© 2018 IJSRSET | Volume 4 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

A Review on Digital Image Watermarking using 3-Level Discrete Wavelet Transform

Laxminarayan Gahalod[1], Dr. Sanjeev Kumar Gupta[2]

[1]Research Scholar Department of Electronics & Communication AISECT University, Bhopal, India

[2]Professor Department of Electronics & Communication AISECT University, Bhopal, India

ABSTRACT

The rapid expansion of internet in the past years has rapidly increased the availability of digital data such as audio, images and videos to the public. The problem of protecting multimedia information becomes more important. A lot of copyright owners are concerned about protecting any illegal duplication of their data or work. This is an interesting challenge and this is probably why so much attention has been drawn toward the development of digital images protection schemes. Digital image watermarking technique solves this problem to the great extent. This paper incorporates different techniques of digital image watermarking and the comparison of various performance criteria of digital image.

Keywords : Digital image watermarking, Discrete Wavelet Transform, PSNR, MSE, Alpha Blending, Imperceptibility.

I. INTRODUCTION

Digital data is now mostly used for processing and distribution, but an easy access to multimedia device can duplicate it to produce the multiple copies of the digital data so it to produce the multiple copies of the digital data so it is necessary to protect data piracy. Digital watermarking is a concept of hiding ownership data into the multimedia data, which can be extracted later on to prove the authenticated owner of the media. Watermarking ensures authenticating ownership, protecting hidden information, prevents unauthorized copying and distribution of images over the internet and ensures that a digital picture has not been altered. Data hiding techniques include Cryptography, Watermarking, and Steganography. Cryptography only prevents the leakage of information being. There is no protection after decryption. Steganography hide the transmission of data itself. Watermarking is basically two types: visible and invisible. In visible watermarking, when the logo is inserted in the image, it remains visible to the users, whereas in invisible watermarking, the logo is transparent to the user.

On the basis of necessities for watermark extraction or detection watermark can be grouped into three schemes namely blind, non-blind and semi blind. In blind watermarking, only the watermarked image is required. In non-blind watermarking the cover or original images are also required for detecting the watermark. In semi blind watermarking scheme original image is not needed but a key or some side information is required.

II. LITERATURE REVIEW

Akhil Pratap Singh and Agya Mishra (2011) discussed that insertion and extraction of the watermark in the grayscale image is found to be simpler than other transform techniques. They explain the digital watermarking technique on digital images based on discrete wavelet transform by analyzing various values of PSNR's and MSE's.

Malika Narang and Sharda Vashisth (2013) propose the watermarking scheme based on DWT (discrete wavelet transform) which works in transform domain. Watermarking algorithms are divided into two groups based on extraction: Blind and Non-blind watermarking. In blind watermarking extraction does not need original image but in non-blind watermarking original image is needed in watermark extraction. In this paper they use non-blind watermarking.

Anum Javeed Zargar and Ninni Singh (2014) designed the system for digital watermarking, using Discrete wavelet transformation and the wave filter, we have used is HAAR wavelet. This system also provides for an MSE, PSNR, and BER, which determines the robustness of the watermark on the digital image. This is necessary in fragile watermarking as they can be easily removed from the basic image transformation. In such a case imperceptibility present in watermark prevent it from malicious attack.

Ravi K Sheth and Dr. V V Nath (2016) suggested a new secured digital watermarking technique that can be used for the data validation. This method is secure and efficient. The secured digital watermark is added by the hybrid method for which they have used combination of discrete cosine transform (DCT) and discrete wavelet transform (DWT) methods along with cryptographic technique (Arnold Transform). This technique provides strong robustness and perception transparency to the watermarked image and original image against different kind of attacks like cropping, noise and scaling. They found that DCT-DWT method is superior to LSB and DCT methods. Hence it can be safely concluded that the suggested technique of DCT-DWT provides stronger robustness and perception transparency to the watermarked image and original image against different kind of attacks like noise, cropping and scaling.

Hina Lala (2017) implement digital image watermarking technique based on discrete wavelet transform using alpha blending technique. This technique embeds visible watermark into the cover image. The cover image is required in the extraction process. The quality of recovered watermark image and watermarked image is depends on the scaling factors k and q.

III. DIGITAL IMAGE WATERMARKING

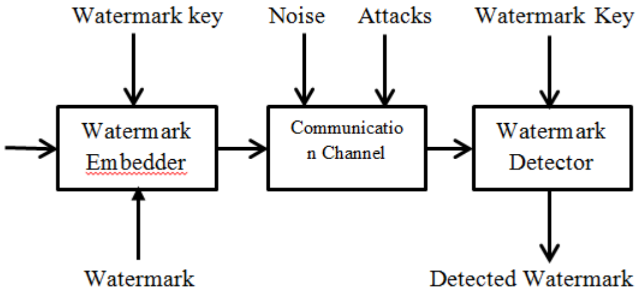

Figure 1. Digital Image Watermarking System

Digital watermarking hides the copyright information into the digital data through certain algorithm. The secret information to be embedded can be some text, author‘s serial number, company logo, images with some special importance. This secret information is embedded to the digital data (images, audio and video) to ensure the security, data authentication, identification of owner and copyright protection. The block diagram shows two phases which are used for embedding of watermark and detection or extraction of watermark.

3.1 Qualities of Digital Image Watermarking:

Following are the basic qualities of digital image watermarking:

- **Robustness:** It simply means ability to survive. When we transmit a watermarked data, then there are various attacks on that and that information may undergo different types of operations. So in these conditions, watermark must not degrade its quality.
- **Imperceptibility:** This simply means that watermark must be such that it cannot be observed by human eyes. It must be such that

it can only be accessed by particular operations on watermarked data.

- **Security:** It means that, the watermark must be such that only authorized users can access it. If any user has no embedding information, he must be unable to detect the watermark. This is termed as security of watermark.
- **Capacity:** It simply means that how much amount of information we are able to embed in the original image. Watermark capacity simply refers the secret information amount present in watermarked image.
- **Computational Cost:** It depends on the method which is used for watermarking. If the watermarking method is more complex, then it contains complex algorithm, requirement of more software and hardware, so computational cost increases and vice versa.

3.2 Watermarking Attack:

A brief introduction to various types of watermarking attacks is as under:

- **Removal Attack:** Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal.
- **Interference attack:** Interference attacks are those which add additional noise to the watermarked object. Lossy compression, quantization, collusion, denoising, remodulation, averaging, and noise storm are some examples of this category of attacks.
- **Geometric attack:** All manipulations that affect the geometry of the image such as flipping, rotation, cropping, etc. should be detectable. A cropping attack from the right-hand side and the bottom of the image is an example of this attack.
- **Low pass filtering attack:** A low pass filtering is done over the watermarked image and it results in a difference map composed of noise.
- **Security Attack:** In particular, if the watermarking algorithm is known, an attacker can further try to perform modifications to render the watermark invalid or to estimate and modify the watermark. In this case, we talk about an attack on security. The watermarking algorithm is considered secure if the embedded information cannot be destroyed, detected or forged.
- **Active Attacks:** Here, the hacker tries deliberately to remove the watermark or simply make it undetectable. This is a big issue in copyright protection, fingerprinting or copy control for example.
- **Passive Attacks:** In this case, the attacker is not trying to remove the watermark but simply attempting to determine if a given mark is present or not.

IV. WATERMARKING TECHNIQUES

Watermarking is the technique to hide the secret information into the digital media using appropriate algorithm. There are various algorithm used to hide the information. They are categorized as:

- Spatial Domain
- Frequency or transform domain

4.1 Spatial Domain:

spatial domain digital watermarking algorithm directly loads the raw data into the original image. In this technique watermark appears in any one of the color bands. Some useful spatial domain algorithms are as:

- **Additive watermarking:** This is most straight forward method for embedding watermark. In this technique pseudo random noise pattern is added to inserting of image pixels. The noise signal is usually integer or some time floating point numbers. To ensure that the watermark can be detected the noise is generated by a key.
- **Least Significant bit (LSB):** This is the old popular technique to embed the watermark. This technique is easy to implement and does not generate serious distortion to the image.

However it is not very robust against attacks. The embedding of the watermark is performed by choosing the subnet of image pixel and substituting the LSB of each of the chosen pixel with watermark bits. The watermark may be spread throughout the image or may be in the select location of the image [11].

4.2 **Frequency (Transform) Domain:** Compared to spatial domain techniques, frequency domain techniques are more widely used. The aim of frequency domain technique is to embed the watermark in the spectral coefficients of the image. The most commonly used transforms are:

- **Discrete Fourier Transform (DFT):** DFT transform the continuous function into its frequency components. It has robustness against geometric attacks like rotation, scaling, cropping etc. Fourier transforms allows analysis and processing of the signal in its frequency domain by means of analyzing and modifying the coefficients.
- **Discrete Cosine Transform (DCT):** DCT also transform a time domain signal into its frequency domain [4]. DCT only uses the real parts of the DFT coefficients. The JPEG compression technique utilizes this property to separate and remove insignificant high frequency components in image [12].
- **Discrete Wavelet Transform (DWT):** DWT is modern technique frequently used in digital image processing, compression, watermarking etc. The transform is based on small waves called wavelet of varying frequency and limited duration. The wavelet transform decomposes the image into three directions i.e. horizontal, vertical and diagonal [18].

V. 3–LEVEL DISCRTE WAVELET TRANSFORM

DWT is the multi-resolution description of an image the decoding can be processed sequentially from a low resolution to the higher resolution. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges [2].

In two dimensional applications, for each level of decomposition, we first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL sub-band of the previous level is used as the input. To perform second level decomposition, the DWT is applied to LL1 band which decomposes the LL1 band into the four sub- bands LL2, LH2, HL2, and HH2. To perform third level decomposition, the DWT is applied to LL2 band which decompose this band into the four sub-bands – LL3, LH3, HL3, HH3. This results in 10 sub-bands per component. LH1, HL1, and HH1 contain the highest frequency bands present in the image tile, while LL3 contains the lowest frequency band [5]. The three-level DWT decomposition is shown in Figure 2.

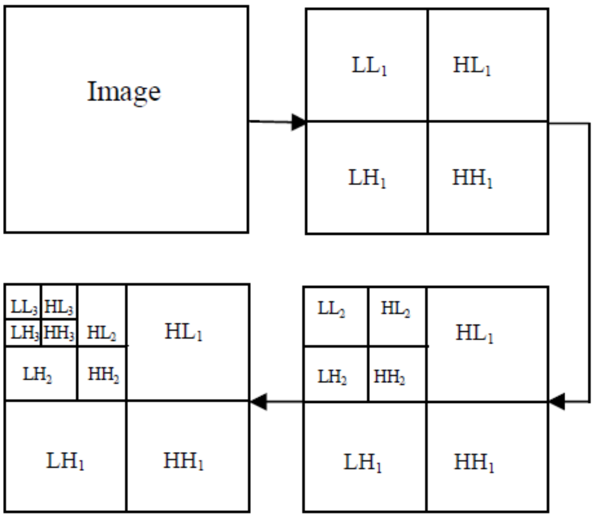

Figure 2. 3-level DWT composition

LL: it consist the low frequency details of the original image, we can say approximation of image lies in this part.

LH: It consist vertical details of the original image.
HL: It consist horizontal details of the original image
HH: It consist high frequency details of the original image. Since we know that the details of the original image lies in low frequency coefficient. The watermark embeds in low frequency coefficient [13].

5.1 Watermark Embedding: To hide personal data into cover image in perceptual visible manner, cover image is decomposed into four components i.e. low frequency approximation, low frequency vertical, low frequency horizontal and high frequency diagonal. The same procedure is applied on the watermark image which is to be imbedded into cover image. Now alpha blending technique is used for inserting watermark in cover image. In this decomposed cover and watermark images are multiplied by particular scaling factor and are added. Figure 3 shows the watermark embedding.

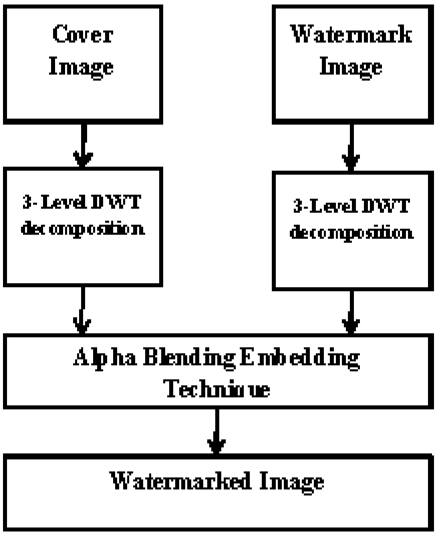
Cover Image
Watermark Image
3-Level DWT decomposition
3-Level DWT decomposition
Alpha Blending Embedding Technique
Watermarked Image

Figure 3. Watermark embedding

The alpha blending formula for embedding the watermark in cover image is given as below:

$$\boldsymbol{WMI = k \times LL3 + q \times WM3}$$

Where WMI = Watermarked Image
LL3 = Low frequency approximation of cover image obtained by 3-level DWT
WM3 = Low frequency approximation of watermark image obtained by 3-level DWT
K and q = scaling factor

After embedding the watermark Image on cover image inverse DWT is applied to the watermarked image coefficient to generate the final secure watermarked image [6].

5.2 Watermark Extraction: To extract watermark image from watermarked image 3-level DWT is applied to both watermarked image and cover image which decomposed the image in sub-bands as shown in figure 4. After that the watermark is recovered from the watermarked image by using the formula of the alpha blending given below:

$$\boldsymbol{RW = \frac{WMI - k \times LL3}{q}}$$

Where RW = Recovered Watermark
WMI = Watermarked Image
LL3 = Low frequency approximation of cover image obtained by 3-level DWT
q = Scaling Factor

After extraction process, Inverse discrete wavelet transform is applied to the watermark image coefficient to generate the final watermark extracted image [6].

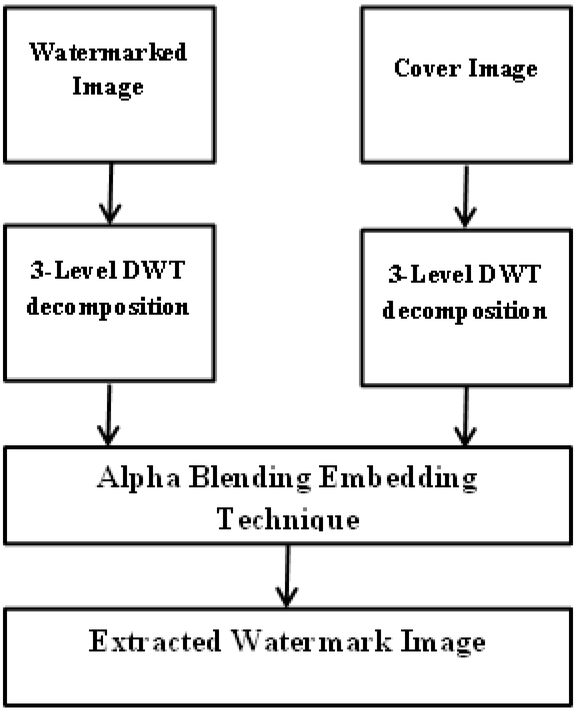
Watermarked Image
Cover Image
3-Level DWT decomposition
3-Level DWT decomposition
Alpha Blending Embedding Technique
Extracted Watermark Image

Figure 4. Watermark extraction

VI. PERFORMANCE PARAMETERS

- **Mean Squire Error (MSE):** It is define as the average squired difference between an original image and distorted image [13]. It is calculated as:

$$MSE = \frac{1}{PQ}\left[\sum_{i=1}^{P}\sum_{j=1}^{Q}\left(m(i,j) - n(i,j)\right)^2\right]$$

  Where: P and Q are defined as the height and width of the image respectively.

  m(i,j) = pixel value of original image

  n(i,j) = pixel value of watermarked image

- **Signal to Noise Ratio (SNR):** SNR measure the sensitivity of the image. It analyzes the effect of signal strength relative to the noise. It is measured as:

$$SNR_{dB} = 10log_{10}\left(\frac{P_{signal}}{P_{noise}}\right)$$

- **Peak Signal to Noise Ratio (PSNR):** PSNR is used to measure the similarity between the original image and the watermarked image. It is calculated as:

$$PSNR = 10log_{10}\left(\frac{L \times L}{MSE}\right)$$

  Where L = highest value of the image. For 8 bit image L = 255.

- **Bit Error Rate (BER):** It is defined as percentage of bits that have errors relative to the total number of bits received in a transmission. It has been calculated as:

$$BER = \frac{No.\ of\ Error\ Bits}{Total\ no.\ of\ bits\ sent}$$

VII. CONCLUSION

A 3-level DWT based image watermarking technique has been implemented. This technique embeds the watermark into the cover image using alpha blending technique which can be recovered by extraction technique. Survey result shows that the quality of the watermarked image depends only on the scaling factors k and q, and the recovered watermark is independent of scaling factor. Survey shows that the recovered images and the watermark are better for 3 level discrete wavelet transform then 1 & 2 level discrete wavelet transform. It also shows that the recovered cover image and the watermark image are identical to the original images.

VIII. REFERENCES

[1]. Akhil Pratap Singh,Agya Mishra,"Wavelet based Watermarking on Digital Image",Indian Journal of Computer Science and Engineering,Vol.1,No.2,2011,pp86-91.

[2]. Nikita Kashyap,G. R. Sinha,"Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)",I.J. Modern Education and Computer Science,2012,3,pp50-56.

[3]. Shilpa P. Metkar,Milind V. Lichade "Digital Image Security Improvement By Integrating Watermarking And Encryption Technique",IEEE International Conference on Signal Processing,Computing & Control (ISPCC),2013.

[4]. Bhupendra Ram,"Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform",International Journal of Advancements in Research & Technology,Volume 2,Issue4,April-2013,pp19-27.

[5]. Pratibha Sharma,Shanti Swami,"Digital Image Watermarking Using 3-level Discrete Wavelet Transform",Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013),pp129-133.

[6]. Malika Narang,Sharda Vashisth,"Digital Watermarking using Discrete Wavelet Transform",International Journal of Computer Applications (0975-8887) Volume 74– No. 20,July 2013,pp34-38.

[7]. Namita Chandrakar,Jaspal Bagga,"Performance Comparison of Digital Image Watermarking

Techniques: A Survey",International Journal of Computer Applications Technology and Research Volume 2– Issue 2,pp126 - 130,2013,ISSN: 2319–8656.

[8]. Suraj Kumar Singh,Varun P. Gopi,P. Palanisamy,"Image Security using DES and RNS with Reversible Watermarking",IEEE International Conference on Electronics and Communication System (lCECS -2014),2014.

[9]. Anum Javeed Zargar,Ninni Singh,"Digital Watermarking using Discrete Wavelet Techniques with the help of Multilevel Decomposition Technique",International Journal of Computer Applications (0975-8887) Volume 101– No.2,September 2014,pp25-29.

[10]. Anita,Archana Parmar,"Image security using watermarking based on DWT-SVD and Fuzzy Logic",IEEE 4th International Conference on Reliability,Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions),2015

[11]. N. Senthil Kumaran,and S. Abinaya,"Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique",IEEE International Conference on Communication and Signal Processing (ICCSP),2016.

[12]. Ravi K Sheth,Dr. V V Nath,"Secured Digital Image Watermarking with Discrete Cosine Transform and Discrete Wavelet Transform method",IEEE International Conference on Advances in Computing,Communication,& Automation (ICACCA) (Spring),2016.

[13]. Sonam Tyagi,Harsh Vikram Singh,Raghav Agarwal and Sandeep Kumar Gangwar,"Digital Watermarking Techniques for Security Applications",IEEE International Conference on Emerging Trends in Electrical,Electronics and Sustainable Energy Systems (ICETEESES–16),pp379-382.

[14]. Amra Siddiqui,Arashdeep Kaur,"A secure and robust image watermarking system using wavelet domain",IEEE 7th International Conference on Cloud Computing,Data Science & Engineering - Confluence,2017

[15]. Ramya M S,Pillai Sanjana Soman,Deepthi L R,"A Novel approach for Image Security using Reversible Watermarking",IEEE International Conference on Advances in Computing,Communication and Informatics (ICACCI),2017.

[16]. Akshay Pushpad,Anjali Ashish Potnis,"Improved Image Security Scheme Using Combination of Image",IEEE 4th International Conference on Signal Processing and Integrated Networks (SPIN),2017,pp293-297.

[17]. Hina Lala,"Digital Image Watermarking using Discrete Wavelet Transform", International Research Journal of Engineering and Technology (IRJET),Volume: 04 Issue: 01 Jan - 2017,pp1682-1685.

[18]. Ramandeep Singh,Sukhveer Singh,"Digital Image Watermarking using Discrete Wavelet Transform (DWT) and Flower Pollination Algorithm (FPA)",International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 6,Issue 5,May 2017,pp359-366.