ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 4, July 2015

Quality evaluation of Image Watermarking using Spatial Domain Technique

Manpreet Kaur, Jatinder Pal Sharma
Assistant Professor
Dept. Of CSE, GIMET, Amritsar
man.kaur39@gmail.com
profsharma88@gmail.com

Abstract

The easy transmission and manipulation of digital data constitutes a real threat for information creators, and copyright owners want to be compensated every time their work is used. Watermark by itself is not sufficient to prevent abuses unless a proper protection protocol is established

This paper deals with the basic idea of image watermarking and gives brief Least Significant Bit (LSB) algorithm for embedding the message/logo into the image. The performance of the developed system is evaluated.

Keywords*: Watermarking, Spatial Domain, LSB,DCT.*

I. Introduction

Digital multimedia files like audio, images and videos are easily available to the public user by the boon of internet. Hence it has become a common practice to create copy, transmit and distribute digital data. Obviously, it leads to unauthorized replication problem. Digital image watermarking is solitary such technology that has been made to protect digital images from illicit manipulations. Digital Watermarking technique includes the process of embedding watermark and extraction of given watermark into the data file. A general definition can be as, "Hiding of a secret message or information within an ordinary message and extraction of it as its destination" [1, 2].

Two types of watermarking techniques are visible and invisible. Example of visible watermarking is the logo visible superimposed on the corner of television channel in a television picture. On the other hand, invisible watermark is hidden in the object which can

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 4, July 2015

be detected by an authorized person. Such watermarks are used for suit the author authentication and detecting unauthorized copying. Digital watermarking is described as one of the possibilities to close the gap between copyright issues and digital distribution of data. It acts as a very good medium for copyright issues as it embeds a symbol or a logo in the form of a watermark, which cannot be altered manually. The digital watermarking technique essentially consists of a watermark inserter and a watermark detector. The watermark inserter 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 [3]. The watermark key has a one-to-one correspondence with watermark information. The watermark key is private and known to only authorized parties and it ensures that only authorized parties can detect the watermark. The digital image watermarking system is shown in figure 1.

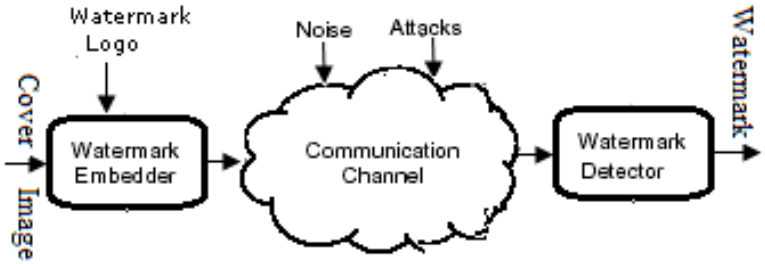

Fig. 1: Digital Image Watermarking

II. Spatial Domain Watermarking

Most watermarking research and publications are focused on images. The reason might be that there is a large demand for image watermarking products due to the fact that there are so many images available at no cost on the World Wide Web, which need to be protected. Image watermarking techniques is broadly classified into spatial domain and transform domain techniques [4].

Techniques in spatial domain class generally share the following characteristics:

- The watermark is applied in the pixel domain.
- No transforms are applied to the host signal during watermark embedding.
- Combination with the host signal is based on simple operations, in the pixel domain.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 4, July 2015

- The watermark can be detected by correlating the expected pattern with the received signal.

The main strengths of pixel domain methods are that they are conceptually simple and have very low computational complexities. However, they also exhibit a major drawback: The need for absolute spatial synchronization leads to high susceptibility to de-synchronization attacks.

Here, the secret messages are embedded directly. On spatial domain, the most common and simplest watermarking method is the least significant bits (LSB) insertion method. It is easy to be attacked. It reserves the image quality, increases embedding capacity but is not robust against attack because it is a spatial domain approach and no transfer is used. Based on the same embedding capacity, the proposed method improves both image quality and security [5, 6]. In Computer-Based Watermarking, several forms of digital media may be used as "cover" for hidden information. Photos, documents, web pages, and even MP3 music files may all serve as innocuous-looking hosts for secret messages. In covert communications through the Internet, digital images are possibly the most practical type of Watermarking medium primarily due to their sheer abundance in the Web. However, one common problem with using digital images is use of insufficient hiding capacities. Most watermarking software hide information by replacing only least-significant bits of an image with bits from the file that is to be hidden. This technique is generally called LSB encoding.

➢ ***Least Significant Bit Insertion***

The LSB is the simplest spatial domain watermarking technique to embed a watermark in the least significant bits of some randomly selected pixels of the cover image. Example of least significant bit watermarking:

Image Pixel (binary):
10010101 00111011 11001101 01010101…
Watermark bits:
1 0 1 0…..
Watermarked Image:
1001010**1** 0011101**0** 1100110**1** 0101010**0**…..

The main advantage of this method is that it is easily performed on images. And it provides high perceptual transparency. When we embed the watermark by using LSB the quality of the

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 4, July 2015

image will not degrade. The spatial domain watermarking is simple as compared to the transform domain watermarking. The robustness is the main limitation of the spatial domain watermarking [7].

III. Related Work

Cheng-Hsing Yang [8] proposes a new LSB-based method, called the inverted pattern (IP) LSB substitution approach to improve the quality of the stego-image. Each section of secret images is determined to be inverted or not inverted before it is embedded. The decisions are recorded by an IP for the purpose of extracting data and the pattern can be seen as a secret key or an extra data to be re-embedded.

Chien-Chang Chen and Yao-Hong Tsai [9] presents an adaptive block sized reversible image watermarking scheme. A reversible watermarking approach recovers the original image from a watermarked image after extracting the embedded watermarks. Experimental results show that the proposed adaptive block size scheme has higher capacity than conventional fixed block sized method.

Han-Min Tsai, Long-Wen Chang [10] proposes a secure reversible visible watermarking approach. The proposed pixel mapping function superposes a binary watermark image on a host image to create an intermediate visible watermarked image.

R. Bangaleea and H.C.S. Rughooputh [11] has proposed an algorithm, where a small number of bits are embedded onto an image in the spatial domain using a method similar to the direct sequence spread spectrum. The message bits are modulated with a PN sequence by Spread Spectrum modulation so that the watermark is tamper proof and has anti-jam properties in the transmission channel.

Dipti Prasad Mukherjee [12] have presented an invisible spatial domain watermark insertion algorithm for which we show that the watermark can be recovered, even if the attacker tries to manipulate the watermark with the knowledge of the watermarking process.

Liu and Tan [13] have proposed the use of SVD in watermarking. In their technique, authors find the singular values of the host image and then modify them by adding the watermark. SVD transform is again applied on the resultant matrix to find the modified singular values. These singular values are combined with the known component for getting watermarked image. This technique shows better robustness against geometric attacks when compared to wavelet based techniques.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 4, July 2015

IV. Results

LSB algorithms were implemented in MATLAB and performance of the developed system is evaluated. The quality performance of watermarking is evaluated in terms of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error). In ideal case PSNR should be infinite and MSE should be zero however in practical large value of PSNR and small value of MSE is desirable.

The Result shown below reveals that the watermarked and original image is perceptually same. This means that minimum degradation occurs when we use LSB watermarking technique. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error.

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

Where M and *N* are the number of rows and columns in the input images, respectively and I_1(m, n) is the original image, I_2 (m, n) is the watermarked image.

The PSNR is calculated using the following equation:

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

Where R represents maximum fluctuation or value in the image, its value is 255 for 8 bit unsigned number.

(a)

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 4, July 2015

(b)

(c)

Fig. 2: (a) Cover Image (b) Logo (c) Watermarked Image after LSB substitution

Fig. 3: Watermarked Image after 5th bit substitution

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 4, July 2015

Fig. 4: Watermarked Image after 8th bit substitution

Fig. 5: Recovered Watermark

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 4, July 2015

TABLE 1: PSNR & MSE for Different Bit Substitution

Method	PSNR	MSE	Embed Time
LSB or 1st Bit	55.9192	0.1664	0.8281
2nd Bit Substitution	50.0900	0.6369	0.8281
3rd Bit Substitution	43.7996	2.7109	0.8281
4th Bit Substitution	38.2486	9.7324	0.8125
5th Bit Substitution	32.4342	37.1247	0.7813
6th Bit Substitution	25.5523	181.0713	0.8750
7th Bit Substitution	20.8188	538.5146	0.7969
MSB or 8th Bit	15.4374	1.8593e+03	0.8594

V. Conclusions

This paper investigates the spatial domain watermarking technique. The performance of LSB based digital watermarking scheme with different bit substitution from LSB to MSB is evaluated. The LSB substitution of logo produce very less degradation and watermarked image has same quality s that of original image. However when we embedded the data in the consequent bits i.e second towards last (MSB) bit, the watermarked image start distorted. The PSNR and MSE values was calculated and shown in table 1.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 4, July 2015

References

1. Naderahmadian, Y.; Hosseini-Khayat, S., "Fast Watermarking Based on QR Decomposition in Wavelet Domain," Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on , vol., no., pp.127,130, 15-17 Oct. 2010.
2. Nan Lin; Jianjing Shen; Xiaofeng Guo; Jun Zhou, "A robust image watermarking based on DWT-QR decomposition," Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.684,688, 27-29 May 2011.
3. E. Vellasques, E. Granger, R. Sabourin, "Intelligent watermarking systems:" a survey, 4th ed., Handbook of Pattern Recognition and Computer Vision, World Scientific Review, 2010, pp. 687–724.
4. Panyavaraporn, J.; Horkaew, P.; Wongtrairat, W., "QR code watermarking algorithm based on wavelet transform,"Communications and Information Technologies (ISCIT), 2013 13th International Symposium on , vol., no., pp.791,796, 4-6 Sept. 2013.
5. Baisa L. Gunjal , R.R. Manthalkar "An Overview Of Transform Domain Robust Digital Image Watermarking Algorithms", Journal of Emerging Trends in Computing and Information Sciences, 2010-11.
6. Mustafa Osman Ali, and Rameshwar Rao., " Fundamentals of Digital Image Watermarking: an Overview". International Conference on Information and Communication Technology. pp. 64–67, Oct. 2011.
7. Henri Bruno Razafindradina, Nicolas Raft Razafindrakoto, Paul Auguste Randriamitantsoa "Improved Watermarking Scheme Using Discrete Cosine Transform and Schur Decomposition ",IJCSN International Journal of Computer Science and Network, Volume 2, Issue 4, August 2013 .
8. Cheng-HsingYang , "Inverted pattern approach to improve image quality of information hiding by LSB substitution", Elsevier , Pattern Recognition vol 41 pp 2674 – 2683, 2008.
9. Chien-Chang Chen and Yao-Hong Tsai, "Adaptive reversible image watermarking scheme", Elsevier , The Journal of Systems and Software vol. 84 pp 428–434, 2011.
10. Han-Min Tsai, Long-Wen Chang, "Secure reversible visible image watermarking with authentication", Elsevier, Signal Processing: Image Communication vol. 25 pp 10–17, 2010.
11. Mustafa Osman Ali, and Rameshwar Rao. Fundamentals of Digital Image Watermarking: an Overview. International Conference on Information and Communication Technology.. pp. 64–67, Oct. 2011.
12. Mustafa Osman Ali and Rameshwar Rao. "An Overview of

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 4, July 2015

13. Hardware Implementation for Digital Image Watermarking,"Proc. of International Conference on Signal, Image Processing and Applications (SIA 2011), Chennai, India, pp. 19-24, Dec. 2011.
14. K. Deb, Md. S. Al-Seraj, Md. M. Hoque and Md. I. H. Sarkar, "Combined DWT-DCT Based Digital Image
Watermarking Technique for Copyright Protection", International Conference on Electrical and Computer
Engineering, (2012) December 20-22.