INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD ISSN: 2455-0620 Volume - 5, Issue - 7, July – 2019
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value: 86.87 Impact Factor: 6.497
Received Date: 17/07/2019 Acceptance Date: 27/07/2019 Publication Date: 31/07/2019

LSB Based Image Hiding System

[1] Nay Myo Aung, [2] Thandar Myint
[1]Lecturer, Department of Information Technology, Technological University (Mandalay), Myanmar
[2]Lecturer, Department of Information Technology, Technological University (Mandalay), Myanmar
[1]naymyothandar@gmail.com, [2]thandar73nay@gmail.com

Abstract: *Digital image watermarking is an efficient technique to protect copyright and ownership of digital information. Today improvement of technologies is rapidly that it easier to send the data/image accurate and faster to the destination. But this advantage is also accompanied with the disadvantage of modifying and misusing the valuable information through intercepting or hacking. In order to transfer the data/image to the intended user without any attacks and to protect the data in unauthorized person. There are many approaches like Cryptography, Watermarking and Steganography to hide data. In this paper, Digital Image Watermarking using Least Significant Bit (LSB) algorithm has been used for embedding the message/logo into the image. Experimental results show an improvement over existing methods n terms of Peak Signal to Noise Ratio (PSNR) and Mean square error (MSE).*

Keyword: *Digital image watermarking, LSB, PSNR, MSE.*

1. Introduction to Digital Image Watermarking:

Nowadays, Internet and Multimedia technologies have become our needs. Hence it has become digital data transfer is populated. Obviously, it leads to unauthorized replication problem. Digital image watermarking is an efficient technique to protect copyright and ownership of digital information.

Privacy is the ability of an individual or group to insulate them or information about themselves and thereby reveal them selectively. Data privacy or data protection has become increasingly important as more and more systems are connected to the internet. In order to circumvent the problem of the security attacks in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography and Digital Image Watermarking.

In digital watermarking, the actual bits are scattered in the image in such a way that they cannot be identified and show resilience against attempts to remove the hidden data.

*Classification of Watermarking
Digital Watermarking techniques can be classified as:
1) Text Watermarking
2) Image Watermarking
3) Audio Watermarking
4) Video Watermarking

Moreover, the digital watermarks can be divided into three different types as follows:
1) Visible watermark
2) Invisible-Robust watermark
3) Invisible-Fragile watermark

The digital image watermarking system essentially consists of a watermark embedded and a watermark detector as shown in figure 1.1.

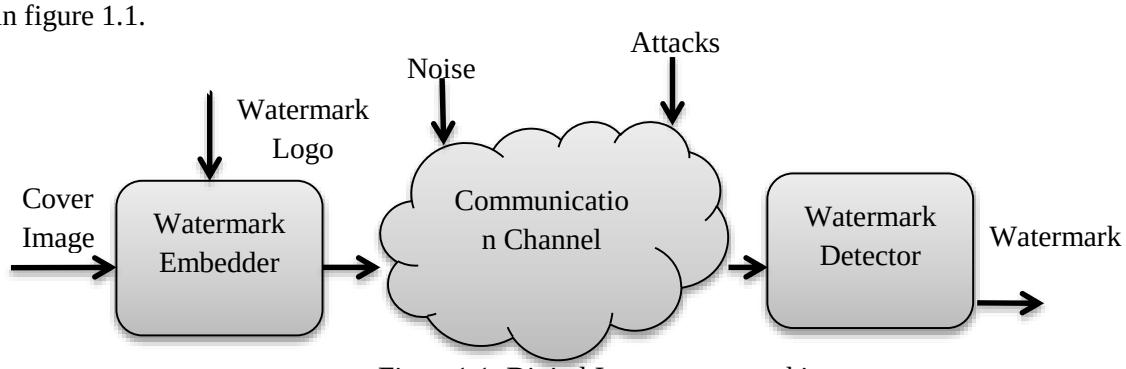


Figure1.1. Digital Image watermarking

The watermark embedded inserts a watermark onto the cover image and the watermark detector detects the presence of watermark information/logo.

2. Digital Image Watermarking Technique

Watermarking takes place either in the spatial domain, where the addition of the watermark is done directly to the pixel values of the image, or in a transformed domain like discrete cosine transformed domain (DCT) or the discrete wavelet transform domain (DWT). The block diagram of watermarking techniques is shown in Fig. 2.1.

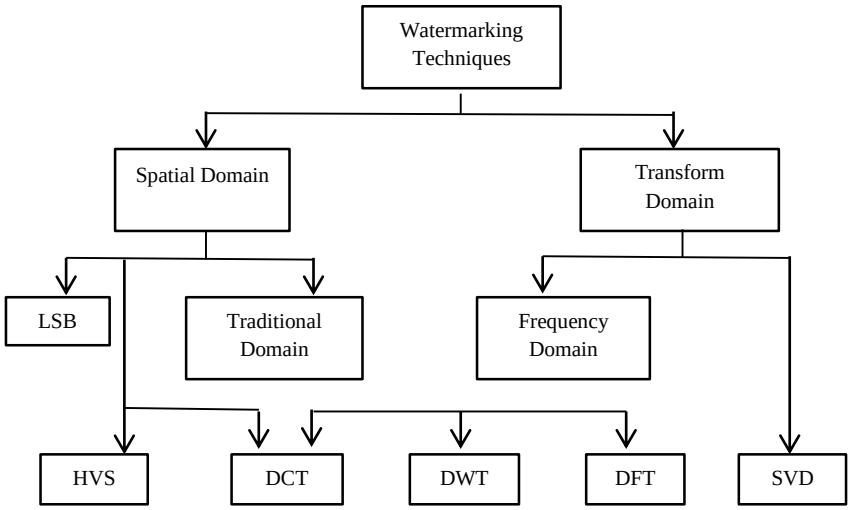


Figure.1. Watermarking Scheme

2.1. Watermarking in the Spatial Domain

Image processing functions in the spatial domain may be expressed as

$$g(x, y) = T[f(x, y)] \quad (3.1)$$

where g (x, y) is the processed image, f (x, y) is the input image, and T is an operator on f, defined over some neighborhood of (x, y). In this case, when the neighborhood is 1x1, g depends only on the value of f at (x, y), and T becomes a gray-level transformation function of the from $S = T(r)$ (3.2) Where r and s are variables denoting the gray level of f (x, y) and g (x, y) at any point (x, y). Thus powerful processing approached can be formulated with gray-level transformations. Because enhancement at any point in an image depends only on the gray level at that point, this technique is referred to as point processing strength.

2.2. Background Theory

The least significant bit (LSB) technique is used for simple operation to embed information in a cover image. The LSB technique is that inside of a cover image pixels are changed by bits of the secret image. Although the number was embedded into the first 8 bytes of the grid, the 1 to 4 least bits needed to be changed according to the embedded image. On the average, only half of the bits in an image will need to be modified to hide a secret image using a cover image. Because the quality of the Watermarked image is low, less than over the 4-bit LSB, changing the LSB of a pixel results in small changes in the intensity of the colors. In Figure 1, the pixel value of the cover image is 198 (11000110) and the secret data is 1. It applies to LSB-1 that the changed pixel value of the cover is 199(11000111). LSB can store 1-bit in each pixel. If the cover image size is 256 x 256 pixel image, it can thus store a total amount of 65,536 bits or 8,192 bytes of embedded data.

2.3. Proposed Method

Most of researchers have proposed the first LSB but our proposed watermarking algorithm is using the 1-bit LSB for hiding the data. This is because of the security reason. So, no one will expect that the hidden data in the LSB. The framework of the proposed method is shown in Figure2.2. First, we select the image which is a grayscale image and we will transfer the data to binary value after typing it. Then, hide the data in the image using the proposed algorithm. The embedding algorithm in MATLAB. Then, we will get the watermarked image. Then, the receiver will retrieve the data back and extracting algorithm in MATLAB. The data will be extracted from the watermarked image.

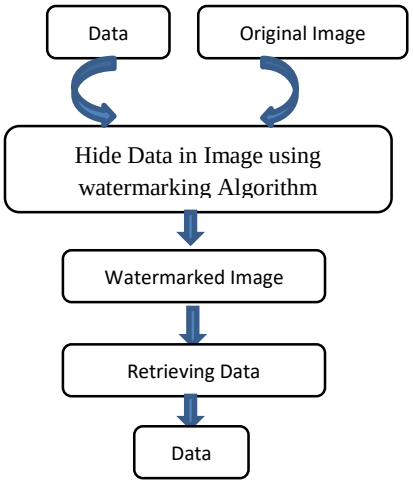


Figure.2.2.The framework of the proposed method

2.4. Watermark Embedding

Step 1: Take a cover image and read it in the MATLAB show in Fig 2.3 and 2.4.

Figure.2.3.Cover Image Figure.2.4.Image Matrix

Step2: Convert the Cover Image from decimal to binary

```
11000110 11000010 11000111 11010001 11000110 11000100 11000111 11001011
11001000 11001000 11000001 11001000 11000011 11000111 11000101 11001000
11000100 11000011 11000011 11000011 11000101 11000101 11000101 11000110
11000100 11000100 11000100 11000100 11000110 11000110 11000110 11000110
11000111 11000110 11000110 11000110 11000110 11000111 11000111 11000111
11000110 11000101 11000101 .......
```

Step 3: Take a watermark image, read in the MATLAB and change RGB to Gray scale show in Fig 2.5 and 2.6.

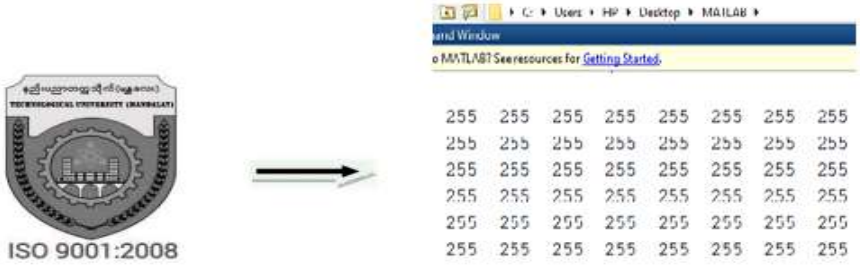
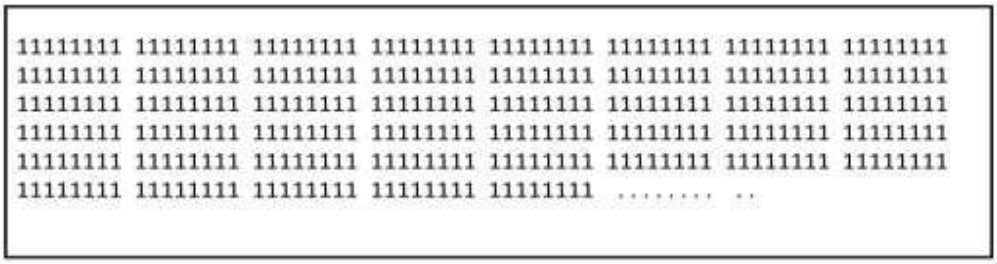
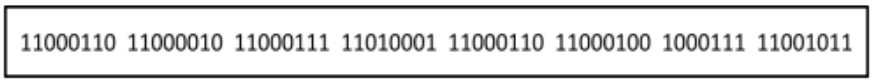


Figure 2.5.Watermark Image Figure 2.6.Image Matrix

Step 4: Convert the Watermark Image from decimal to binary



Step 5: Take first 8 byte of original data from the Cover Image.

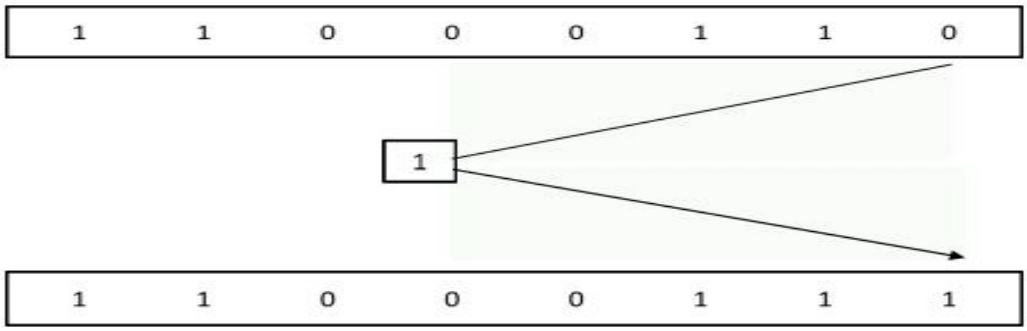


Step 6: Replace the least significant bit by one bit of the data to be hidden.

- First byte of original data from the Cover Image

- First bit of the data to be hidden

- Replace the least significant bit



- Finally get watermarked image show in Fig 2.7

Figure 2.7. Watermark, Cover Image and Watermarked Image

2.5. Watermark Extraction

- Extract embedded bits as LSB and get the watermark image show in Fig 2.8 and 2.9.

Figure 2.8.Watermarked Image

Figure 2.9.Watermark

2.6. Performance Measuring of Digital Watermarking

The performance of the digital watermarking system can be determined by using different statistical measures. The differences between the original cover image and the watermarked image decide how the watermarking system is good or not. The most commonly used error metrics for comparing are Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) [13Ali].

2.6.1. Mean Square Error (MSE)

It is calculated by comparing byte by byte performance of cover image and watermarked image. The MSE is calculated with the formula as below:

$$MSE = \frac{\sum M,N\ [I1(m,n) - I2(m,n)]^2}{M * N} \tag{2.3}$$

Where M is rows and N is columns in the input images and $I1$ (m, n) is the original image, $I2$ (m, n) is the Watermarked image. The value of MSE should be as small as possible because it indicates the dissimilarity between the cover and watermarked images.

2.6.2. Peak Signal to Noise Ratio (PSNR)

The quality of watermarked image compared with cover image is measured by Peak Signal to Noise Ratio (PSNR) in decibels. The higher value of PSNR gives the better image quality. The PSNR for an image is computed as follows:

$$PSNR = 10 \log_{10} \left[\frac{R^2}{MSE} \right] \tag{2.4}$$

Where R is maximum fluctuation or value in the image, its value is 255 for 8 bit unsigned number. It is observed that the human vision cannot identify any distortions in watermarked-images having PSNR beyond 36 dB for gray scale images. Thus, appropriate PSNR value is between 30-60dB for images and video media.

3. Design of the Proposed System

Design of the Proposed System is shown in Figure 3.1 and Figure 3.2.

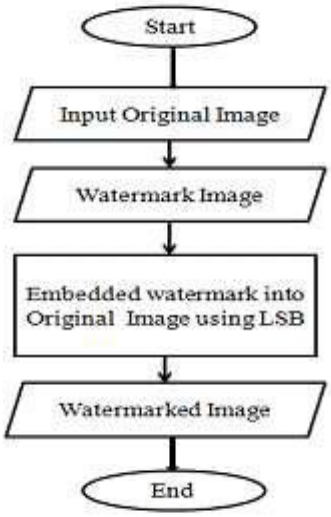


Figure .3.1.Embedding of image watermarking

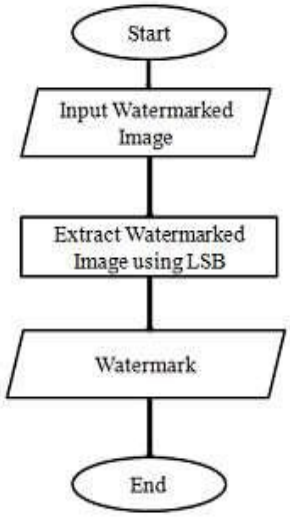


Figure .3.2. Extraction of watermark

3.1. Digital Image Watermarking Implementation

There are a few steps in digital image watermarking system. When the user run this program, menu window appear as shown in Fig. 3.3. This menu consists of two items. There are input image and hiding process. The first item consists of input cover image and watermark image. The second item consists of hide using LSB. If these items are clicked, open dialog box will be appeared as shown in Fig. 3.4.

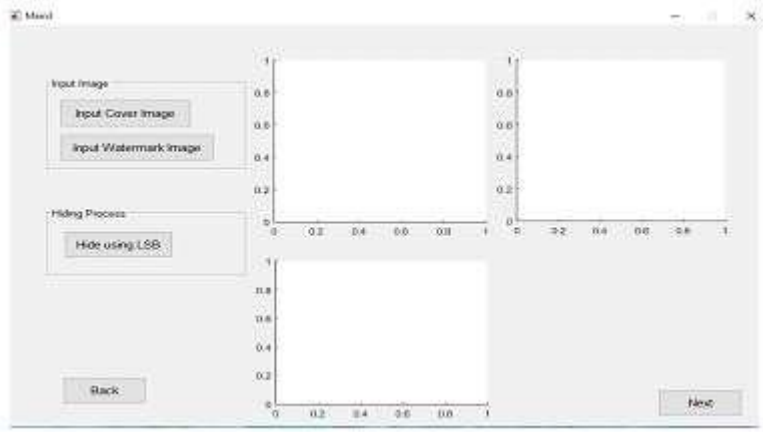


Figure 3.3. Menu Window

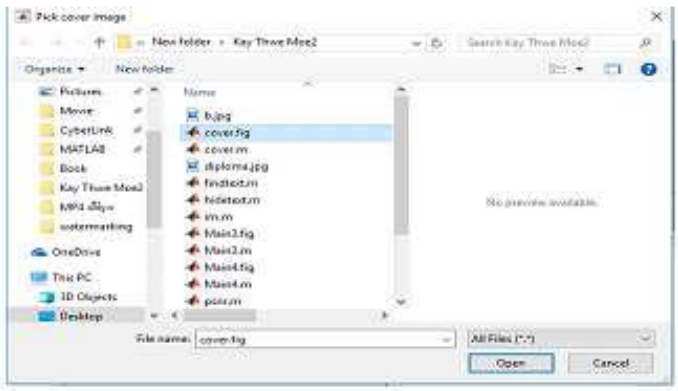


Figure 3.4. Open Dialog Box

The cover image and watermark image can be seen in Fig. 3.5 and Fig. 3.6 respectively. In this thesis, my own certificate image is used as a sample image. In the experiment, the size of the cover image is 512 x 512

INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD ISSN: 2455-0620 Volume - 5, Issue - 7, July – 2019
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value: 86.87 Impact Factor: 6.497
Received Date: 17/07/2019 Acceptance Date: 27/07/2019 Publication Date: 31/07/2019

with 256 intensities. The watermark is used Technological University Mandalay Logo. The watermark is a visually meaningful binary image ofsize 128 x 128.

Figure 3.5. Cover Image Figure 3.6 Watermark Image

The “hide using LSB” button is used to embed the watermark image into cover image. Fig.3.7 shows the watermarked image.

Figure3.7. Watermarked Image Figure3.8. Embedding of image watermarking

Figure3.8. show the embedding of image watermarking and Fig.3.9. show the two items, there are input image and extraction process. The first item consist of input watermark button and second item consists of extract watermark and PSNR buttons. The quality of watermarked image compared with cover image is measured by Peak Signal to Noise Ratio (PSNR) in decibels. The higher value of PSNR gives the better image quality.

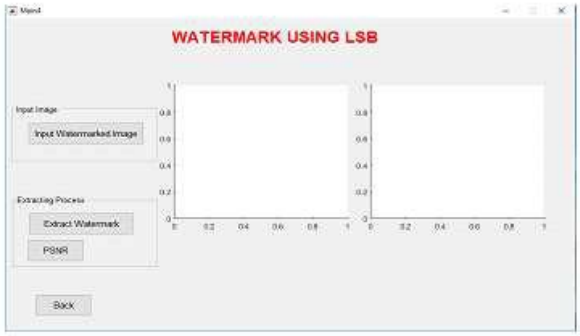


Figure 3.9.Watermark extracted from watermarked image and Calculated PSNR value

The “extract watermark” button is used to extract watermark from the watermarked image. If the input image is same as the watermark image in the embedding state, the watermark will be extracted as shown in Fig.3.10. This extracted watermark image can be easily used to identify the owner of the cover image.

Figure3.10. Extracted watermark and result of PSNR value

3.2. Table for Performance Measuring of Digital Watermarking

The proposed system performs evaluation of results with design metrics such as MSE and PSNR. And the results are shown in table3.1. As the experimental result, the proposed system can resist many attack or distortions to the cover image. The proposed can detect the integrity of the watermark in the distorted cover image. The PSNR values of the worst embedding case and the most common one for 1 bit-planes by LSB substitution.

Table.3.1. Results of RSNR value

Cover Images	Extracted Watermark	PSNR Level (dB)
		42.8778
		42.8063
		28.7585
		27.6525

3.3. Summary

The fully implementation of digital image watermarking system has presented. This adaptive digital image watermarking system can produce the reliable and reasonable results. This system is used to protect against copyright infringements and also to prove the image is original. Extracted watermark can be easily used to identify the owner the host image. The proposed algorithm is robust to common image processing operations like JPEG image compression and median filter.

4. DISCUSSION:

This system has introduced the background information, requirements and evaluation techniques required for the digital image watermarking technique and implementation of non-blind digital image watermarking system in the spatial domain, which is computationally efficient. This technique expended the LSB substitution strategy and develops an advanced method by comparing the As precious discussion, the block size depended on the size of the watermark. In this case, the watermark size is 128 x 128 pixels, so the host image (512 x 512) divided into 4 x 4 not supposable equivalent size block. Thereafter, comparing the between cover image and watermarked image using PSNR.

5. CONCLUSION:

The recent expansion of the internet medium and usage in communications engineering besides in the daily life of the human beings, corporations, organizations, establishments, governments, military, etc and the networked multimedia systems has necessitated the need for protection of digital media. This is especially critical for the protection involves the authentication of object (text/image/video) ownership, and the identification of illegal copies of a (possibly forged/fake) object. An adaptive digital image watermarking system can be used to protect and enforce intellectual property right of the image creator or owner. The biggest advantage of this method is the security of original watermark is being covered.

REFERENCES:

1. Balsa L. Gunjal Department of Computer Engineering, Amrutvahini College of Engineering, Sangamner, Dist:A'nagar, MS, India. hello_baisa@yahoo.com: AN OVERVIEW OF TRANSFORM DOMAINROBUST DIGITAL IMAGE WATERMARKING ALGORITHMS
2. Ms. Patil V. A. and 2Ms. S. S. Tamboli, Image Watermarking Using Least Significant Bit (LSB) Algorithm; International Journal of Trend in Research and Development, Volume 3(3), ISSN: 2394-9333 www.ijtrd.com
3. Puneet Kr Sharma1 and Rajni2, ANALYSIS OF IMAGE WATERMARKING USING LEAST SIGNIFICANT BIT ALGORITHM, International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012
4. Ali Al-Haj; Combined DWT-DCT Digital Image Watermarking, Journal of Computer Science 3 (9): 740-746, 2007 ISSN 1549- 3636, 2007 Science Publications
5. Ali Ahmed Kamal; Digital Watermarking of Still Images, School of Electrical and Electronic Engineering, University of Manchester, (2013).