DIGITAL WATERMARKING

Jyoti
Computer Science Engineering Department
Giani Zail Singh PTU Campus
Bathinda,India
jkjyotikhichi@gmail.com

Jyoti Rani
Computer Science Engineering Department
Giani Zail Singh PTU Campus
Bathinda,India
csejyotigill@gmail.com

Abstract— : *Due to the rapid advancement in internet technology and evolution of high speed networks working throughout the world, security of multimedia content is immediately required., information transmission faces a big confront of security. People need a protected and safe way to widen information. Digital watermarking is a process of data hiding, which provide security of data. The Digital watermarking method provides the quick and inexpensive distribution of digital information over the Internet. This technique provides new ways of ensuring the adequate security of copyright holders in the rational property dispersal process. The belongings of digital watermarking images allow insertion of additional data in the image without altering the value of the image. This message is secret in unused visual space in the image and stays below the human visible threshold for the image. This paper presents a watermarking technique which least significant bit (LSB), its steps and its process with matlab images. The benefits of the LSB are its simplicity to embed the bits of the message directly into the LSB plane of cover-image and many techniques using these methods.*

Keywords— *Watermarking, spatial domain, frequency domain, spread spectrum, LSB*

I. INTRODUCTION

The technique digital watermarking is used for extracting the hidden data and to hide the data within the carrier signal. The hidden data can be image, audio, text and video. Hidden messages are a group of bits describing information pertaining to the signal or the name of the author. The piece of information which we can insert is called watermark which can't be easily known to third person. Digital watermarking is a process which adds the data without change in its visual appearance. A digital watermark can be unique to each copy or common to multiples to many copies. There are many techniques used for security purposes like hashing, cryptography, admission control, but for the exclusive rights protection watermarking is the only technique used. Watermarks can be visible or invisible. It is widely used for the security purposes like ownership, copyright protection, authenticity etc.

II. CLASSIFICATION OF WATERMARKING

The classification of Digital Watermarking techniques as:

- ✓ Text Watermarking
- ✓ Image Watermarking
- ✓ Audio Watermarking
- ✓ Video Watermarking

Digital watermarks are of three types as follows:

- Visible watermark
- Invisible-Robust watermark
- Invisible-Fragile watermark

III. TECHNIQUES OF DIGITAL WATERMARKING

A. Frequency Domain Watermarking

In order to produce high quality image in the frequency or transform domain technique by first transmute the real image into the frequency domain by using DCT, DWT and DFT. It is applied to the selected or lower frequencies carry crucial elements of the real image because high signals will be missed during compression or scaling.

B. Spread Spectrum

In the spread spectrum watermark can be applied to the perceptual regions of the data despite the risk of potential reliability distortions. In spread spectrum extraction is completed not including using real unmarked images. Spread spectrum can be used for spatial as well as frequency domain.

C. Spatial Domain Techniques

The term spatial domain refers to the aggregate of pixels composing an image. In spatial domain technique the watermark in directly embedded in the pixel values and there is no transformations are done on the host signal.

In the pixel domain combination with the host signal is on the basis of simple operations. In this image imperceptibility is being maintained. The detection of the watermark can be done with expected data from receiving signals. The comparison is done between the original image and watermarked image during the extraction process. The spatial domain process is denoted by

$G(x,y)=T[f(x,y)]$

The mostly used algorithm in spatial domain is LSB

IV. LEAST SIGNIFICANT BIT

The simplest algorithm in the spatial domain is the Least Significant Bit (LSB). In the digital image processing, information can be inserted into all bit of image information or the busiest areas of an image can be calculated so as to hide such messages in less perceptible region of an image. There are two techniques were accessible to hide the data in the Spatial domain of images from them. These methods were based on the pixel value's LSB modifications. The algorithm anticipated by Kurah and McHughes to embed in the LSB and it was known as image reduction. An example of the less undetectable is Least Significant Bit insertion. During insertion each 8-bit pixel's least significant bit is overwritten with a bit from the watermark. The procedure of embedding is straightforward and accommodating. It moreover explains the functioning of an 8-bit grayscale image and their effects of varying in an image. If we apply a grayscale bitmap image which is 8-bit, next we require reading the file and then adding data to the least significant bits of all pixels. In a grayscale image each one pixel is represented by 1 byte having 8 bits and represent 256 gray colors between black which is 0 to the white which is 255. The process of encoding uses the Least Significant Bit of each of these bytes, which is as of the bit on the faraway right side. If data is encoded in only the last two significant bits of each color component it not to be detectable. The human retina has the limiting factor in viewing images. For example, just the least significant bit of every pixel will be used for embedding information. If the pixel value is 162 which is 10100010 in binary and the watermark bit is 1 then the value of the pixel will be 10100001in binary which is 161 in decimal (change the underlying pixel).

V. RELATED WORK

In this we will look into the review of digital watermarks used for images. This describes the preceding work which had been done on digital watermarking using LSB and other technique.

HAJJAJI in 2011 [1] proposed watermarking of medical image, in which a set of numbers or data is inserted in a medical image. The watermarking method is based on the least significant bits (LSBs) in order to check the integrity and confidentiality of medical information and to maintain confidentiality for patient and hospital data. For 10% compression rate, the watermark is successfully recovered. Disadvantage of these technique is that, all the substituted extract when a Gaussian noise is applied in the watermarked image

Puneet Kr Sharma and Rajniin 2012 [2] proposed image watermarking & different security issues. To hide logo (secret image) into the cover image they used LSB algorithm. LSB each of the pixel of the cover image is replaced by the bits of the secret image. Then 2nd LSB of each pixel of the cover image is replaced by the bits of the secret image and so on. Then PSNR and MSE are calculated for bit substitution from LSB to MSB in image.

Deepshikha Chopra in 2012 [3] watermarking technique and a visible watermarking technique using Least Significant Bit algorithm, the least significant bits of pixels selected to hide the information. They applied various attacks on the watermarked image and their impacts on quality of images are measured using MSE and PSNR.

Koushik Pal in 2012 [4] proposed biomedical image watermarking technique, modified bit replacement algorithm in spatial domain, which is much better than the conventional simple LSB technique. They embedded multiple copies of the same information in several bits of the cover image starting from the lower order to the upper orders. If some of the information is lost due to an attack, they still collect the left over information and recover the watermark from the cover image using the bit majority algorithm.

Hong Jie He in 2006 [5] proposed a wavelet-based fragile watermarking scheme for secure image authentication. In their proposed scheme, they generated the embedded watermark using the

discrete wavelet transform (DWT), and then they elaborated security watermark by scrambling encryption is embedded into the least significant bit (LSB) of the host image.

Gil-Je Lee in 2008 [6] undertaken a new LSB digital watermarking method by using random mapping function. The main idea behind their proposed algorithm is to embed watermark randomly in the coordinates of the image by using random functions to be more robust than the traditional LSB method.

Saeid Fazli in 2010 [7] proposed a watermarking scheme by using SSIM Quality Metrics. In their algorithm, they used significant bit planes of the watermark image rather than the lower bit-planes of the asset picture.

Abdullah Bamatraf in 2011 [8] proposed a new LSB based digital watermarking method with the combination of LSB and inverse bit. Their algorithm is also tested using Peak signal-to-noise ratio (PSNR) and the result is compared with traditional LSB and maintains the quality of watermarked image. Their paper also shows the results when combining different positions and the combination between the LSB.

Amit Jain in 2013[9] proposed a new LSB digital watermarking technique by using inverse bit. In their algorithm first insert watermark into least significant bit place and then the inverse of least significant bit(LSB), is to insert second least significant bit. This algorithm is supple with the length of the watermark text.

Gurpreet Kaur in 2011[10] presented an image watermarking using LSB algorithm using two parameters standard deviation and mean. Image watermarking can do either by text is used for secret message or by image is used for secret image. Different parameters are compared like PNSR, MSE, entropy, mean and standard deviation.

VI. CONCLUSION

There are different techniques used in watermarking for security of images. Frequency domain, Spatial domain and spread spectrum. Spatial domain method of the LSB is used for security of images, which is easy and simple and more effective method. The process of the LSB is simple and easy when we use in MATLAB. A different image in MATLAB tells dissimilar process steps and their outcome. In future LSB
maybe also apply on other type of data and test on different type of images may also apply on other type of data and test on different type of images.

REFERENCES

[1] Mohamed Ali HAJJAJI Abdellatif MTIBAA El-bey BOURENNANE, “A Watermarking of Medical Image: Method Based "LSB"”, Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 12,December 2011, ISSN 2079-8407, pp. 714-721.

[2] Puneet Kr Sharma and Rajni, “Analysis of Image Watermarking using Least Significant Bit Algorithm” International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012, pp. 95-101.

[3] 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.

[4] Koushik Pal, Goutam Ghosh, Mahua Bhattacharya, “A Comparative Study between LSB and Modified Bit Replacement (MBR) Watermarking Technique in SpatialDomain for Biomedical Image Security” International Journal of Computer Applications and Technology (2278 - 8298) Volume 1 – Issue 1, 2012, pp. 30-39.

[5] He, H. J., Zhang, J. S. and Tai, H. M., (2006), A Wavelet-Based Fragile Watermarking Scheme for Secure Image Authentication. Springer-Verlag Berlin Heidelberg 2006.

[6] G. J. Lee, E. J. Yoon, And K..Y. Yoo, “A new LSB based Digital Watermarking Scheme with Random Mapping Function”, in 2008 IEEE DOI 10.1109/UMC.2008.33.

[7] S. Fazli, and G. Khodaverdi, “Trade-off between Imperceptibility and robustness of LSB Watermarking using SSIM Quality Metrics” in 2010 IEEE DOI 10.1109/ICMV 2009.68.

[8] A. Bamatraf, R. Ibrahim and M. N. M. Salleh , “A new Digital Watermarking using LSB and Inverse bit” Journal of Computing, Vol. 3, April 2011, ISSN2151-9617.

[9] 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, Vol. 3, February 2013, ISSN 2250-2459, ISO 9001:2008.

[10] Kaur Gurpreet and Kaur Kamaljit, “Implementing LSB on Image Watermarking using Text and Image”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, April 2011

[11] L. Robert and T. Shanmugapriya, “A Study on Digital Watermarking Techniques”, International Journal of Recent Trends in Engineering, Vol. 1, No.2, pp. 223-225, 2009

[12] H. Varma, A. Singh, and R. Kumar, ”Robustness of Digital Image Watermarking Techniques against brightness and rotation attacks”, International Journal of Computer Science and Information Security, Vol.1, 2009

[13] M. Kaur, S. Jindal, and S. Behal, “A Study of Digital Image Watermarking”, IJREAS ,Vol. 2, pp-126-136February,2012

[14] D. Chopra, P. Gupta, S. Gaur, and A. Gupta., “LSB based Digital Image Watermarking for Gray Scale Image”, IOSR Journal of Computer Engineering, Vol. 1(Sep-Oct. 2012), pp 36-41 ISSN 2278-0661, IBSN 2278-8727

[15] Preeti Gupta, “Cryptography based digital image watermarking algorithm to increase security of watermark data”, International Journal of Scientific & Engineering Research, Vol. 3, September 2012, ISSN 2229-5518.