ISSN No. 0976-5697

Volume 2, No. 6, Nov-Dec 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Imperceptible LSB Based Image Watermarking Algorithm

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

Abstract: The main objective of digital watermarking is copyright protection of multimedia documents. A simple and fast blind watermarking algorithm applicable to any grayscale image is proposed in this paper. The watermark is embedded in the least significant bits of the original image. The algorithm is robust to watermark removal attacks due to secure selection of criteria for watermark insertion and bit position in a pixel. The method guarantees low noise insertion while embedding the watermark**.** The original image undergoes no visible degradations. Hence the watermarked image is also appealing to HVS.

Keywords: image watermarking, watermark signal, embedding, extraction, noise, psnr.

I. INTRODUCTION

Digital image watermarking is a tool for protecting the ownership rights of digital documents. Any digital document including text, image, audio or video can be watermarked. Ownership details are integrated into the document imperceptibly for the purpose of owner identification. The unique information embedded can be the owners' logo, name or other details. The watermarked copies can then be used for distribution instead of the original copy. As the watermarked copies contain hidden information, when misuses are reported in future, it shall be possible for the actual owner to extract the watermark as a proof for his rightful ownership.

Many have argued that watermarking is same as steganography. Watermarking has strong resemblance to steganography in that a information, i.e. watermark, is hidden into the host media without being visible to viewers. However, the receivers do not extract the integrated information as in steganography. Watermark is extracted by the owner only when false claims or abuses are reported. Steganography is covert communication [1]. In short, the purpose and intension for information integration greatly differs in both cases.

In addition to copyright protection there are many more applications for watermarking. Watermarking is effective for tamper proofing, document labeling, broadcast monitoring and source tracking [2]. Watermarking can be broadly classified into Visible or Invisible, Blind or Non-blind, and Fragile or Robust [2]. Visible Watermarking on images is visible to human eyes and provide means for overt assertion of ownership rights. Invisible watermarks are imperceptible to the viewers and provide means for covert protection of rights. In blind methods, extraction of watermark message from the marked image does not require the original image. However for non-blind methods, watermark extraction is possible only in the presence of the original image. Watermarking can be Fragile or Robust. Robust watermarks are designed to withstand degradations or attacks on watermarked images. A robust watermark should not be lost when any illegal operations as cropping, compression or appending is performed on the image.

Fragile watermarking however is broken or altered when they are subject to attacks.

Watermarking Systems uses different techniques for information integration into the host media. Watermarking techniques can be classified into two as [3]:

a. Spatial domain method
b. Transform domain methods

In spatial domain, watermark integration is done by modulating the intensity of certain selected pixels in the host image. Least significant bit (LSB) replacement methods [4] and Histogram based methods [5] are two popular methods under spatial domain watermarking techniques. Transform domain methods widely uses DCT [6, 7] or DWT [8, 9] transforms for selecting the coefficients whose magnitude is then modified to contain the watermark information.

II. THE PROCESS

A Watermarking system comprises two stages: Embedding and Detection. Watermark embedding process employs an algorithm and a unique watermark for encoding this into the host media.

An image can be represented using intensity values in the range 0-255 for individual pixels. Using this scale, any image can be created by selecting a specific set of values arranged in a two dimensional array of size M x N. In the process of watermarking, the intensity values from the original image are modified by certain levels to integrate the watermark signal as well. This has the effect of noise addition that sometimes may affect the appearance of the image. Hence while embedding watermark bits it must be ensured that addition will affect the quality of the image and that the modifications are spread across the area of the image. If the effects of watermarking are localized to some corners, the visibility features of the image will be adversely affected and many times these effects will be prominent in certain portions. As the human eyes are very sensitive, if the watermarking effects are too less in some portions compared to the other portions within the image, the variations may standout distracting the eyes. To make the watermarked image visibly appealing to HVS (Human Visual System) a method for calculating the hit ratio is devised. Based on this value a pixel within a block may be selected or discard during watermarking.

A pixel from the host image is watermarked based on the decision rule [(bm: 0/1), bx]. Here, bm is a bit position chosen from MSB and bx is a bit position taken from LSB for a pixel. The value at bm can be chosen, 0 or 1, as desired by the encoder. One of the bits from four LSB, bx, is used as bit location for watermark bit embedding. Before introducing the change, a 3X3 block is considered around the pixel which is to be watermarked. The decision rule defined is applied to all the pixels in the block selected to determine how many eligible pixels are present. This count is used to calculate the ratio

$$hr = \frac{c}{n} \qquad ?\,?\,?\,?\,?\,?\,?\,1\,?$$

In the above equation, c is the count of eligible pixels in a block of n = 3X3. A range 0.3 to 0.7 is considered good enough for enforcing the watermark, as this will be insensitive to eyes. A lower ratio if used will result in modifications that may get highlighted in the final product. An upper bound value may distort the image as there will be too many altered pixels. Hence a moderate value can be considered as best suit while deciding to watermark or not.

A. The Algorithm:

Steps for watermark insertion are outlined below:

Step 1: Input the host image, I, size be i = M and j = N.
Step 2: Input the binary watermark, w_k, k = 1 to m.
Step 3: Choose an appropriate decision rule, [(bm: 0/1), bx], for watermarking
Step 4: consider a I(i, j), construct a 3X3 block around this pixel I(i, j).
Step 5: Calculate the ratio, *hr*
Step 6: If *hr* within a predetermined acceptable limit, embed the watermark w_k.
Step 7: Select next I (i, j), w_k and repeat step 4.
Step 8: End when all pixels in I are marked.
Step 9: Output the watermarked image I'.

Consider the example illustrated below. A portion of the image may be assumed as shown. The pixel in interest is the one with intensity value 117. The others form a 3 X 3 block around the selected pixel. The decision rule [(bm: 0/1), bx] is assigned the values [(7:1), 2] and hr value be selected as (0.3>hr<0.6). As per the criteria, three positions are eligible to carry the carry the watermark and the calculated hr ratio, 0.33, is also found acceptable. Hence the algorithm will choose the pixel 117 to represent the watermark in its second LSB bit. Shown below is the resultant values after the watermarking process for $w_k = 1$.

Input: Host image block

$$\begin{bmatrix} 34 & 126 & 97 \\ 48 & 117 & 54 \\ 182 & 156 & 62 \end{bmatrix}$$

Binary form of the Host image block

$$\begin{bmatrix} 00100010 & 01111110 & 01100001 \\ 00110000 & 01110101 & 00110110 \\ 10110110 & 10011100 & 00111110 \end{bmatrix}$$

Output: Watermarked block

$$\begin{bmatrix} 00100010 & 01111110 & 01100001 \\ 00110000 & 01110111 & 00110110 \\ 10110110 & 10011100 & 00111110 \end{bmatrix}$$

B. Watermark Extraction:

The decoding algorithm retrieves the watermark w from I'. The techniques that do need the original image while decoding are said to be blind methods. The proposed is a blind method which accepts I' as input and outputs the watermark signal.

Step 1: Input the watermarked image, I'.
Step 2: Apply the rule adopted in embedding for locating the watermarked pixels.
Step 3: Read the bit from position bx from identified I'(i, j).
Step 4: Increment i, j for i =2 to M-1and j =2 to N-1. End when pixels are scanned.
Step 5: Else, repeat from Step 2.
Step 6: Output the watermark, w.

III.EXPERIMENTAL RESULTS

The figure.1.a shows the image I used for implementing the proposed algorithm. The watermark w, which is used for embedding into the image I is in figure 1.b. After the process of watermark embedding, the resultant watermarked image I' is in figure. 1.c. During the second stage, watermark extraction stage, the embedded watermark is successfully regenerated from the watermarked image I'. The extracted watermark is shown in the figure 1.d. Figure.2 shows more examples.

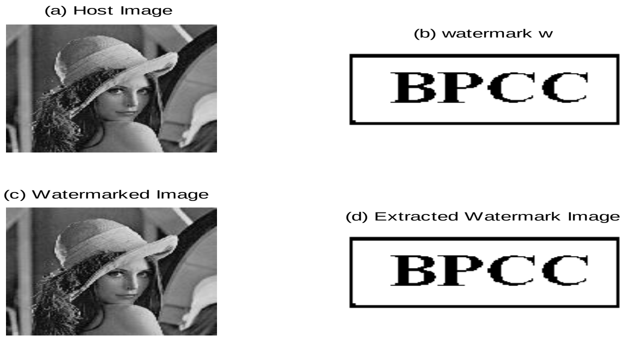

Figure 1. Watermark Embedding Process

The quality of watermarked image can be compared with that of the original image using PSNR (Peak Signal to Noise Ratio). To calculate PSNR, mean squared error (MSE) of the watermarked image is to be computed as

$$MSE = \frac{\Sigma\,(\,I(i,j) - I'(i,j)\,)}{N^2} \qquad ?\,?\,?$$

The summation is over all positions i, j = 1 to N. The root mean squared error (RMSE) is the square root of MSE. PSNR in decibels (dB) is then computed using

$$PSNR = 20\log_{10}\left(\frac{255}{RMSE}\right) \qquad ?\,?\,?$$

Table.1 shows the experimental results for PSNR and MSE after watermark insertion on different images.

Table 1. Experimental results for MSE and PSNR measurement

Image	*Image Size*	*No. of watermark bits Embedded*	*PSNR (dB)*	*MSE*
Lena	512X512	17699	62.92	0.033
Deer	939X953	56484	63.21	0.031
Bridge	751X749	22987	64.89	0.021

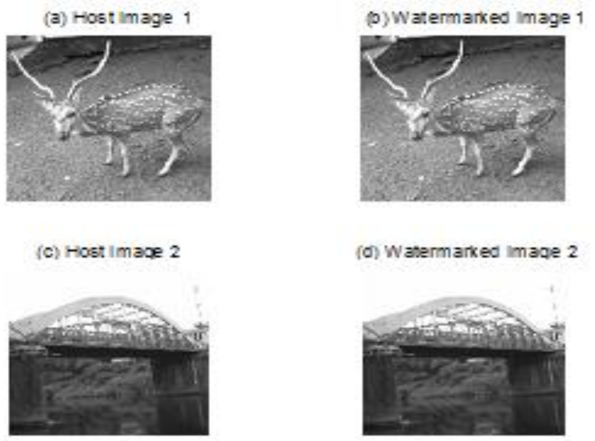

Figure 2. Watermark Embedding Process. Original input image I, Watermarked Image I’

A lower value for MSE means lesser error during processing, and as seen from the inverse relation between MSE and PSNR. Also a higher PSNR ensures the watermarked image is not significantly distorted from the original. Logically it means that the ratio of Signal to Noise is higher. As a PSNR of above 60dB is resulted during experimental analysis watermarked images of good quality can be generated by our method.

IV. CONCLUSION

A blind imperceptible watermarking algorithm which is applicable to any grayscale image is proposed. The strength of an algorithm depends on its ability to withstand watermark decoding or removal attacks attempted by the illegal users. This method is robust in the sense that watermark detection is difficult to attackers. The key used in various combinations for different images during watermark embedding makes the algorithm stronger. The method is effective for images that are to be published via the Internet. Documents and other resources are downloaded and widely reused after some minor modifications even by naïve users. The watermarking algorithm is efficient for detecting such misuses.

The method also guarantees low noise insertion while watermarking. As we have a PSNR of above 62dB, watermarked images of good quality and visual features are generated by the proposed method. The capacity, i.e. the number of watermark bit embedded, is also higher compared to any other method. As only one bit from LSB position is affected during the process of watermarking, no significant distortion is introduced. In addition, hit ratio used ensures that the watermark will remain imperceptible on host image.

V. REFERENCES

[1] Frank Hartung, Martin Kutter," Multimedia Watermarking Techniques", Proceedings of IEEE, Vol 87, 1999 .

[2] Vidyasagar M Potdar, Song Han, Elizabeth Chang," A Survey of Digital Image Watermarking Techniques " IEEE International Conference on Industrial Informatics, 2005

[3] 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.

[4] 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

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

[6] Tribhuvan Kumari, Vikas Saxena, "An Improved Robust DCT based Digital Image Watermarking Scheme", International Journal of Computer Applications, 2010, pp. 28-31.

[7] Neminath Hubbali, Kanyakumari D.P, "Novel DCT based Watermarking Scheme for Digital Images", International Journal of Recent Trends in Engineering, 2009.

[8] Yiewei Wang, John F. Doherty, Robert E Van Dyke, " A Wavelet based Watermarking Algorithm for Ownership Verification of Digital Images", IEEE Transactions on Image Processing, Vol.11,2002.

[9] P. Ramana Reddy, V.N.K Prasad, D.Sreenivasa Rao, " Robust Digital Watermarking of Color Images under Noise Attacks", International Journal of Recent Trends in Engineering, 2009.

