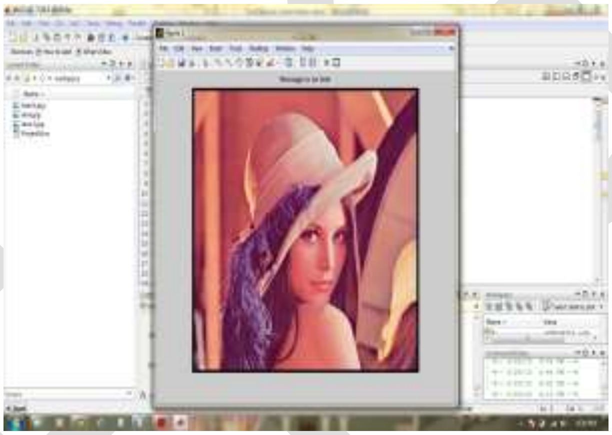
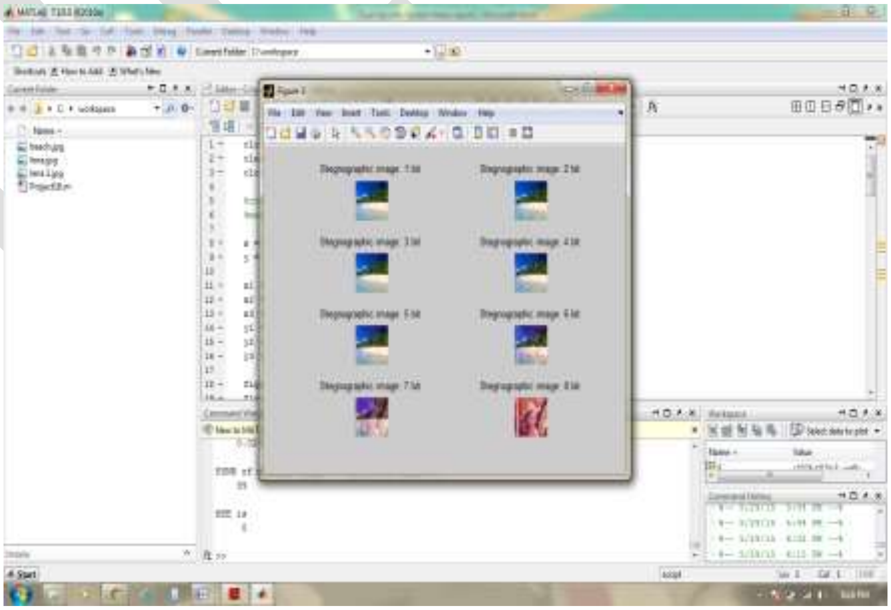
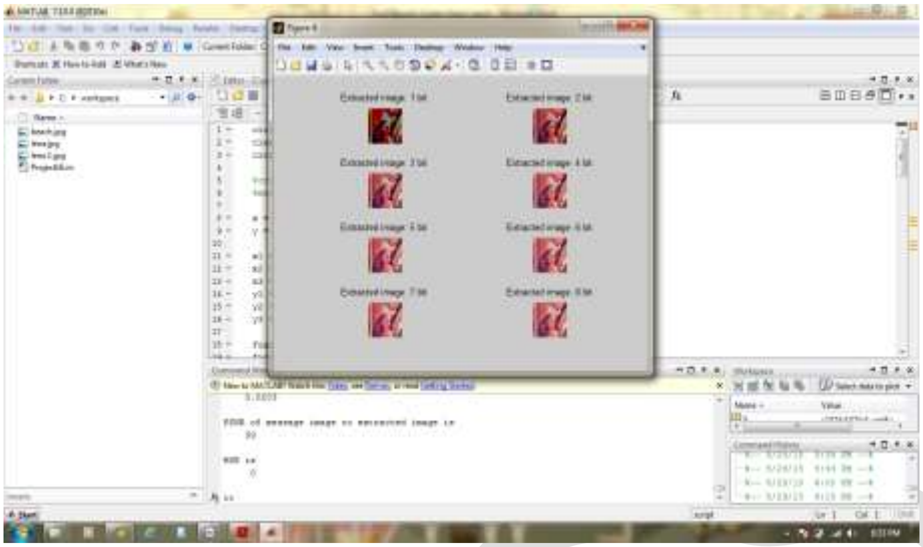


Figure 6 Message Image



MATLAB 7.10.0 (R2010a)
Figure 1
File
Edit
View
Insert
Tools
Desktop
Window
Help
Steganographic image 1 bit
Steganographic image 2 bit
Steganographic image 3 bit
Steganographic image 4 bit
Steganographic image 5 bit
Steganographic image 6 bit
Steganographic image 7 bit
Steganographic image 8 bit

Figure 7 Watermarking Encryption

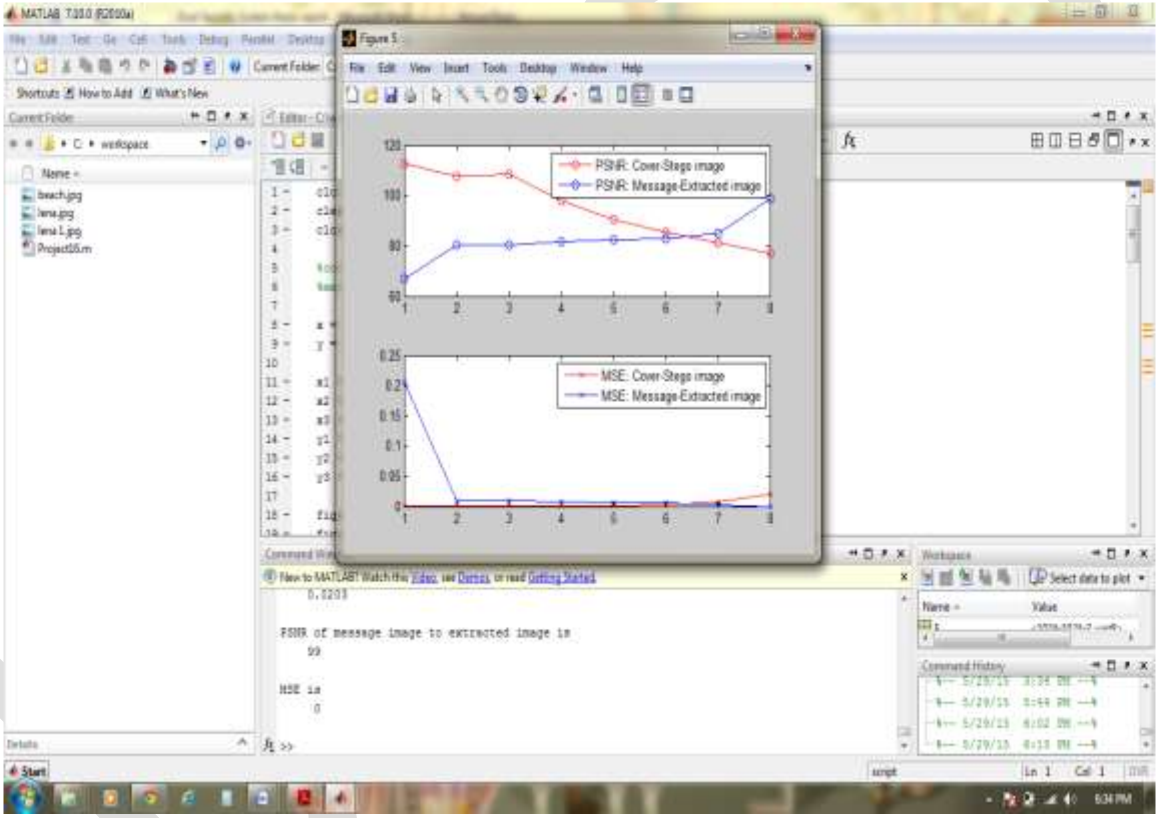


```
    5.0203

PSNR of message image to extracted image is
    99

MSE is
     0

fx >>
```

Figure 8 Watermarking Decryption

Table 1 Watermarking PSNR & MSE Performance data

BITS	**Cover and Stegano Image**		**Message and Extracted Image**	
	PSNR	**MSE**	**PSNR**	**MSE**
1	112.6254	0.0000	067.0760	0.2056
2	107.8026	0.0000	080.4077	0.0095
3	108.3338	0.0000	080.4417	0.0095
4	097.9986	0.0002	081.4062	0.0076
5	090.5155	0.0009	082.5240	0.0059
6	085.2998	0.0031	083.0040	0.0053
7	081.2784	0.0078	084.8493	0.0034
8	077.1236	0.0203	099.0000	0.0000



New to MATLAB? Watch this Video, see Demos, or read Getting Started.

```
     0.0203

PSNR of message image to extracted image is
    99

MSE is
     0

>>
```

Figure 9 Watermarking PSNR & MSE Performance chart

CONCLUSION

The result of watermarking using LSB method shows that that the best PSNR and MSE are obtained for 1st bit. Thus 1 bit LSB yields the best results. Though the best extraction PSNR and MSE is obtained for 8 bit LSB (also called 1 bit MSB) but this eventually shows the message thus is not useful.

From best to worse, the following LSB is:

1 → 2 → 3 → 4 → 5 → 6 → 7 → 8

Finally we can conclude that Watermarking using LSB is the easy to understand and best method for encryption and decryption.

FUTURE SCOPE

In the future user can improve the results of PSNR and MSE by use of different algorithms. We have been show that MSE and PSNR are better for 1 bit. For the future enhancement we can further improve the values of PSNR and MSE. We can reduce more to MSE and improved the value of PSNR. Image water marking have bright future in the digital communication. In all the devices of digital communication security is the main issue. So by the water marking we can send any digital image data by use proposed method without any Error

REFERENCES:

1 International Journal of Computer Science and Information Technologies, Vol. 3 (2) , 2012,3757-3760 **"Digital Image Watermarking for Copyright Protection"** by Shankar Thawkar Department of Information Technology Hindustan College of Science and Technology, Mathura (UP), India

2. **"Image Watermarking Using LSB (Least Significant Bit)**" Gurpreet Kaur, Kamaljeet Kaur

3. (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (2), 2012,
Digital Image Watermarking For Copyright Protection by Shankar Thawkar Department of Information Technology Hindustan College of Science and Technology, Mathura (UP), India

4. Journal Of Computing, Volume 3, Issue 4, April 2011, Issn 2151-9617 **"A New Digital Watermarking Algorithm Using Combination Of Least Significant Bit (LSB) And Inverse Bit** by Abdullah Bamatraf, Rosziati Ibrahim And Mohd. Najib Mohd. Salleh