

# LSB Based Digital Watermarking Technique

Rajni Goyal<sup>1</sup>, Naresh Kumar<sup>2</sup>

Department of Computer Science & Engineering, Giani Zail Singh PTU Campus Bathinda, Punjab

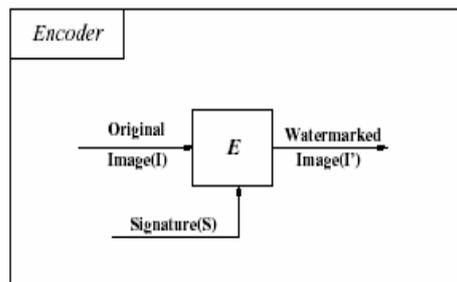
## ABSTRACT

*In the present scenario, data security is one of the major challenges. Watermarking is a technique in which a digital signal or pattern is inserted into a digital image for security reasons. Watermarking is mainly used for copyright protection, owner authentication and id card security. In this paper we have present the LSB watermarking technique. We will calculate the PSNR value of the given image. The result provide a better security and better PSNR values.*

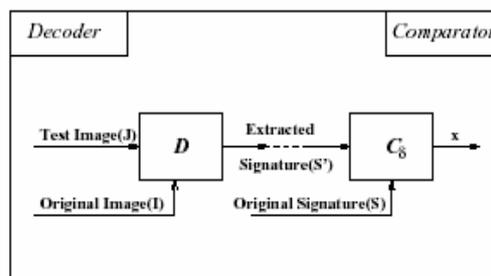
**Keywords :-**DCT, PSNR, NC

## 1. INTRODUCTION

Digital watermarking is the technique of embedding a digital signal (audio, video or image) or hide a small amount of digital data which cannot be easily removed is called digital watermarking.<sup>[1]</sup> Digital watermarking is also called data embedding. Watermarking can be applied to images, audio, video and to any software also. Digital watermarking is used to hide the information inside a signal, which cannot be easily extracted by the third party. Its widely used application is copyright protection of digital information. It is different from the encryption in the sense that it allows the user to access, view and interpret the signal but protect the ownership of the content. Figure represents the general framework of watermarking.<sup>[2]</sup>



**Fig. 1** General encoding process of watermarking



**Fig. 2** General decoding process of watermarking

## 2. RELATED WORK

In the related work, the most common method which is used to hide the message involve the usage of LSB developed by Chandramouli et al.<sup>[4]</sup>, by applying the filtering, masking and transformation on the cover media. Weiqi Luo et al.<sup>[5]</sup> proposed LSB matching revisited image steganography and edge adaptive scheme which can select the embedding regions according to the size of secret message. For large embedding rates, smooth edge regions are used while for lower embedding rate, sharper regions are used.

### Classification of Watermarking

Digital Watermarking techniques can be classified as:

- Text Watermarking
- Image Watermarking

- Audio Watermarking
- Video Watermarking

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

- I. Visible watermark
- II. Invisible Robust watermark
- III. Visible Fragile watermark

## TECHNIQUES OF WATERMARKING

### A.Frequency Domain Watermarking

These methods are similar to spatial domain watermarking in that the values of selected frequencies can be altered. Because high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies containing important elements of the original picture.

### B.Spread Spectrum

This technique can be used for both spatial domain and frequency domain. The spread spectrum method has the advantage that the watermark extraction is possible without using the original unmarked image [1].

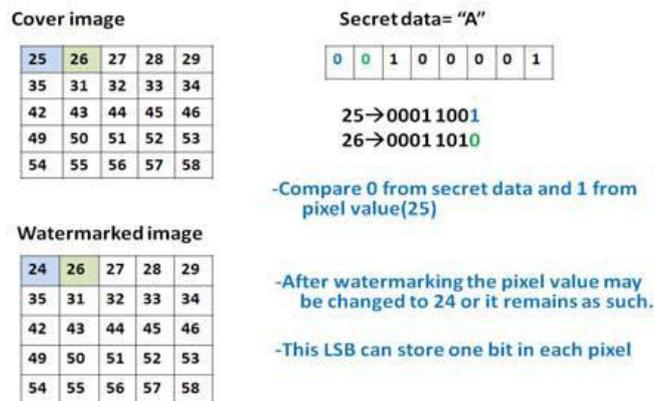
### C.Spatial Domain Techniques

Techniques in spatial domain class generally share the following characteristics:

1. The watermark is applied in the pixel domain.
2. No transforms are applied to the host signal during watermark embedding.
3. Combination with the host signal is based on simple operations, in the pixel domain.
4. The watermark can be detected by correlating the expected pattern with the received signal

## 4.LEAST SIGNIFICANT BIT

There are many algorithms available for invisible digital watermarking. The simplest algorithm is Least Significant Bit (LSB) Insertion, in which each 8-bit pixel's least significant bit is over written with a bit from the watermark. In a digital image, information can be inserted directly into every bit of image information or the more busy areas of an image can be calculated so as to hide such messages in less perceptible parts of an image. This method is based on the pixel value's Least Significant Bit (LSB) modifications.



**Fig. 4** Representing LSB Technique

The principle of embedding is fairly simple and effective. If we use a grayscale bitmap image, which is 8-bit, we would need to read in the file and then add data to the least significant bits of each pixel, in every 8-bit pixel. In a grayscale image each pixel is represented by 1byte consist of 8 bits. It can represent 256 gray colors between the black which is 0 to the white which is 255. The principle of encoding uses the Least Significant Bit of each of these bytes, the bit on the far right side. If data is encoded to only the last two significant bits (which are the first and second LSB) of each color component it is most likely not going to be detectable; the human retina becomes the limiting factor in viewing pictures [7].For the sake of this example only the least significant bit of each pixel will be used for embedding information. If the pixel value is 138 which is the value 10000110 in binary and the watermark bit is 1, the value of the pixel will be 10000111 in binary which is 139 in decimal. In this example we change the underline pixel. [11]. Features of LSB (Least-Significant-Bit)

- a. It is simple to understand
- b. Easy to implement
- c. It results in stego-images that contain hidden data yet appear to be of high visual fidelity.

## 5.RESULTS

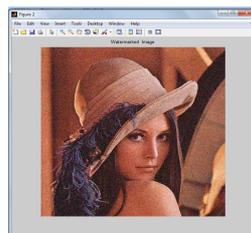
We take leena .jpg as the cover image. Size of the image is 512\*512. Koala.jpg is embedded in the cover image as the watermark.



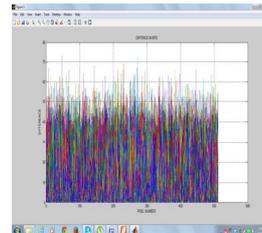
a. Cover Image  
(leena.jpg)



b. Watermark image  
(Koala.jpg)



c. Watermarked image



d. Difference in bits

we applied this method on different images like Leena.jpg, koala.jpg and pepper.jpg and we get the following results.

**Table 1.** Results for different images

Image	PSNR Value
Leena	55.96
Koala	54.32
Pepper	54.12

## 6.CONCLUSION & FUTURE SCOPE

The increasing amount of security threats we need large security needs .Multimedia documents and specifically images are affected. In the current state of research, it is difficult to affirm which watermarking approach seems most suitable to ensure an secure transfer of data. The tool used for the execution of this algorithm was Matlab. The aim of the program is to replace the LSB of the base image with the MSB of the watermark. In future LSB may also use for other type of data and test on different type of images and we can get more noise free images with improved PSNR values.

## REFERENCES

- [1] Deepshikha Chopra, Preeti Gupta, Gaur Sanjay B.C., Anil Gupta, ” Lsb Based Digital Image Watermarking For Gray Scale Image”, IOSR Journal of Computer Engineering (IOSRJCE)ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 1 (Sep-Oct. 2012), PP 36-41
- [2] Dr. Ajit ,Preeti Kalra, Sonia Dhull, ”Digital Watermarking” ,International Journal of Advanced Research in Computer Science and Software Engineering, ISSN:2277 128X, Volume 3, Issue 4. April 2013

- [3] Preeti Gupta, “Cryptography based digital image watermarking algorithm to increase security of watermark data”, International Journal of Scientific & Engineering Research, ISSN 2229-5518 Volume 3, Issue 9 (September 2012)
- [4] Manpreet Kaur, Sonika Jindal, Sunny Behal, “A Study of Digital Image Watermarking”, IJREAS ,Volume 2, Issue 2 (February 2012) pp-126-136
- [5] B Surekha, Dr GN Swamy, “A Spatial Domain Public Image Watermarking”, International Journal of Security and ItsApplications Vol. 5 No. 1, January, 2011
- [6] Robert, L., and T. Shanmugapriya, “A Study on Digital Watermarking Techniques ”, International Journal of Recent Trends in Engineering, vol. 1, no. 2, pp. 223-225, 2009.
- [7] H.Arafat Ali, “Qualitative Spatial Image Data Hiding for Secure Data Transmission”, GVIP Journal, Volume 7, Issue 2 , pages 35

#### **AUTHOR**



**Rajni Goyal** Completed her Graduation degree from Rayat Bahra Group of Institutes, Kharar in the year 2010 and pursuing M.Tech from GZSPTU Campus Bathinda.