



Implementation of a Least Significant Bit (LSB) based Spatial Domain Watermarking Technique

Sanjay Kumar*, Ambar Dutta

Department of Computer Science, Birla Institute of Technology, Mesra,
Kolkata Campus, India

Abstract— *Digital Watermarking has become one of the burning topics of research for the last few decades in the field of information security. This can be attributed to the rapid development of internet and wide usage of digital multimedia. Digital Watermarking is one of the techniques used for guaranteeing the authenticity of digital multimedia. The present paper reviews different types of watermarking techniques which are classified based on their characteristics and application. This paper also overviews LSB based watermarking techniques in spatial domain and the effect of different types of noise (Gaussian, Salt-and-pepper etc) over the watermarked images. The results of a LSB-based watermarking technique are studied with the help different cover images and watermark images. In order to measure the quality of the watermarked image with respect to the cover image, two most popular metrics, called Mean Square Error and Peak Signal Noise Ratio are used.*

Keywords— *Digital Watermarking, LSB, MSE, PSNR, Spatial Domain*

I. INTRODUCTION

Due to the rapid growth in computer and network technology, the need for securing digital information became an important issue [1, 2, 3, 4]. With the reduced cost and widespread usage of Computer and networking facilities, there is a huge need for approaches to store, access and distribute digital multimedia data. This is mainly due to property such as compact storage, distortion free transmission, and easy editing. This free access to digital multimedia communication provides offenders huge opportunities to pirate copyrighted materials. Hence the interest of using digital watermark has significantly increased in order to detect and trace copyright violation which results in active research in watermark embedding robustness with respect to compression, cryptographic attacks and image processing operations in recent years. It is evident from the literature that developed techniques have grown and been improved a great deal over time. Digital watermarking, also referred to as simply watermarking, is a method to hide the data or identifying information within the digital multimedia. The digital multimedia includes text, images, video, digital audio and software. Digital watermarking process involves the two major steps – (i) Watermark embedding- in which the watermark is inserted into the host image using a defined algorithm, and (ii) Watermark extraction- in which the watermark is extracted from the image[4]. Digital Watermarking is considered as a suitable tool for identification of creator, source, owner, distributor or authorized consumer of a document [5]. It is also used to check whether an image or document has illegally been modified, distributed or tampered. Watermarking, when complemented by encryption, finds huge applications in data authentication, broadcast monitoring and copyright protection [5, 6].

The remainder of the paper is structured as follows. In section II, detailed classification of watermarking is presented. Section III deals with discussion of different spatial domain watermarking techniques. An implementation of a LSB-based watermarking technique along with the experimental results is presented in section IV. Finally, conclusion is made in section V.

II. CLASSIFICATION

In the literature, there exists a number of ways in which existing watermarking techniques are classified. In this paper, classification of watermarking is done based on characteristics and application [5].

A. Classification based on Characteristics

The watermarking techniques can be categorized into the following five classes based on the characteristics of the embedded watermarks.

1) *Blind and Non-blind*: The watermarking technique that does not need access to the actual unwatermarked data to recover the watermark is termed as blind watermarking. On the other hand, watermarking technique is said to be non-blind if the original data is required for the extraction of watermark. Non-blind watermarking is more robust because the watermark can only be extracted by knowing the unwatermarked data. But, blind watermarking found its usefulness in most of the applications compared to its non-blind counterpart.

2) *Perceptible and Imperceptible*: A watermark that is visible to human eyes is called perceptible watermark, otherwise the watermark is said to be imperceptible. The perceptible watermark is used in the primary application. Whereas the imperceptible watermarks are used in the complex application such as document identification where the content which

is watermarked should be in unchanged states. One of the limitation of the perceptible watermark is that, it is only applicable for the images ex-maps, graphics etc.

3) *Private and Public*: A watermark is private watermark if authorized user can detect it. Use of private, pseudo-random key makes it difficult for unauthorized user to extract the watermark. This private key specifies the secret location of watermark in the host image. On contrary, watermarking technique that allows anybody to read watermark are called public watermarking. Private watermarking is more robust than public one

4) *Robust, Semi-fragile and Fragile*: Robust watermarks are those which are designed to survive against intentional and unintentional, arbitrary malicious attacks. They found their application in copyright protection. A semi-fragile watermark is intended to detect any unauthorized modification, allowing some image processing operations. A fragile watermark is a watermark that is easily modified or altered when the host image is modified through a linear or non-linear transformation. Fragile watermarks have limited robustness; they are applied for detection and modification of data rather than conveying inerasable information.

5) *Spatial and Frequency-domain*: In spatial domain watermarking method the watermark is directly embedded by modifying the gray value of the pixels of the original image without applying any transformation. On the other hand, in frequency domain method the watermark is embedded after performing some transformation such as, DWT, DFT, DCT etc. Spatial domain techniques are simpler, but less robust compared to frequency domain techniques.

B. Classification based on Application

The watermarking techniques can also be classified into the following five categories based on their applications.

1) *Copyright Protection Watermarks*: The availability and efficiency of global computer network for the communication of digital information has made easier to stored, manipulate transmit the digital data. The watermark for copyright protection is developed to identify both the source of the image and its authorize user.

2) *Data Authentication Watermarks*: Digital signature is one of the well known cryptographic approaches for data authentication. But in the event of the loss of the signature, the authentication work could not be performed. The solution for this problem is that the signature can directly be embedded into the work using watermarking [5]. An effective authentication scheme should be able to govern whether an image has been modified or not, identify any modification made on the image and merge, authentication data host image

3) *Fingerprint Watermarks*: Because of the advancement of technology, one of the possible applications of digital watermarking is fingerprinting. Fingerprinting in digital watermarking is generally used as the process of embedding the uniqueness to the image such that it is difficult to tempered or abolish. This permits the copyright holder to discover freebooter if the image is distributed illegally.

4) *Copy Control Watermarks*: Digital media have an advantage that can be copied without loss in quality but at the same point of time it is having disadvantage from copyright management view. There are various research on copy control is going on. IBM, Tokyo Research Laboratory first proposed the use of watermarking technology for DVD copy protection in September 1996. The security and control can be maintained at the time of distributing and publishing information, two approaches may be used – (i) *Use of watermarking for copyright protection*, (ii) *Establishing digital right management system for copy control of distributed information* where intellectual right protection and copy control are major concerns.

5) *Device Control Watermarks*: Device control watermarking is a technique in which, watermarks are embedded to control access to resource using a verifying device. Synchronization and control watermarks may be embedded into radio and TV signal. Several techniques of watermarking are developed in audio devices in past decades, including lowest-bit coding, spread spectrum quantization index modification. Watermarking systems embeds an authorization code in signal and transmit it into a verifying device. Video watermarking on a mobile device is a great challenge due to the limited resource of device. One of the techniques for video watermarking in mobile converts the video to Ycbcr representation and insert the watermark in Y component of the extracted frame of the video.

III. SPATIAL DOMAIN WATERMARKING TECHNIQUES

The approaches in the spatial domain watermarking shares the following attribute [1]-

1. The watermark implementation is carried out in pixel domain.
2. During embedding phase, no transform are applied to the host signal.
3. Correlating the required pattern with receive signal watermark will be detected

A. LSB Substitution

One of the simplest algorithms for the digital watermarking is Least Significant Bit Insertion. Wang and Lin [3] developed an algorithm to insert essential data in the host image so that the interceptor will not notice the existence of data in the image. They used genetic algorithm to hide important data in the right most k-LSB of the host image to obtain a high quality result. Dharwadkar and Amberkar [7] proposed a spatial domain LSB based watermarking method for colour image. They stored number of bits in each pixel in variables based on the original colour value of the pixels. They used the red, green and blue channel of the colour image for watermark embedding capacity, equivalent to the cover image size. In their method, use of secret key and permuting the watermark bits preserved the security. Singh and Jain [8] proposed the algorithm for digital watermarking using Least Significant Bit using the binary value of watermark text in Least Significant Bit, and in place of second Least Significant Bit the inverse of their correspond LSB bit. The proposed

method had given the better authenticity due to using 2nd Least Significant Bit. Radouane and Boujiha [9] proposed an algorithm of digital watermarking based on embedding watermark into sub image with LSB technique. In their work, watermark was embedded into an individual block of the cover image. The blocks were selected on the basis of entropy values, the block having the maximum entropy value is selected for embedding. In this method no distortion occurred for the watermarked image.

B. Additive Watermarking

Smitha and Navas [2] worked on the estimating the data hiding capacity of ROI medical image. They also focused on the optimizing the JPEG survival level that allow fair JPEG compression for conventional spatial domain watermarking. In their additive watermarking algorithm, the cover image and the watermark used in it were of the same size. Let C(m, n) is the cover image and D(m, n) is a watermark which is to be embedded on the cover image. The primary embedding formula used in [2] is

$$W(m, n) = C(m, n)(1 + \alpha * D(m, n))$$

where A is embedding strength, and W(m,n) is watermark image.

The retrieval of the cover image will be done using-

$$D(m, n) = \frac{W(m, n) - C(m, n)}{\alpha * C(m, n)}$$

Smitha and Navas took the watermark as a text image of size 128*128 and added the watermark value to cover image with a suitable embedding strength value.

IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

In this work of watermarking all images of size 256*256 pixel by 8 bit per pixel gray scale image are taken [1]. An image CI (cover image or base image) is selected in which watermark is inserted. Now, watermark image is selected which is further added to the base image.

A. Watermarking Technique (Embedding and Extraction)

In order to embed a watermark into cover image, the steps are as follows:

1. For each pixel in the cover image, n least significant bits (LSB) are set to zero (1<=n<=7)
2. For each pixel in the watermark, intensity values are shifted right by 8 – n bits.
3. Modified cover image and watermark are added to find the watermarked image.

On the other hand, in order to extract the watermark, for each pixel of the watermarked image, intensity values are shifted left by 8 – n bits.

B. Experimental Results

In order to measure the quality of the watermarked image (W) with respect to the cover image (C), two popular metrics, namely Mean Square Error (MSE) and Peak Signal Noise Ratio (PSNR) are used. MSE is signal fidelity measure with an aim to make the comparison between two signals by providing the approximate score which describes the error/distortion level between them.

$$MSE(W, C) = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N [C(i, j) - W(i, j)]^2$$

MSE is often converted into a peak-to-peak signal-to-noise ratio (PSNR) measure

$$PSNR = 10 \log_{10} \frac{L^2}{MSE}$$

where L is the dynamic range of allowable image pixel intensities. In order to examine the efficiency of the implemented algorithm, experimentation was done with the help of a number of cover image and watermark. But, in this paper, results with respect to only one set of cover image and watermark is shown.



Cover Image



Watermark Image

The experimental data are shown in the following tables. Table 1 shows the watermark image with respect to the above cover image and watermark without noise and in the presence of Gaussian and salt-and-pepper noise. Table 2 gives the MSE and PSNR values with respect to watermark image and cover image in the presence/absence of noise.

Table 1: Watermark Image in the presence/absence of noise












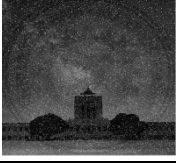









	Watermark Image without noise	Watermark Image with Gaussian noise	Watermark Image with Salt-and-pepper noise
1 st Bit Substitution			
2 nd Bit Substitution			
3 rd Bit Substitution			
4 th Bit Substitution			
5 th Bit Substitution			
6 th Bit Substitution			
7 th Bit Substitution			

Table 2: MSE and PSNR values in the presence/absence of noise

	Watermark Image without noise		Watermark Image with Gaussian noise		Watermark Image with Salt-and-pepper noise	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
1 st Bit Substitution	0.3688	52.4968	0.3954	52.1940	0.3686	52.4997
2 nd Bit Substitution	2.567	44.0694	2.8613	43.5991	2.6047	44.0072
3 rd Bit Substitution	13.0546	37.0072	14.5298	36.5422	13.3006	36.9261
4 th Bit Substitution	59.4535	30.4230	64.7418	30.0529	60.5928	30.3406
5 th Bit Substitution	125.1976	27.1888	130.3216	27.0146	124.1165	27.2265
6 th Bit Substitution	171.6518	25.8183	169.4309	25.8749	169.0044	25.8858
7 th Bit Substitution	188.5223	25.4112	192.7706	25.3144	185.3647	25.4845

It is seen from the two tables that the implemented spatial-domain watermarking technique based on LSB substitution is robust with respect to noise. It is evident from the result that MSE and PSNR values are not varying much with the introduction of Gaussian and salt-and-pepper noise into cover image.

V. CONCLUSIONS

In this paper, different types of digital watermarking techniques are explored. It is followed by an implementation of an LSB-based spatial domain watermarking technique. The results of the implemented algorithm are shown with the help of a cover images and watermark image. The results of the techniques are also discussed after adding different types of noise to the cover image. The present work can be extended to a comparative study of different spatial domain watermarking techniques with respect to different cover images and watermarks.

REFERENCES

- [1] D. Chopra, P. Gupta, G. Sanjay, A. Gupta, "Lsb Based Digital Image Watermarking For Gray Scale Image", ISOR Journals of Computer Engineering, Volume 6, Issue 1, pp 36-41, 2012.
- [2] B. Smitha and K. A. Navas, "Spatial Domain-High Capacity Data Hiding In ROI Images", IEEE International Conference on Signal Processing, Communications and Networking, Chennai, India, pp.528-533, 2007
- [3] R. Z. Wang, C. F. Lin, J. C. Lin, "Image hiding by optimal substitution and genetic algorithm". Pattern Recognition 34 (2001) 671-683.
- [4] M. O. Ali, E. A. Osman and R. Row, "Invisible Digital Image Watermarking in Spatial Domain with Random Localization" International Journal of Engineering and Innovative Technology, Volume 2, Issue 5, 2012.
- [5] F. Y. Shih, "Digital Watermarking and Steganography: Fundamentals and Techniques", CRC Press, First Indian Reprint, 2012.
- [6] I. J. Cox, M. L. Miller, J.A Bloon, J. Fridrich, T. Kalker, "Digital Watermarking and Steganography", Morgan Kaufman Publication, Second edition, 2011.
- [7] N. Dharwadkar and B. B. Amberker, "Secure Watermarking Scheme for Color Image Using Intensity of Pixel and LSB Substitution", Journal of Computing, Volume 1, Issue 1, December 2009.
- [8] A. Singh, S. Jain and A. Jain, "Digital Watermarking method using Replacement of Second Least Significant Bit (LSB) with inverse of LSB", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 2, February 2013.
- [9] M. Radouane , T. Boujiha, R. Messoussi, N. Idrissi, A. Roukh, "A Method of LSB Substitution based on image blocks and maximum entropy", International Journal of Computer Science Issues, Vol. 10, Issue 1, January 2013.