Watermarking Grayscale Images using Text for Copyright Protection

Jobin Abraham
Research Scholar
M.G University
Kottayam, India

Dr.Varghese Paul
Cochin University
Kochin, Kerala
India

ABSTRACT
This paper proposes a novel method for watermarking gray scale images in spatial domain by modifying the least significant bits of the pixels in the image. The embedding process creates a watermarked image with hidden information that in future can proclaim its ownership details. Data to be embedded is integrated in the image selectively on a subset of pixels using a rule that replaces the LSB's of the image with the watermark signal bits. The method is successful in generating marked copies of the original image with high PSNR value and good visual qualities suitable for distribution via any media or publishing in Internet.

Keywords
digital watermarking, spatial domain, gray scale images, LSB Replacement, watermark, embedding, extraction, mse, psnr.

1. INTRODUCTION
Usage of digital data formats offers many advantages as easy generation, modification, storage and transmission of information. The very same factors also favor illegal attacks as editing and alterations on to the original digital content [1]. Such unauthorized reproduction and redistributed of information can be extremely costly for the production companies considering the data productions costs and other revenue losses.

Digital multimedia data published and distributed especially via Internet is faced with two major concerns; one is with the ownership protection of the actual creator of the document and the other is the preservation and verification of the contents integrity. It must be possible for the original document owner to identify and prove with sufficient supporting evidences whenever the contents are tampered and used against the will and interests. Copyright protection of digital documents can be made possible if they are watermarked prior to distribution. Digital watermarking can be described as the process of embedding the owners' unique signature information as his logo or a text string imperceptibly in the digital multimedia content [2]. Digital watermarking is an emerging area and has immense application in digital world that includes applications as digital imaging systems, storage databases, communication systems and many more [3].

1.1 Related works
Digital watermarking is an area of interest for researchers as security in digital world will always be a prime concern. A number of algorithms and schemes were proposed in the recent years to effectively address these concerns. Watermarking can be done using: Spatial domain methods and Transform domain methods [4, 5]. Histogram based methods [6, 7] and least significant bit (LSB) replacement methods [8] are the two most common techniques under spatial domain watermarking. Transform domain uses DCT (Discrete Cosine Transform) [9, 10], DFT (Discrete Fourier Transform), or DWT (Discrete Wavelet Transform) [11, 12] transforms for watermark embedding.

Spatial methods based on LSB replacement usually adopt two common procedures for watermarking. One is, use of a binary image as watermark. The 1's and 0's taken from the binary image is embedded by addition to the host image pixels or by replacement of least significant bits. And in second, a grayscale image is used as the watermark. The most significant bits, usually four bits, separated from the watermark are placed instead of the four least significant bits on the chosen subset of pixels in the original image. Doraiswamy presented an invisible and blind watermarking scheme for copyright protection [13]. A binary image is used as watermark data and its pixels are embedded in the host image. Two distinct mathematical operations were performed for embedding the watermark bits. On implementation, this algorithm yielded a PSNR value in the range 40-50dB when experimented with various known grayscale images. Mona M describes a scheme that utilizes an image watermark. The method replaces the least significant bits with the most significant bits from the watermark signal [14]. The PSNR of the marked image is 27.9dB. Roseline NesaKumari et al [15] propose a grey level modification watermarking system. This method embeds a single bit in least significant bit of an image pixel. For determining a suitable window for embedding, the entire image of the size n x n, consisting n^2 pixels is sorted. The characters from the text are then embedded bit by bit into the sorted pixel array.

Most methods found in literature are highly complex and involve multiple execution stages. In this paper, we describe a novel scheme for text integration in grayscale images to create a watermarked copy of the original image. This spatial domain watermarking replaces two bits of the image pixels with bits from the watermark. In Section II, the algorithm of the proposed method is outlined, section III gives the details of experimental results obtained and section IV is the inferences and conclusion of the study.

2. THE METHOD
2.1 Features of the Proposed Method
The watermarking method proposed has many superior qualities and delivers most of the desirable features as low noise distortions, fair computation speed, imperceptibility [16] etc. Significant features of the method include the following:

- Imperceptibility – only the least two significant bit of the selected image pixels are altered to represent the watermark; hence no major visible modification to the content takes place during the process of watermarking.
- Effective for images of any size - Works equally well with small images and any m x n asymmetric sized images
- Robust against geometric attacks - as cropping and drawing. The watermark effect is localized and is not spread across all the pixels in the image. Watermark extraction is hence possible except in extreme cases of attacks.
- High PSNR – distortions are kept low. The experimental results shows very good signal to noise ratios as high as 60dB.
- Higher computational speed – The watermarking process is not complex and the computational time consumed for generation of watermarked copy is low.
- Blind - In blind watermarking methods, extraction of embedded watermark from the watermarked image do not require the original image.

2.2 Watermark Embedding Process

The watermarking algorithm is applicable on any m x n sized image. A grayscale intensity value is defined as the lead pixel value. Around this, a 2x2 block is imagined for embedding watermark bits. Selection of this lead pixel block value is important as embedding capacity is dependent on its frequency. Peak histogram bin value is a natural choice for this selection. Characters from the text watermark are converted into an equivalent binary code. These bits are then substituted with the bits in the LSB locations across the pixels in the block considered. Detailed steps for watermark insertion are outlined below:

1. Input the host image, I of any size m x n.
2. Find an eligible key pixel around which the watermark bits can be embedded. Select the pixel value that has maximum representatives in the image I. Let grayscale intensity value of that is mgv.
3. Choose a text or character string as the watermark.
4. Convert the characters into corresponding seven bit binary ASCII code. Let the binary bits be b_6b_5-b_0.
5. Consider a 2X2 block at positions in image I with a pixel I(i, j) == mgv, in intensity.
6. Select the image pixels in three neighboring positions I(i+1,j), I(i,j+1) and I(i+1,j+1).
7. Embed by replacing two bits in pixels selected with bits from the watermark.
   i. Embed bits b_1b_0 of watermark in I(i+1,j).
   ii. Embed bits b_3b_2 of watermark in I(i,j+1).
   iii. Embed bits b_1b_0 of watermark in I(i+1,j+1).
   iv. Assume last bit b_6, which always a 1, is embedded in I(i, j).
8. Before integrating the modifications, check if any new pixel value in block equals mgv.
9. If yes, skip the block, as any overlap with mgv value can affect the watermark extraction process. Else, enforce the modifications to I.
10. Reset I(i, j) slightly, say by mgv-1.
11. Select the next eligible block to embed the next watermark character by repeating from steps4
12. Store the watermarked image I_w.

2.3 Watermark Extraction Process

Watermark extraction stage requires the watermarked image and lead pixel value, used in the Embedding process (mgv), around which the blocks were constructed during the embedding process. Extraction is straight forward and involves the steps outlined below:

1. Input the watermarked image Iw. Let the size be m x n.
2. Locate every pixels I (i, j) == mgv in intensity.
3. Construct a 2X2 block around I (i, j).
4. Read I(i+1,j), I(i,j+1) and I(i+1,j+1)
5. Check if any of above equals mgv, if yes jump to step3 as the block was unused. Else continue.
6. Read the least significant two bits from the pixels. Bits b_1b_0 from I(i+1,j), b_3b_2 from I(i,j+1) and b_5b_4 from I(i+1,j+1).
7. Built the code by combining bits b_6b_5-b_0., with b_6=1.
8. End if i=m and j=n for the image Iw. Else repeat from steps 2, for retrieving the next character
9. Output the array of watermark strings.

3. EXPERIMENTAL ANALYSIS

The algorithm described in section II is implemented and experimented on different known grayscale images. The text string 'BPCC' is used as watermark. The characters from the string are converted into their corresponding binary equivalent of ASCII code. The bits from character are then embedded into three host image pixels around a lead pixel per character. For watermark extraction stage the key information required is the pixel value used as key, around which the watermark bits are placed. Hence it is important that during embedding the unused key pixel values are slightly modified to avoid error during extraction. The figure.1 shows various images, I, upon which the algorithm was implemented and their corresponding watermarked copy Iw. Values for mean square error (MSE) and peak signal to noise ratio (PSNR) are measured. Table.1 lists all the experimental results obtained for variously sized images. The best results was obtained for peppers image where the embedding process could integrate as many as 2800 characters and yet yielded a PSNR of 56.5 dB, which is far superior to many other watermarking schemes. The quality of watermarked image can be compared with that of the original image using PSNR (Peak Signal to Noise Ratio). A higher PSNR ensures the watermarked image is not significantly distorted from the original.

a) Original Image

b) Watermarked Image

c) Original Image

d) Watermarked Image

e) Original Image

f) Watermarked Image

Figure 1. Watermark Embedding Process. Original input image I, Watermarked Image Iw

Table 1. Experimental results for MSE and PSNR measurement

Image	**Image Size**	**Characters Embedded**	**No. of bits Embedded**	**PSNR** (dB)	**MSE**
Lena	512X512	1246	8722	61.26	0.05
Cameraman	256X256	540	3780	58.55	0.09
Boy	291X240	1063	7441	55.70	0.18
Peppers	384X512	2789	19523	56.56	0.14

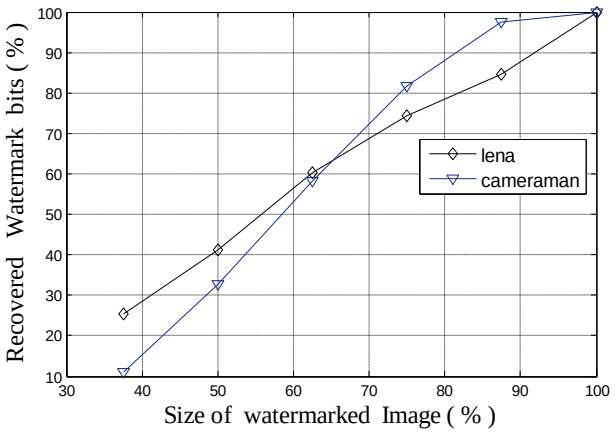

Figure 2: Comparative plotting of Image after cropping attack versus Recovered Watermark Information

The watermarked image was subjected to various geometrical attacks to test the robustness of the proposed method. Tampering by cropping is the most common attack attempted even by naïve users using tools as Adobe Photoshop. The method is found to be extremely robust against cropping, withstanding downsizings up to 65 percent of the image. Figure 2 shows the plot for various dimensions of cropping versus the amount of watermark information successfully retrieved. As the method utilizes selected 2x2 blocks to integrate the watermark meaningful information can be rebuild even after malicious cropping.

4. CONCLUSION

Digital watermarking is a tool that could be effectively used for multimedia copyright protection, authentication and tamper proofing. Digital watermarking is closely related to cryptography. Cryptography is a traditional method used from very ancient days for data protection by hiding the critical information's very smartly from the visibility of the intruders. Digital watermarking, on the other hand, integrates the ownership information into multimedia contents for the purpose ownership identification and establishment.

In the method proposed, a set of pixels that constitute a block jointly share the bits from the watermark. Two least significant bits are replaced. If more than two bits of the original image pixels are replaced it shall adversely affect the visual quality of the watermarked image and thereby degrades the usability of the original contents itself. Values for mean square error (MSE) and peak signal to noise ratio (PSNR) are measured. The results indicate the method introduces low noise and hence ensures lesser visible distortions. The psnr value of about 60dB attained is much higher when compared with any other proposed methods. Also as selected 2x2 blocks are utilized to integrate the watermark; extraction of meaningful ownership information is possible even after multiple cropping attacks on watermarked image.

5. REFERENCES

[1] S. Voloshynovskiy, S.Pereira, T. Pun, Attacks on Digital Watermarks: Classification, Estimation Attacks and Benchmarks, IEEE Communications Magazine, 2001, pp115-126

[2] Shiguo Lian, Dimitris Kanellopoulos, Giancarlo Ruffo, Recent advances in Multimedia Information System Security, Informatics (33) 2009, pp3-24

[3] Ingemar J.Cox and matt L Miller, The first 50 years of Electronic Watermarking, EURASIP Journal of Applied Signal Processing, (2) 2002, pp126-132

[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, (2) 2010, pp 37- 42

[5] Kamran Hameed, A Mumtaz, Gilani, Digital Image Watermarking in the Wavelet Transform Domain, World Academy of Science, Engineering & Technology, (13) 2006, pp 86-89

[6] Zhicheng Ni, Yun-Quing Shi, Nirwan Ansari, Wei Su, Reversible Data Hiding, IEEE Transactions on Circuits and Systems for Video Technology (16) 2006, pp 354-362

[7] Shumei Wang, Wenbao Hou, Proceedings of International Workshop on Information Security and Application , A Robust Watermarking Algorithm based on Histogram, 2009, pp 453-456

[8] M.Hamad Hassan, S.A.M Gilani, A Fragile Watermarking scheme for Image Authentication, World Academy of Science, Engineering & Technology (19) 2006 pp39-43

[9] Tribhuwan Kumar Tewari, Vikas Saxena,"An Improved and Robust DCT based Digital Image Watermarking Scheme',International Journal of Computer Applications (0975 – 8887)Volume 3 – No.1, page(s): 28- 31 June 2010.

[10] Sami Baba, Lala Krekor, Thawar Arif, Zyad Shaaban, Watermarking Scheme for Copyright of Digital Images, International Journal of Computer Science and Network Security, Vol.9(4), 2009.

[11] Ali Al Haj, Combined DWT-DCT Digital Image Watermarking, Journal of Computer Science, 3(9) 2007 pp740-746

[12] Chi-Man Pun, Xian-Chen Yuan, Geometric Invariant Digital Image Watermarking Algorithm Based on Histogram in DWT Domain, Journal of Multimedia, 5 (2010), pp434-442

[13] Dr.Doraiswamy M.A, A Novel Invisible and Blind Watermarking Scheme for Copyright of Digital Images, International Journal of Computer Science and Network Security, Vol.9(4), 2009, pp71-78.

[14] Mona M El-Ghoneimy, Comparison between two Watermarking Algorithms Using DCT Coefficient and LSB Replacement, Journal of Theoretical and Applied Information Technology, 2008, pp132-139

[15] G. RoselineNesa Kumari, B.Vijayakumar, L.Sumalatha, Dr.V.V Krishna, Secure and Robust Digital Watermarking on Grey Level Images, International Journal of Advanced Science and Technology, (11) 2009, pp1-8

[16] Jen Bang Feng, Lin, Tsai, Yen-Ping Chu, Reversible watermarking: Current Status and Key Issues, International Journal of Network Security, Vol2 2006, pp161-171