3-Level DWT Based Digital Image Watermarking

Deepika Sardana¹, Ajit Singh²

¹M.tech Scholar, Department of computer science
²Assistant Professor, Department of computer science,
T.I.T&S, Bhiwani-127021

Abstract:-In this digital era of information, data authenticity is one of the major issues. Digital watermarking is a way of copyrights in digital data such as an image. It is typically used to recognize the rights of copyright. The previous literatures used least significant bit technique directly into image pixels; this decreases the security of watermarking scheme. In this paper instead of embedding watermark in a simple time domain image, a new technique has been proposed which embed the secret text in spatial domain (by using three level wavelet transform) using least significant bit technique. The Huffman coding used in proposed work in order to increase the security of secret message. In proposed work watermark is made complex and hence more effectual.

Keywords: Huffman Code; LSB; digital watermark; wavelet transformation.

1. INTRODUCTION

1.1 Digital watermarking

A digital watermark is a process of secretly embedding some data in noise-tolerant signals such as audio or image. It is prominently used for banknote authentication. 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 [13]

1.2 Types of digital watermarks

Watermarking techniques can be classified into the following four categories according to the type of the multimedia document to be watermarked:
1. Image Watermarking
2. Video Watermarking
3. Audio Watermarking

1.2.1 Digital Image Watermarking

In the beginning, there was an ancient art called steganography [1], writing hidden message into another message. This process is done in such a way that no one except the sender and the intended recipient knows that there is secret information embedded into the message. Digital watermarking is derived from steganography: it is a technique which is supposed to embed some information into a medium such as an image, video or audio document [1]. There are two kinds of watermarking: visible and invisible. We will focus on invisible watermarking and more precisely on images. The purpose is to hide some information, like a copyright, into an image in an imperceptible way. The watermark which often consists in a binary sequence is embedded with a key which is known by the owner of the file and can be extracted using this key. Obviously it is very important that the watermarked image looks like the original but, there is a second criterion to consider for watermarking algorithms: the robustness. A watermarking algorithm cannot be robust against all kinds of attacks but the challenge is to have a robust algorithm against a large range of attacks. The owner of a document could use this type of algorithm in order to make sure of the integrity of the file. If the file has been modified in any way, the mark will not be found which a proof of modifications. [1]

2. WORK DONE

2.1 Existing Work

As Data Protection and Copyright 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 [1]. Various schemes [3, 4, 5, 6, 7] have been made to give a apparent imminent view of watermarking schemes. Dorairangaswamy et al. [3] gives blind watermarking method for protecting rightful ownership of Digital Images. It describe watermarking scheme as binary watermark, image is invisibly embedded into host image for achieving copyright protection in binary format. In watermark embedding, every pixel of the watermark image is embedded into the individual blocks of the host image.

Kang et al. [4] proposed Blind digital image watermarking using adaptive casting energy in different resolutions of wavelet transform” Digital image watermarking technique for protecting the digital images based on discrete wavelet transform due its frequency spread, excellent spatial localization, and multi-resolution analysis similar to human visual system. The method involves a visual watermark (grayscale image) which is transformed using discrete sine 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 [4]. Chandra [5] described overview of “Digital watermarking technique for protecting Digital images” 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 be detected or extracted later to make an assertion about the data.\cite{1}
Zhang et al. \cite{6} developed a new kind of Digital Image watermarking Algorithm with Double Encryption by Arnold Transform and Logistic”. 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.
Yang et al. \cite{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.

2.2 Proposed Algorithm
Presented Research Work proposes a novel watermarking scheme based on least significant bit technique. Instead of embedding watermark in a simple time domain cover image, a new technique has been proposed which embed the secret text in spatial domain (by using three level wavelet transform) using least significant bit technique. To improve the security of hidden text, proposed work also introduce Huffman coding to encode the secret message sooner than converting the message sequence into bit sequence for LSB operation.

The proposed algorithm is described below:
1. Examine Cover Image and Set I=input cover image;
2. If I is RGB image Then Convert it into Gray scale mage 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
   \((A_i, H_i, V_i, D_i)=dwt2 (I, \text{Wave});\)
   /*Here, \(A_i=\)approximation coefficients
   \(H_i=\)horizontal coefficients
   \(V_i=\)vertical coefficients
   \(D_i=\)diagonal coefficients*/
5. Second Level: Set \(I_{di}=dwt2 (A_i, \text{Wave});\)
6. Third Level: Set \(S_i=dwt2 (I_{di}, \text{Wave});\)
7. Let, Huff= Huffman coding of input and Message2bit= conversion of message into bit sequence \(C_t=\text{Huff} (W); \) //\(C_t=\)
   Coded text using Huffman encoding Scheme
8. Apply Huffman Coding on input message.
9. Convert message into bit sequence using decimal to binary keyword
   \(C_t=\text{Message2bit} (C_t);\)
10. Embedding of watermark text with cover image using LSB technique
    \(W_i=\)is watermarked image after watermarking process
12. Watermark Extraction Process
    If noise added through channel
    \(W_i=\text{Noise} (W_i);\)
    Else
    \(W_i=W_i;\)
End
13. Apply Inverse three levels DWT.
14. Let, \(i\text{Huff}=\) Huffman decoding, and \(\text{bit2message} =\) bit sequence to message conversion
    \(M_b=\text{bit2message} (M_f);\)
    \(W_f=i\text{Huff} (M_b);\)
15. Set \(W_f\) as recovered watermark from watermark image.
16. Calculate PSNR and MSR

www.ijcsit.com 1616
2.3 Data Flow Chart of Algorithm

![Data Flow Chart](image)

3. Experimental Evaluation

### 3.1 Discrete Wavelet Transform:

Discrete wavelet transform (DWT) [10] of image produces multi-resolution representation of an image. The multi-resolution representation provides a simple framework to interpret the image information. The discrete wavelet transformation analyses the signal at multiple resolutions. [10] DWT divides the image into two types of quadrants one is high frequency quadrant and another is low frequency quadrant. Then the low frequency quadrant is again divided into two more parts which are high and low frequencies and this process is repeated until the signal has been entirely decomposed. The single DWT is transformed into two dimensional image and into four parts: one part is the lower frequency of the original image, the top right contains the horizontal details of image, the one bottom left contains the vertical details of original image and the bottom right contains higher frequency of the original image. The lower frequency coefficients are more robust to embed watermark because it contains more information of the original image [10]. The reconstruction of the original image from decomposed image is performed by IDWT.

The digital wavelet transform are scalable in nature. DWT is more frequently used in digital image watermarking due to its excellent spatial localization and multi-resolution techniques. The excellent spatial localization property is very convenient to recognize the area in cover image in which the watermark is embedded efficiently.
MSE is a Risk function, corresponding to the expected impulse response.

**3.2 Mean Squared Error (MSE)**

MSE is a Risk function, corresponding to the expected impulse response. The coefficients are:

\[ W_{LL} = \sum_{x=0}^{N-1} g(x) h(y)_{LL}(2u-x)(2v-y) \]

\[ W_{LH} = \sum_{x=0}^{N-1} g(x) h(y)_{LH}(2u-x)(2v-y) \]

\[ W_{HL} = \sum_{x=0}^{N-1} h(x) g(y)_{HL}(2u-x)(2v-y) \]

\[ W_{HH} = \sum_{x=0}^{N-1} h(x) g(y)_{HH}(2u-x)(2v-y) \]

Where \( J \) is level of the 2-D DWT, \( h(n) \) and \( g(n) \) are the impulse response.

**3.3 Peak Signal to Noise Ratio (PSNR)**

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise. In this 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 observed value then the MSE of the predictor is:

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

**3.4 Weighted Peak Signal To Noise Ratio (WPSNR)**

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.

\[ \text{WPSNR} = 10 \log_{10} \left( \frac{L_{\text{max}}^2}{\text{MSE} \times \text{NVP}} \right)^2 \]

**4. PERFORMANCE EVALUATION**

In evaluation of performance of the watermarking scheme for robustness, this work use the mean square error(MSE) between original and watermarked images respectively, peak signal to noise ratio(PSNR), and Weighted peak signal to noise ratio(WPSNR). The image pixels are supposed to be 8 bits to give a greatest pixel value of 255. To test the effectiveness of proposed algorithm for better invisibility, this work use PSNR and MSE between input cover media and watermarked media (after embedding watermark in original image). The Basic aim of the work is to test the efficiency of watermarking process by comparing the input cover image and the cover image after embedding the watermark using proposed method. When \( 512 \times 512 \) sizes of Lena are taken by existing algorithm (previous Research work), then the PSNR was 57.98 and by proposed algorithm it is 64.74. When \( 512 \times 512 \) sizes of BARBRA are taken by Previous Research work then the PSNR was 53.78 and by proposed algorithm it is 60.57. When \( 512 \times 512 \) size of Lena is taken by previous research work then the PSNR was 54.93 and by proposed algorithm it is 61.78.

**4.1 Comparative Analysis of Results by Proposed Algorithm and Previous Related Research Work**

![Table 1: Comparison table of result of proposed work and The Result Extracted from the Previous Related Research Work](image)

<table>
<thead>
<tr>
<th>Image Name (512x512)</th>
<th>Proposed System</th>
<th>Base paper Method</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PSNR</td>
<td>MSE</td>
</tr>
<tr>
<td>LENNA</td>
<td>64.7422</td>
<td>1.28674</td>
</tr>
<tr>
<td>BARBARA</td>
<td>60.5740</td>
<td>1.30225</td>
</tr>
<tr>
<td>MANDRILL</td>
<td>61.7834</td>
<td>1.30202</td>
</tr>
</tbody>
</table>

On the basis of result it is clear that the PSNR is increased by applying the Proposed algorithm. The PSNR is increased for all images hence the Proposed algorithm is modification over the existing LBS based algorithm in terms of security. The parameters like Weighted Peak Signal To Noise Ratio (WPSNR), Mean signal Error(MSE), and Peak Signal To Noise Ratio (PSNR), have been Calculated. The calculated result is then compared to the result extracted from the previous related research work.
5. RESULTS
The Figure below shows the result extracted in proposed system in terms of peak signal to noise ratio.

6. CONCLUSION & FUTURE SCOPE

6.1 Conclusion
This paper contributes in the field of digital watermarking. In this paper different Techniques are applied which include discrete wavelet transform, Huffman Coding, Least significant bit technique. The security issues of existing algorithm are solved in this proposed method. The PSNR is increased for all images hence the Proposed algorithm is modification over the existing LBS based algorithm in terms of security.

6.2 Future Work
This paper introduced an efficient algorithm for watermarking using LSB technique. The security issues of existing algorithm are solved in this proposed method but algorithm complexity is not reduced in the proposed algorithm as there are number of techniques used to make the whole system. In future one can work on the complexity of the system.

Proposed algorithm is work only for a definite bit length of secret data. Other kind of data like special characters data is not acceptable by the proposed algorithm. The research can be extended in this direction so that different type of data can also be used.

The computational is a bit more, as doing wavelet transform in order to convert an image from time domain to spatial domain takes a bit of time. So work can be extended in this field also.

REFERENCES
[12]. https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio