ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Gray Scale Image Watermarking using LSB Modification

Jobin Abraham
Research Scholar,
M.G University, Kerala, India
jnabpc@gmail.com

Abstract: This paper proposes a method for watermarking gray scale images in spatial domain by modifying the least significant bits in the image. After the embedding process we get the watermarked image with hidden information that proclaims its ownership details. Data to be embedded is integrated in the image selectively using a rule that sets or resets the LSB's of the image pixels. Since in this method, the pixels are modified slightly the watermarking remains imperceptible and watermarked image is nearly indistinguishable from the original image.

Keywords: digital image watermarking, LSB modification, watermark, embedding, extraction, psnr.

I. INTRODUCTION

The data in digital formats can be easily copied and modified when compared to analog counterparts [1]. Today, Internet is the gateway for many e-commerce applications, content-on-demand services, social networking and more. The data's that are transferred via Internet is always at the risk of being stolen and reused without any proper permission from their actual creator or the publisher. These concerns have lead to the research and development of robust watermarking techniques that are able to conceal the watermark information from the unauthorized users attempting to modify and manipulate the original contents.

Digital watermarking is a technique used for protecting the ownership rights [2][3]. A variety of algorithms are available for ownership information integration. Watermarking methods can be broadly classified as [4]:

a. Spatial domain methods and
b. Transform domain methods.

In spatial domain, watermark integration is done by modulating the intensity of certain pixels in the host image. Histogram based methods [6-9] and least significant bit (LSB) replacement methods [10] are two popular methods under spatial domain watermarking techniques. In LSB methods, the watermark is embedded in the least significant bits (LSB) of the original image. On the other hand, Transform domain methods widely uses DCT [12] or DWT [13-14] transforms for selecting the coefficients whose magnitude is then modified in some specific way to contain the watermark information.

A. Digital Watermarking Classifications:

Watermarking, in general can be classified as Visible or Invisible based on the perceptibility of the hidden watermark in the host media. Visible Watermarking is visible to human eyes and they provide a means for overt assertion of ownership rights. Invisible watermarks are imperceptible to the viewers and they provide means for covert protection of rights.

Watermarking is also classified into Fragile or Robust watermark. Robust watermarks are designed to withstand degradations or attacks on watermarked images. Fragile watermarking however is broken or lost when watermarked images are subject to any intentional or even unintentional attacks [11]. Fragile watermarks, hence is widely used to verify the content integrity or as a tool for tamper proofing.

B. Features of the Proposed Method:

Most desirable features of Watermarking are robustness, imperceptibility, reversibility and good embedding capacity [15]. The proposed method, delivers many of the desirable features as low noise distortions, fair computation speed, high psnr etc.

a. Blind - Most methods need the original no watermarked image during the watermark extraction stage. In blind methods, extraction of embedded of watermark from the watermarked image do not require the original image.
b. Low computational cost – the computational time consumed for watermarking process is low as the proposed method is less complex and performs the watermarking in spatial domain.
c. High PSNR – distortions are kept as low as possible. The experimental results exhibits very good signal to noise ratios.
d. Imperceptibility – only the least significant bit is altered to represent the watermark; no major modification to the content takes place during the process of watermarking.

In this paper a watermarking algorithm that embeds the information signal in accordance with the statistical characteristics of the gray scale image is discussed. Section II outlines the method proposed, section III gives the details on experimental results observed and section IV includes the inferences and conclusion.

II. THE METHOD

The basic principle of this scheme is based on the comparison between two pixels grouped in as a pair based on a specific rule. The least significant bits of the pixels paired are then set or reset in a specific fashion to represent the information contained in the watermark bit. For embedding the watermark, a key is also used which is a representative value that specifies the step size used for selecting the subsequent pixel couples. Key thus can be a real number such as 4 or 8. This key is also needed during the detection stage for extraction of watermark.

A. Embedding Algorithm:

Steps for watermark insertion are outlined below:

a. Input the host image, I, let the size be n X n.
b. Compare any two non overlapping pixels in pairs, say (I(i, j) and I(j, i)).

c. Get $w_{k,}$ the watermark bit. For each paired bins (x, y) and w_k the following rule is applied for embedding.
d. i .if $w_k = 1$, set x and y to Even, by modifying LS
   ii. if $w_k = 0$, set x and y to Odd, by modifying LSB
e. Next, w_k and pixel pair (I(i, j+s) and I(j+s, i)) is chosen.
f. Repeat process from step 4.
g. End when all paired host image pixels are marked.

The pixels from host image are coupled as per the rule outlined above and then compared for even or odd pairs based on the watermark bit to be integrated. A step, s, may be employed which in turn is based on the payload of the watermark. If more watermark bits have to be integrated the step s has to be lowered accordingly to include more number of ready pixel pairs for watermarking. However, smaller the step size, greater will be the noise introduction and so will exhibit poor visible qualities.

B. Extraction Process:

Watermark extraction is the process that is carried out whenever the ownership rights or the content integrity has to be ensured. If the original owner is able to generate the watermark containing the ownership information from the suspected image he can establish that the digital document rightfully belongs to him. The watermarked image and the decoding algorithm are needed for the process of watermark extraction. As this method does not require the original image as one of the input, this process qualifies to be a blind Watermarking system.

Steps for watermark extraction:
a. Input the watermarked image, I'
b. Pair the pixels, as done while embedding,
   here as (I(i, j) and I(j, i)).
c. For each pair (x, y) apply the following rule for watermark extraction.
d. if (x , y) pair is Even , $w_k = 1$
   if (x , y) pair is Odd, $w_k = 0$.
e. Find the next watermark containing pairs based on the key, s.
f. Repeat process from step 4.
g. End, when all watermarked image pixels are scanned.

III. EXPERIMENTAL RESULTS

The figure.1 shows the image I used during the experimentation for implementing the proposed algorithm. Also shown is the watermark w, embedded into the image I and the resultant watermarked image I'. During the watermark extraction stage, the embedded watermark is successfully regenerated from the watermarked image I'. The extracted watermark is shown in the figure 1.d.

The histogram distribution of the images, I and I' are also shown in figure 2. It can be observed that the histograms of the original image and watermarked image are similar to a great extent; this testifies the data hiding ability of the method used.

Experimental results after watermark insertion for different payloads of watermark is shown in Table.1. A higher PSNR ensures the watermarked image is not significantly distorted from the original.

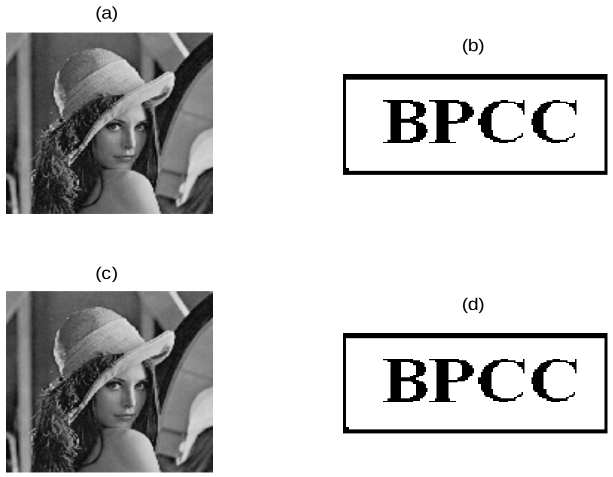

Figure 1. a) Original Lena image I. b) Watermark w.
c) Watermarked Image I' d) Extracted watermark from image in c.

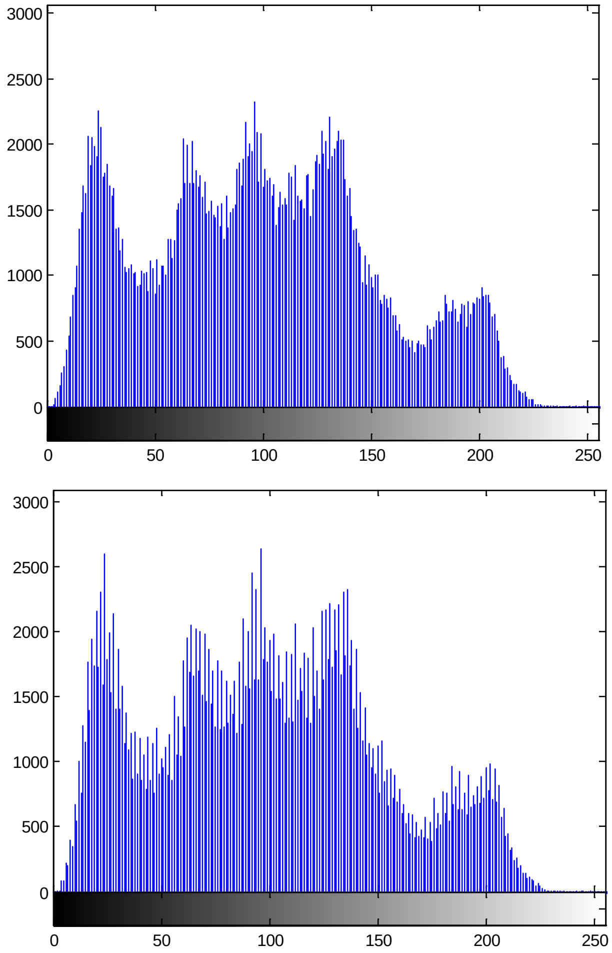

Figure 2. a) Histogram of the image I in fig.1
b) Histogram of watermarked image I'

Table 1. Experimental results for MSE and PSNR measurement

Image	*Bits embedded (size)*	*MSE*	*PSNR*
Lena Size:512X512	32512	0.13	57.12
	16128	0.06	60.17
	13260	0.05	61.02
	10856	0.04	61.91
	7936	0.03	63.28

IV. CONCLUSIONS

Digital Watermarking is a technique for copyright protection of multimedia content. Watermarking has also emerged as a trustable technique for forgery detection in digital multimedia documents that are published and distributed. The spatial domain watermarking schemes used have less computational overhead compared to frequency domain watermarking methods such as DCT or DWT. The method proposed in this paper has delivered acceptable and sound results during the experimental stage. Values for mean square error (MSE) and peak signal to noise ratio (PSNR) are measured. The results indicate the method introduces low noise and lesser visible distortions. The psnr of about 60db delivered by this method is much higher when compared with other proposed methods in the literature. When more of watermark bits are embedded the performance and visual qualities degrades. If the watermark payload chosen is minimal, the watermark will remain imperceptible and also the usability of the original contents is not much affected. The key used during the embedding process serves as an additional level of security against watermark removal attempts by unauthorized persons. The watermark remains undetectable to attackers if the correct key is not applied.

V. REFERENCES

[1] Martin Steinebach, Jana Dittmann, “Watermarking –based Digital Audio Data Authentication”, EURASIP Journal of Applied Signal Processing, 2003:10, 1001-1015.

[2] Shiguo Lian, Dimitris Kanellopoulos, Giancarlo Ruffo, “ Recent advances in Multimedia Information System Security”, PP 3-24, Informatics 33, 2009

[3] Ingemar J.Cox and matt L Miller ,”The first 50 years of Electronic Watermarking”, EURASIP Journal of Applied Signal Processing, 126-132, 2002.

[4] Baisa L Gunjal, R. R Manthalkar, “An overview of transform domain robust digital image watermarking Algorithms”, Journal of Emerging trends in Computing and Information Science, Vol2 PP 37- 42, 2010.

[5] Soo –Chang Pei, Yi-Chong Zeng, “Hiding Multiple Data in Color Images by Histogram Modification”, Proceedings of 17th International Conference on Pattern Recognition 2004.

[6] Zhicheng Ni, Yun-Quing Shi, Nirwan Ansari, Wei Su, “Reversible Data Hiding ”, IEEE Transactions on Circuits and Systems for Video Technology Vol16,2006.

[7] Shumei Wang, Wenbao Hou, “A Robust Watermarking Algorithm based on Histogram”, Proceedings of IWISA 2009.

[8] Chi-Man Pun, Xian-Chen Yuan, “Geometric Invariant Digital Image Watermarking Algorithm Scheme Based on Histogram in DWT Domain”, Journal of Multimedia, Vol.5, No.5, Oct2010.

[9] E.Chrysochos, V .Fotopoulos, A.N Skodras, M.Xenos, “Reversible Watermarking Algorithm based on Histogram Modification”, 11th Panhellenic Conference in Informatics.

[10] G. RoselineNesa Kumari, B.Vijayakumar, L.Sumalatha, Dr.V.VKrishna, “Secure and Robust DigitalWatermarking on Grey Level Images”, International Journal of Advanced Science and Technology, Vol11, October 2009.

[11] S. Voloshynovskiy, S.Pereira, T.Pun, “Attacks on Digital Watermarks: Classification, Estimation based Attacks and Benchmarks”, IEEE Communications Magazine, Vol.39, pp115-126, 2001.

[12] Patrick Lam, Orion Winkelmeyer,” Watermarking Technologies-Analysis and Design Report”, 2005.

[13] P. Meenakshi Devi , M. Venkatesan and K. Duraiswamy, “A Fragile Watermarking scheme for Image Authentication with Tamper Localization Using Integer Wavelet transform” , Journal of Computer Science 5(11) PP831-837, 2009.

[14] Kamran Hameed, Adeel Mumtaz and S.A.M Gilani, “Digital image Watermarking in the wavelet transform domain”, World Academy of Science, Engineering and Technology 13 2006.

[15] Jen Bang Feng, “Reversible watermarking: Current Status and Key Issues”, International Journal of Network Security, Vol 2, PP161-171, May 2006.