A WAVELET BASED DIGITAL IMAGE WATERMARKING SCHEME USING LSB TECHNIQUE

Ritu Chhikara
Department of Computer Science and Applications, Chaudhary Devi Lal University, Sirsa, India

ABSTRACT:
In this present era of information technology and rapid technological advancements, the Internet is increasingly playing a role in the offering of multimedia resources through digital networks. This poses a threat of unauthorized possession and usage of digital material. An additional threat is the illegal tampering and modification of digital material. The need for techniques to protect the copyright of digital material thus arises. The present challenges and factors that need to be taken into consideration are the protection of ownership rights against illegal activities in such a manner that the ownership of the digital material is beyond dispute. The previous literatures used least significant bit technique directly into image pixels, this degrade the perceptibility of image and also decreases the security of watermarking scheme. It is better if one put the secret message using LSB technique in any other domain e.g. in spatial domain, so that, no one can modify or alter the original message information. Furthermore, to increase the security of secret message, message should be encoded before embedding it in cover image. The Huffman coding used in proposed work in order to increase the security of secret message by encoding the message into Huffman code before embedding it using least significant bit in spatial domain.

Keywords: Watermarking, Huffman Code, LSB, METLB, Wavelet Transformations, PSNR, MSR, WPSNR.

[1] INTRODUCTION

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should [1], but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and
for banknote authentication. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied.

One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

Every watermarking system consists of two different units:
- The watermark embedding unit and
- The watermark detection/extraction unit.

Both units can be considered as separate processes.

In the extraction/detection process a detector function takes an image whose ownership is to be determined. The image can be a watermarked or an un-watermarked image. In a general case, it can be also an altered image. The detector function either recovers a watermark we from the image, or checks the presence of the watermark in a given watermarked image. In this procedure the same key is used.

In the evaluation of the performance of the watermarking scheme, for robustness validation this work use the mean square error (MSE) between the original and watermarked images, respectively, peak signal to noise ratio (PSNR), correlation factor between input and output watermarked image and Weighted peak signal to noise ratio WPSNR.

The previous literatures used least significant bit technique directly into image pixels, this degrade the perceptibility of image and also decreases the security of watermarking scheme. It is better if one put the secret message using LSB technique in any other domain e.g. in spatial domain. So that, no one can modify or alter the original message information. Furthermore, to increase the security of secret message, message should be encoded before embedding it in cover image. The Huffman coding used in proposed work in order to increase the security of secret message by encoding the message into Huffman code before embedding it using least significant bit in spatial domain.

[2] RELATED WORK

As data protection and copy right issues are very important in digital world, a lot of work has been done by different researchers in this field of image processing with watermarking from
previous years. Various proposals [3, 4, 5, 6, 7, 8, 9] have been made to give a clear insight view of watermarking schemes. Dorairangaswamy et al. [3] gives innovative invisible and blind watermarking scheme for copyright protection of digital images with the purpose of defending against digital piracy. It describes watermarking scheme as binary watermark image is invisibly embedded into host image for achieving copyright protection. In watermark embedding, every pixel of the watermark image is embedded into the individual blocks of the host image.

Zhang et al. [4] developed a new kind of watermark-inserting and detecting algorithm based on stationary wavelet transform. The encrypted watermarking was transformed to one-dimensional row vector, and the pixel value was sorted. The coefficient of one-dimensional of primitive image of stationary wavelet transformation was sorted too, then inserted sorted watermarking to the sorted low frequency, and turned it to two dimension data. Then the image is reconstructed with coefficients of high-frequency. Finally withdraw the watermarking and obtained the primitive watermarking after the anti-Arnold transformation. Experimental results indicate that this algorithm not only enables the watermarking to have the very good invisibility, but also makes the watermarking have very strong robustness to the general image attacks, such as noise, filter, rotation, compression and so on. Kang et al. [5] proposed digital image watermarking technique for protecting the digital images based on discrete wavelet transform due its excellent spatial localization, frequency spread and multi-resolution analysis similar to human visual system. The method involves a visual watermark (grayscale image) which is transformed using discrete cosine transform for getting low frequency coefficients in frequency domain. The low frequency coefficients of transformed watermark image contain maximum visual data information. Then, the original image is transformed using the discrete wavelet transform and watermark is embedded by modifying the coefficients of LL bands with appropriate imperceptibility and robustness.

Chandra [6] described overview of digital image watermarking technique and proposed an algorithm for copy write protection of digital images in DCT domain. It described Digital watermarking as the process of embedding a certain piece of information, technically known as watermark into multimedia content including text documents, images, audio or video streams, such that the watermark can detected or extracted later to make an assertion about the data. This algorithm is also implemented using MATLAB. Yang et al. [7] presented a scheme of digital image watermarking using iterative blending based on discrete wavelet transform (DWT). The method is based on decomposing host image and watermarking image by DWT, and then embedding the significant coefficients of watermarking image into the same part of host image using iterative blending. The watermarking won't be visible and can be extracted later.

Dinghui et al. [8] combined the scrambling technique of digital images and discrete wavelet transform to meet well the requirements of transparency, robustness, and security of digital image watermarks at one time, the watermarking technique of digital images in wavelet transform domain has been seriously studied according to the basic characteristic of human visual system. Singh et al. [9] gives a brief overview of digital image watermarking techniques in spatial and frequency domain, advantages of frequency domain over spatial domain techniques and proposed a watermarking algorithm in frequency domain by using the discrete wavelet transforms.
A WAVELET BASED DIGITAL IMAGE WATERMARKING SCHEME USING LSB TECHNIQUE

The previous literatures used least significant bit technique directly into image pixels, this degrade the perceptibility of image and also decreases the security of watermarking scheme. It is better if one put the secret message using LSB technique in any other domain e.g. in spatial domain. So that, no one can modify or alter the original message information. Furthermore, to increase the security of secret message, message should be encoded before embedding it in cover image. The Huffman coding used in proposed work in order to increase the security of secret message by encoding the message into Huffman code before embedding it using least significant bit in spatial domain.

[3] PARAMETERS USED IN WATERMARKING

In the watermarking the following parameters are used for evaluation of performance of any proposed schemes.

[3.1] Mean squared error (MSE)

MSE is a risk function, corresponding to the expected value of the squared error loss or quadratic loss. The difference occurs because of randomness [10]. In this research work, MSE is used to compute the performance of watermarked image.

If $\hat{Y}$ is a vector of $n$ predictions, and $Y$ is the vector of the true values, then the (estimated) MSE of the predictor is:

$$MSE = \frac{1}{n} \sum_{i=1}^{n} (\hat{Y}_i - Y_i)^2$$

Source-http://en.m.wikipedia.org/wiki/peak_signal-to-noice-ratio

[3.2] PEAK SIGNAL TO NOISE RATIO

The PSNR is most commonly used as a measure of quality of reconstruction in image compression etc. It is most easily defined via the Mean Squared Error (MSE). For two m x n monochrome images $I(x, y)$ and $K(x, y)$, where one of the images is considered a noisy approximation of the other, MSE is defined as:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} ||I(i, j) - K(i, j)||$$

The PSNR in terms of MSE is defined as:

$$PSNR = 10 \cdot \log_{10} \left( \frac{MAX_i^2}{MSE} \right) = 20 \cdot \log_{10} \frac{MAX_i}{\sqrt{MSE}}$$

Source-http://en.m.wikipedia.org/wiki/peak_signal-to-noice-ratio

Here, $MAX_i$ is the maximum pixel value of the image. When the pixels are represented using 8 bits per sample, value of $MAX_i$ is 255.

[3.3] WEIGHTED PEAK SIGNAL TO NOISE RATIO
The weighted PSNR (WPSNR) has been defined as an extension of the traditional PSNR. This allows us to determine the optimal watermark location and strength for watermark embedding stage.

$$WPSNR = 10\left(L_{\text{max}}^2\right)(\text{MSE} \times \text{NVF})^2$$

Source-http://en.m.wikipedia.org/wiki/peak_signal-to-noice-ratio

[4] INPUT DATABASE

The input database images taken for the experimental purpose are Lena, Mandrill, and Barbara along with the single watermark. All images are in bmp format (bitmap image file). Figure below shows the RGB image files for the three input cover images.

[4.1] PROPOSED ALGORITHM

The proposed algorithm is described below:

1. Read Cover Image and Set I=input cover image; 
2. If I is RGB image Then Covert it into Gray scale image  I=rgb2gray(I); 
Else
3. Read secret message Set W=input Secret Message;  
4. Watermarking process for cover image
   Let, dwt2= 2D Discrete Wavelet Transform of a given input value for cover image
   $$(A_i,H_i,V_i,D_i)=\text{dwt2}(I, \text{Wave});$$
   /*Here, $A_i=$approximation coefficients
   $H_i=$horizontal coefficients
   $V_i=$vertical coefficients

Ritu Chhikara
A WAVELET BASED DIGITAL IMAGE WATERMARKING SCHEME USING LSB TECHNIQUE

\[D_i=\text{diagonal coefficients}^*/\]

5. Second Level : Set \( I_{di} = \text{dwt2}(A_i, \text{Wave}); \)
6. Third Level : Set \( S_i = \text{dwt2}(I_{di}, \text{Wave}); \)
7. Let, \( \text{Huff} = \text{Huffman coding of input and Message2bit} = \text{conversion of message into bit sequence} \)
   \( C_t = \text{Huff}(W); \) //\( C_t = \text{Coded text using Huffman encoding Scheme} \)
8. Apply Huffman Coding on input message.
9. Convert message into bit sequence using decimal to binary keyword
   \( \text{Ctb} = \text{Message2bit}(C_t); \)
10. Embedding of watermark text with cover image using LSB technique
    \( \text{Wi} = \text{is watermarked image after watermarking process} \)
12. Watermark Extraction Process
    If noise added through channel
       \( \text{Wi} = \text{Noise(Wi)}; \)
    Else
       \( \text{Wi} = \text{Wi}; \)
13. Apply Inverse three level DWT.
14. Let, \( \text{iHuff} = \text{Huffman decoding, and bit2message} = \text{bit sequence to message} \)
    \( \text{Mb} = \text{bit2message}(Mf); \)
    \( \text{Wf} = \text{iHuff}(Mb); \)
15. Set \( \text{Wf} \) as recovered watermark from watermark image.
16. Calculate PSNR and MSR.

[5]RESULTS

The proposed LSB-DWT based watermark technique has been applied to several images, including the 512 \( \times \) 512 sizes of Lena, Mandrill, and Barbara images. The parameters like Peak signal to Noise ratio (PSNR), Weighted Peak signal to Noise ratio (WPSNR), Mean signal Error (MSE) have been calculated. The calculated result is then compared to the results extracted from the previous related research work.

The[Figure3] below shows the result extracted in proposed system in terms of peak signal to noise ratio.
CONCLUSION

This paper contributes in the field of digital watermarking. Different Techniques are applied in different blocks of proposed system which include discrete wavelet transform, least significant bit technique, Huffman coding etc. In order to assess and compare the performance of the proposed techniques measures such as PSNR as considered. The watermarking algorithm developed and presented in this paper is a watermarking algorithm in wavelet domain, just like many of the existing algorithms but the embedding of secret message is performed using LSB technique. Using this algorithm the impact of different noise on the watermark robustness was investigated. The robustness of this algorithm is additionally improved by using the Huffman coding scheme in order to encode the secret message.

REFERENCES


