Digital Image Watermarking Based on LSB for Gray Scale Image

Jitendra Jain1 **Punit Johari2**
Department of Computer Science,
Madhav Institute of Technology and Science Gwalior

Abstract
In recent years, internet revolution resulted in an explosive growth in multimedia applications. The rapid advancement of internet has made it easier to send the data/image accurate and faster to the destination. Besides this, it is easier to modify and misuse the valuable information through hacking at the same time. Digital watermarking is one of the proposed solutions for copyright protection of multimedia data. A watermark is a form, image or text that is impressed onto paper, which provides evidence of its authenticity. In this paper an invisible watermarking technique (least significant bit) and a visible watermarking technique is implemented. This paper presents the general overview of image watermarking and different security issues. In this paper, Image Watermarking using Least Significant Bit (LSB) algorithm has been used for embedding the message/logo into the image. This work has been implemented through MATLAB.

Keywords
Least Significant bit (LSB), Peak Signal to Noise Ratio (PSNR), Watermark, Mean Square of Error (MSE), And Digital Image

1. INTRODUCTION

Watermarking could be a technique wont to hide information or characteristic data inside digital transmission. Our discussion can focus totally on the watermarking of digital pictures, though digital video, audio, and documents are habitually watermarked. Digital watermarking is turning into popular, especially for adding undetectable identifying marks, like author or copyright data.

The digital watermarking process embeds a signal into the media without significantly degrading its visual quality. Digital watermarking is a process to embed some information called watermark into different kinds of media called Cover Work [1, 2]. 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. Digital watermarking involves embedding a structure in a host signal to "mark" its ownership [3]. Digital watermarks are inside the information so that ownership of the information cannot be claimed by third party [4]. While some watermarks are visible [5], most watermarks are invisible.

Manuscript received June 5, 2014
Manuscript revised June 20, 2014

The best known Watermarking method that works in the Spatial Domain is the Least Significant Bit (LSB), which replaces the least significant bits of pixels selected to hide the information. This method has several implementation versions that improve the algorithm in certain aspects.

2. Process of Watermarking

The process of watermarking begins when the encoder inserts watermark into image, producing watermarked image. The decoder extracts and validates the presence of watermarked input or unmarked input. If the watermark is visible, the decoder is not needed. Otherwise, the decoder may or may not require a copy of decoder to do this job. If input image and/or watermarked image are used, the watermarking system is called a private or restricted-key system; otherwise, the system is public or unrestricted-key system. The decoder is so designed to process both marked as well as unmarked image. Finally, the decoder needs to correlate the extracted watermark with original image and compare the result to a predefined threshold that sets the degree of similarity accepted as a match. If the correlation matches the threshold value, then watermark is detected i.e. original image belong to the user otherwise the data does not belong to the user [6, 7].Digital image watermarking is similar to the concept of watermarking physical objects with the difference that the watermarking technique is used for digital content instead of physical objects in digital image watermarking a secret information or logo is embedded in another image in an impercitible manner. This secret information or logo is called watermark and it contains some metadata, like security or copyright information about the main data/image. The main image in which the watermark is embedded is known as cover image since it covers the watermark. The digital image watermarking system essentially consists of a watermark embedder and a watermark detector as shown in figure 1.1.

The watermark embedder inserts a watermark onto the cover image and the watermark detector detects the presence of watermark information/logo. Sometime a watermark key is also used during the process of embedding and detecting watermarks

Figure 1.1 Digital Image Watermarking

The watermark key has a one-to-one relation with watermark information. The watermark key is private and known to only intended users and it ensures that only desirable set of users can detect the watermark. Further, note that the communication channel can be noisy and hostile (i.e., prone to security attacks) and hence the digital image watermarking techniques should be resilient to both noise and security attacks [8].

3. Least Significant Bit Modification

The most common method of watermark embedding is to embed the watermark into the least significant-bits of the cover object [9]. Despite being a simple method, LSB substitution suffers from many drawbacks. Although it can survive transformations like cropping, any addition of undesirable noise or lossy compression but a more sophisticated attack that could simply set the LSB bits of each pixel to one can fully defeat the Watermark with negligible impact on the cover object. Once the algorithm is known to a hacker, the embedded watermark could be easily modified by him without any difficulty.

A more sophisticated approach over conventional LSB method would be to use a pseudorandom number generator which determines the pixels to be used for embedding watermark based on a given key [9]. Security of the watermark would be enhanced greatly as the Watermark could now be no longer is easily viewable to the hackers or any other unintended user. Although this algorithm is still vulnerable to replacing the LSB's with a constant value.

4. Litrature review and Methodology:

In the previous work, an original image (cover image) and a watermark image is embedded with bit by bit in LSB technique. Primarily 1 bit watermark is substituted, so that no results are affected but after 4 bit imbedding the watermark begins to show affected. Since, our aim is to hide watermark so there was drawback in previous work.

The aim of this paper is to hide watermark with any number of bits substitution, so that it can be hide watermark in a cover image so that unauthorised user can't read/watch message. The steps of algorithm are as follows-

1. This paper has taken two differet-2,image one is original image and other is watermark.
2. Determine the size of both images.
3. Calculate the height and width of original image.
4. Calculate the height and width of message object(watermark)
5. Scaling the original image with scaling factor.
6. Now we generate a watermark object.
7. Watermark(ii,jj)=message(mod(ii,Mm)+1, mod (jj,Nm)+1)
8. Now set the lsb of cover _object to the value of Watermark as a beset function. Watermarked_image(ii,jj)= bitset(watermarked_image(ii,jj),n,watermark(ii,jj));
9. Write the watermarked image.
10. Calculated PSNR and NC(normal correlation)

5. Result and Discussion

The Mean Square Error (MSE) [2,3]and the Peak Signal to Noise Ratio (PSNR) [2,3] are the two error metrics used to compare image compression quality. This ratio is often used as a quality measurement between the original and a watermarked image. If one of the signals is an original signal of acceptable (or perhaps pristine) quality, and The other is a distorted version of it whose quality is being evaluated, then the MSE may also be regarded as a measure of signal quality. MSE is a signal fidelity measure. The goal of a signal fidelity measure is to compare two signals by providing a quantitative score that describes the level of error/distortion between them. Usually, it is assumed that one of the signals is a pristine original, while the other is distorted or contaminated by errors. Suppose that x = { $\mathbf{x_i}$ i = 1, 2, · · ·, N} and y = {$\mathbf{y_i}$ i = 1, 2, · · · , N} are two finite-length, discrete signals (e.g., visual images), where N is the number of signal samples (pixels, if the signals are images) and $\mathbf{x_i}$ and $\mathbf{y_i}$ are the values of the i th samples in x and y, respectively. The MSE between the signals x and y is

$$\text{MSE}(x,y) = = \frac{1}{N}. \sum_{i=1}^{N} (\mathbf{x_i} - \mathbf{y_i})^2$$

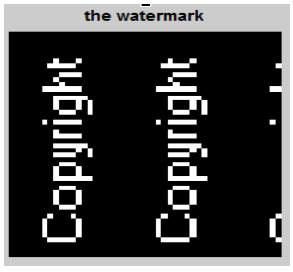
In the MSE, we will often refer to the error signal $\mathbf{e_i} = \mathbf{x_i} - \mathbf{y_i}$ which is the difference between the original and distorted signals. If one of the signals is an original signal of acceptable (or perhaps pristine) quality, and the other is a distorted version of it whose quality is being evaluated, then the MSE may also be regarded as a

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

$$PSNR = \frac{20log10L}{\sqrt{MSE}}$$

Where L is the dynamic range of allowable image pixel intensities. For example, for images that have allocations of 8 bits/pixel of gray-scale, L = 28−1 = 255. The PSNR is useful if images having different dynamic ranges are being compared, but otherwise contains no new information relative to the MSE.

Original image



Watermark

Bit 1 watermarked

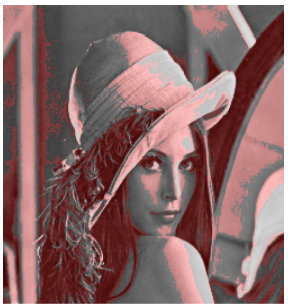
Bit 2 watermarked

Bit 3 watermarked

Bit 4 watermarked

Bit 5 watermarked

Bit 6 watermarked



Bit 7 watermarked

Bit 8 watermarket

Bit	Elapsed Time	PSNR	NR
1	0.3594	51.1440	0.9997
2	0.3750	45.1193	0.9993
3	0.4688	39.1116	0.9985
4	0.4219	33.1051	0.9980
5	0.4063	26.9516	0.9622
6	0.4063	21.6501	0.9736
7	0.4219	15.1870	0.9458
8	0.4375	10.6623	0.9331

Table- Bit wise Elapsed Time, PSNR value and NC (Normal Correlation)

6. CONCLUSION

In this a data hiding method by improved LSB substitution process is proposed. The image quality of the stego-image can be greatly improved with low extra computational complexity.Experimental result show the effectiveness of the proposed method. The results obtained also show significant

Improvement in PSNR than the method proposed in Ref. [10] with respect to image quality and computational efficiency.

A good balance between the security and the image quality is achieved. Our future work will focus on improving the efficiency of the proposed algorithm. The algorithm proposed in the current work describes a method such that the stego image which is obtained thereby cannot be proved as stego image using the steganalysis approach. In the proposed algorithm, the the number of steps are very less. Thus, the computational complexity is reduced. The algorithm is usage for both 8 bit and 24 bit image of the same size of cover and secret image, so it is easy to be implementing in both grayscale and color image. Benefited from the effective optimization, a good balance between the security and the image quality is achieved. The future work will focus on improving the efficiency of the proposed

REFERENCES

[1] Preeti Gupta, “Cryptography based digital image watermarking algorithm to increase security of watermark data”, InternationalJournal of Scientific & Engineering Research, Volume 3, Issue 9 (September 2012) ISSN 2229-5518.

[2] B Surekha, Dr GN Swamy, “A Spatial Domain Public Image Watermarking”, International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011.

[3] 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.

[4] H.Arafat Ali, “Qualitative Spatial Image Data Hiding for Secure Data Transmission”, GVIP Journal,Volume 7,Issue 2 , pages 35- 37, 2, August 2007.

[5] Cox, Miller and Bloom, “Digital watermarking”, 1st edition 2001, San Fransisco: Morgan Kaufmann Publisher.

[6] K. Watermarking digital Image and video data. IEEE Signal Processing Magazine, 17:20–46, 2000.

[7] C. Rey and J.L. Dugelay (2002). A survey of watermarking algorithms for image authentication. EURASIP Journal on Applied Signal Processing, 6:613–621.

[8] Brigitte Jellinek (Jan 2000), “Invisible Watermarking of Digital Images for Copyright Protection” submitted at University Salzburg, pp. 9 – 17.

[9] Frank Hartung, Martin Kutter (July 1999), “Multimedia Watermarking Techniques”, Proceedings of the IEEE, Vol. 87, No. 7, pp. 1085 – 1103.

[10] Amanpreet Kaur1, Renu Dhir2, and Geeta Sikka3 .A New Image Steganography Based On First Component

Alteration Technique (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 3, 2009).
[11] Rafael C.Gonzalez,"Digital Image Processing" second edition.
[12] Rao V. Dukkipati, "MATLAB An Introduction with Applications".