Digital Image Watermarking using LSB Technique

Anum Javeed Zargar

Abstract-Watermarking belongs to hide particular information, so that you can easily detect any tamper detection .It is used for confidenality, authentication and copy right protection. In this paper watermarking is done with the help of least significant bit technique (LSB).As LSB technique is used as it has less effect on image. This new algorithm is using LSB of original image and İdoing '&&' operation with MSB of watermark image, and same watermarked image is then extracted from host image by replacing its LSB with MSB and making its LSB zeroes, so then watermark is extracted from host image

Index terms: Watermark Grayscale images, PSNR, Least significant bit, Watermark text

******

1. INTRODUCTION

Privacy of data or images is important nowadays, as threat and Hackers are all over the world so we insert watermark in our cover image so we can easily detect our original image, with the help of our inserted watermark, if some eavesdropper try to claim the image. So Watermarking plays important role in terms of authencity and confidenality, and we can easily detect tamper detection. Watermarking is a pattern of bits inserted into a digital image, Audio or video file that specifies the file's copyright information such author rights and so on [1]. Thus, watermarking approach is used to make sure of the protection of the data. However, watermarking is also designed to be completely invisible. The actual bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and tampered [2].Thus, the watermarking must be robust enough so that it can withstand normal changes to the files such as attacking by noise. Contrast to printed watermarks, digital watermarking is a technique where bits of information are embedded in such a way that is completely invisible [3]. The problem with the traditional way of printing logos or names is that they may be easily tampered or duplicate

- Anum Javeed Zargar is currently pursuing masters degree in Japyee university information and technology. Email-id anumjaved11@gmail.com

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 [4]. Media watermarking research is a very active area and digital image watermarking became an interesting protection measure and got the attention of many Researchers since the early 1990s [5].

The rest of this paper is organized as follows: Section 2 describes the related work and LSB. Section 3 discusses the review lsb. In Section 4 discusses proposed work. In Section 5 embedding and extraction algorithms. In Section 6 Experiments and results are discussed. In Section 7 conclusion and references are discussed.

2. RELATED WORK

In this section we will look into the review of digital watermarks used for images. It describes the previous Work which had been done on digital watermarking by using LSB technique and other techniques, including the analysis of various watermarking schemes and their Results. Gaur Bhatnagar et al [6], presented a semi-blind reference watermarking scheme based on discrete wavelet Transform (DWT) and singular value decomposition (SVD) for copyright protection and authenticity. Their Watermark was a gray scale logo image. For watermark embedding, their algorithm transformed the original Image into wavelet domain and a reference sub-image is formed using directive contrast and wavelet coefficients. Then, their algorithm embedded the watermark into reference image

by modifying the singular values of reference image using the singular values of the watermark.

3 REVIEW OF LSB

In a digital image, information can be inserted directly into every bit of image information or the more busy Areas of an image can be calculated so as to hide such messages in less perceptible parts of an image [9],[10]. Tirkel et al [11] were one of the first used techniques for image watermarking. Two techniques were presented to hide data in the spatial domain of images by them. These methods were based on the pixel value's Least Significant Bit (LSB) modifications. The algorithm proposed by Kurah and McHugh's [12] to embed in the LSB and it was known as image downgrading [13]. An example of the less predictable or less perceptible is Least Significant Bit insertion. This section explains how this works for an 8-bit grayscale image and the possible effects of altering such an image. The principle of embedding is fairly simple and effective. If we use a grayscale bitmap image, which is 8-bit, we would need to read in the file and then add data to the least significant bits of each pixel, in every 8-bit pixel. In a grayscale image each pixel is represented by 1 byte consist of 8 bits. It can represent 256 gray colors between the black which is 0 to the white which is 255.The principle of encoding uses the Least Significant Bit of each of these bytes, the bit on the far right side. If data is encoded to only the last two significant bits (which are the first and second LSB) of each color component it is most likely not going to be detectable; the human retina becomes the limiting factor in viewing pictures [6]. For the sake of this example only the least significant bit of each pixel will be used for embedding information. If the pixel value is 138 which is the value 10000110 in binary and the watermark bit is 1, the value of the pixel will be 10000111 in binary which is 139 in decimal.

4 PROPOSED METHOD

Based on lsb technique we propose a new watermarking algorithm, which is simple and resistant to number of attacks. In it we took a gray scale Lena image and crop it according to desired parameters and convert it pixel value from decimal to binary form .Then took any watermark image and also crop it according to desired pixels of watermark image. SO both watermark and cover image will be cropped according to desired pixels

Now make lsb of cover image 0000, and '&& 'its lsb with MSB of watermark image. So in our host image watermark will be embedded and it will similar to our original image. To detect that it is original image we can easily extract watermark from it .Now we make lsb 0000 of host image and make it lsb its msb .so we will get watermark image as 4 subplots...

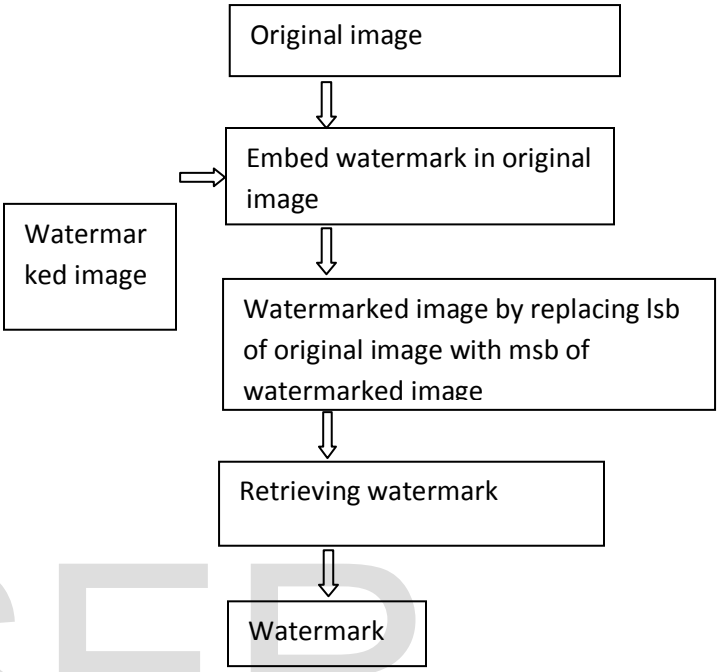
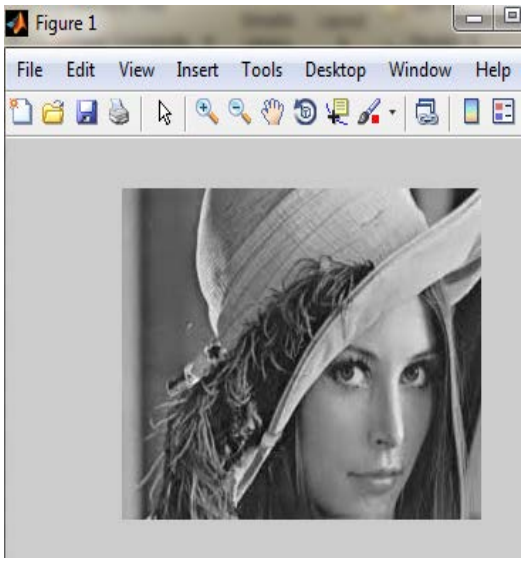


Figure 1

5 EMBEDDING ALGORITHM

In embedding algorithm, we first took an original image and read it in the mat lab then crop it according to desired pixels, and then took a watermark image read it accordingly in mat lab and crop it according to the pixels of cover image**.** Then change their pixel values from binary to decimal form, now after changing it into decimal form. Replace lsb of original image with msb of watermark image, as value ranges from 0-255 and lsb images are of less value, so we will get a host image with MSB of watermark image and lsb of its own.



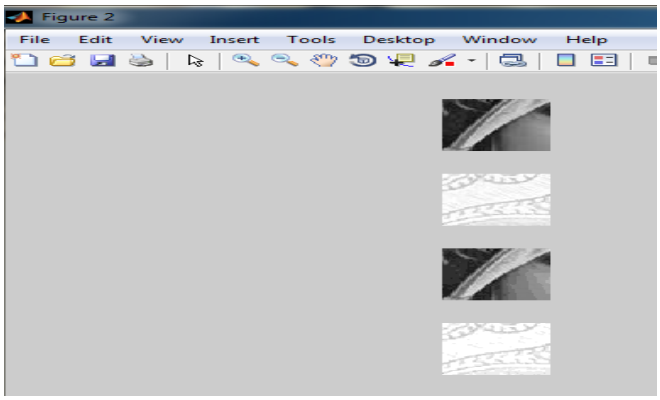
Original image before applying watermark on it

5.2 Extraction Algorithms

In this algorithm please temporary array is chosen in which value of lsb of host image is put and its replace with msb and lsb is made zeros of host image.

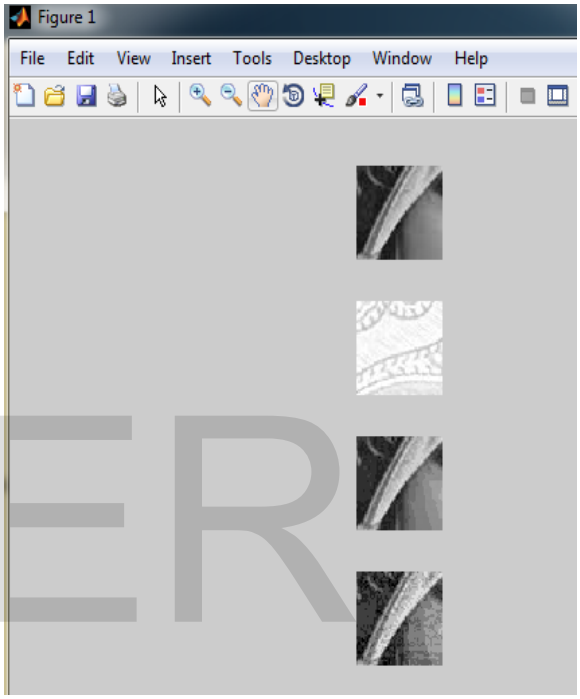
6 Experiments and Results

Here simple Lena's gray scale image is taking of size 157 kilobytes and then it's cropped and watermark is inserted in it of according size. Then you can see less distortion is produced. And we can easily extract watermark. This is figure from mat lab tool in which watermark is embedded in it



6.1 Change in pixel values

By changing value of msb in pixel lot of distortion will occur in images and output will be shown as: so it shows we can't change the msb value. As lsb has least significant value it has to be swapped: This is another figure from mat lab tool while distorting msb.In it watermark image is not extracted, cover image will be obtained in distorted form



7Conclusion

This paper proposed a new lsb technique with it combination of lsb with msb, which is considered as a desired approach. This approach also shows number of other approaches; by changing pixel value and comparing it with other lsb technique. It shows we cannot change the msb value of origin al.In the future we can make it resistant to various other attacks.

7.1 References:

[1] *Cramer C. (2005),* About Digital Watermarking. *From* http://www.willamette.edu/wits/idc/mmcamp/watermarking.htm. 2005

[2] Gulati, K. (2003), Information Hiding Using Fractal Encoding.

Thesis for master degree, Mumbai, India.
[3] Mandhani, N. K. (2004), "Watermarking Using Decimal Sequences", Master thesis submitted to the Graduate Faculty of
The Louisiana State University, India.
[4] Katzenberg, S. and Petitcolas, F.A.P., (2000). Information Hiding techniques for steganography and digital watermarking.Artech House Publishers.
Nagra, J., Thomborson, C. and Collberg, C. (2002), a functional
Taxonomy for software watermarking, in M. Oudshoorn, ed., `Proc.
25th Australasian Computer Science Conference 2002', ACS, pp.
177-186.
[5] Bhatnagar, G. and Raman, B. (2008), A new robust reference
Watermarking scheme based on DWT-SVD, Elsevier B.V. All rights
Reserved.
[6] Luo, H, Chu, S. H. and Lu, Z. M. (2008), Self Embedding Watermarking Using Half toning Technique, Circuits Syst Signal
Process (2008) 27: 155–170
[7] Yang, W. C., Wen, C. Y. and Chen, C. H., (2008), Applying
Public-Key Watermarking Techniques in Forensic Imaging to
Preserve the Authenticity of the Evidence. Springer-Verlag Berlin
Heidelberg 2008.
[8] 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
[9]Lee, G. J., Yoon, E. J. and Yoo, K. Y. (2008), "A new LSB based
Digital Watermarking Scheme with Random Mapping Function", in
2008 IEEE DOI 10.1109/UMC.2008.33
[10]Titty, T., Steganography: Reversible Data Hiding Methods for
Digital Media. Bachelor project
[11]Tickle, A., Rankin, G., Schyndel, R. V., Ho, W., Mee, N., AND Osborne, C. 1993. Electronic watermark. In Proceedings of DICTA.666–672.
[12]Kurah, C. AND McHugh's, J. 1992. A cautionary note on image downgrading. In Proceedings of the IEEE Computer Security Applications Conference. Vol. 2. IEEE Computer Society Press, Los Alamitos, CA, 153–159.
[13]Zheng, D., Liu, Y., Zhao, J. and El Sadden, A., (2007), a Survey of RST Invariant ImagWatermarking Algorithms, ACM