Watermarking and related concepts: A review

Preeti Kumari*

M.Tech student of BSSITM, Lucknow, Uttar Pradesh

Abstract –The advent of the Internet has resulted in many new opportunities for the creation and delivery of content in digital form. Applications include electronic advertising, real time video and audio delivery, digital repositories and libraries, and Web publishing. An important issue that arises in these applications is the protection of the rights of all participants. Sometimes current copyright laws are not enough for dealing with digital data protection. This has led to an interest towards developing new copy protection techniques. One of such technique is digital watermarking techniques. Digital watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and security. Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, and video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. This paper includes watermarking definition concept and various methods of watermarking process. It starts with overview, techniques, application, challenges and limitations of watermarking.

Keywords: Digital Watermarking, DWT, DCT, LBP (Local Binary Pattern).

1. Introduction

The data hiding represents a useful example to the construction of a hypermedia document or image, which are very less convenient to manipulate. The aim of the steganography is to hide the message/image in the source image by some key techniques or methods and cryptography is a process to hide the message content in the image. The main objective is to hide a message inside an image keeping its visible properties and the source image as close to the original image. The most common methods to make these changes is usage of the least-significant bit (LSB) produced through masking, filtering and transformations on the source image.

According to visibility, there are two types of digital watermarking: visible and invisible. In a visible watermarking, data is visible in the image or video. Usually the information is a text message or a company logo which recognizes the owner of the media. Most television channels have logos that indicate that the information on the specific channel is protected. Nobody is allowed to use this data without permission from the channel that owns the data. The logo means a visible watermark that can be added . An invisible watermarking is information added to a digital multimedia object such as a text, audio, image, or video. An object that contains an “invisible watermark” should look like the original object. One of the most important applications of an “invisible watermark” is copyright protection. It is useful as a way of recognizing the author, creator, owner, and authorized client of a document or information.

2. Understanding Images

As a matter of fact, a computer manipulates images as a group of picture elements called pixels. Each pixel represents a stream of binary numbers that express the pixel's intensity or color. According to the color, images can be categorized into two kinds of images. One is a grayscale image, in which each pixel has 8 bits (1 byte) and the second is color image, in which each pixel has 24 bits (3 bytes). The 8- bit image has 256 different gray palettes (28 =256). This type of image will be displayed as a black-and-white picture (0 refers to black and 255 is white). A 24-bit image consists of three fundamental colors: "red, green, and blue" (RGB); each pixel is represented by three bytes. Each byte refers to the intensity of the three main colors RGB, respectively. This type of image has good quality, and the number of palettes is more than 16 million (224) different color.

According to extensions, images are divided into many types such as JPEG (Joint Photographic Experts), BMP (Bitmap), PNG (Portable Network Graphics), GIF (Graphics Interchange Format), TIFF (Tagged Image File Format), and etc. Most of these extensions use RGB format to show intensity of pixel color. The web page programming such as Hypertext Markup Language (HTML) uses RGB, where each two hexadecimal digits represent one primary color. This means each pixel has six hexadecimal digits. For example, the color yellow can be created by a full amount of red color (decimal 255, hex FF); the full amount of green, the pixel's value will be "#FFFF00" in the hexadecimal system number. Images are of different sizes, which depend totally on the number of pixels and also on the number of bits in each pixel. The size of an 8-bit gray image consists of resolution 320 by 240 pixels which is equal to 75 Kilobytes (320*240 bytes), while the size of an image with a full color (24-bit RGB) is going to be 225 Kilobytes. It is necessary to reduce image file sizes when transmitting via the internet. For this purpose many compression methods were developed over recent years. The two most popular types of compression are lossy and lossless compression, which are widely used in image processing. Compression processes are especially useful in BMP, GIF, and JPEG file image types [6, 14]. Lossy compression scheme uses by JPEG images this technique try to expand the file near to the size of original file. On the other hand, lossless compression is a scheme that uses to rebuild the original image by applying some software. GIF and 8-bit BMP are two types of images which use for this scheme.

3. Watermarking

Watermarking is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills.

However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications. There are several ways in which we can model a watermarking process. These can be broadly classified in one of two groups. The first group contains models which are based on a communication based view of watermarking and the second group contains models based on a geometric view of watermarking.

3.1 Communication-based models:

Communication based models describe watermarking in a way very similar to the traditional models of communication systems. Watermarking is in fact a process of communicating a message from the watermarking embedder to the watermarking receiver. Therefore, it makes sense to use the models of secure communication to model this process. In a general secure communication model we would have the sender on one side, which would encode a message using some kind of encoding key to prevent eavesdroppers to decode the message if the message was intercepted during transmission. Then the message would be transmitted on a communications channel, which would add some noise to the noise to the encoded message. The resulting noisy message would be received at the other end of the transmission by the receiver, which would try to decode it using a decoding key, to get the original message back. This process can be seen in the below figure 1.

In general, communication-based watermarking models can be further divided into two sub-categories. The first uses side-information to enhance the process of watermarking and the second does not use side-information at all. The term side-information refers to any auxiliary information except the input message itself, that can be used to better encode or decode it. The best example of this is the image used to carry the message, which can be used to provide useful information to enhance the correct detection of the message at the receiver.

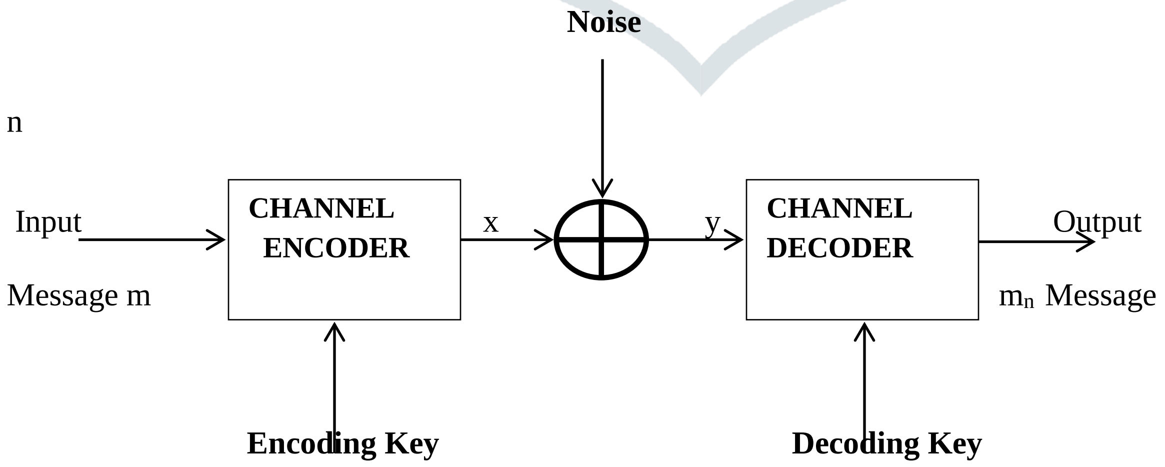

Figure 1: Communication model

It is often useful to think of watermarking in geometric terms. In this type of model, images, watermarked and un-watermarked, can be viewed as high-dimensional vectors, in what is called the media space. This is also a high-dimensional space that contains all possible images of all dimensions. For example a 512 X 512 image would be described as a 262144 elements vector in a 262144-dimensional space.

3.2 Geometric based Models:

Geometric models can be very useful to better visualize the watermarking process using a number of regions based on the desirable properties of watermarking. One of these regions is the embedding region, which is the region that contains all the possible images resulting from the embedding of a message inside an un-watermarked image using some watermark embedding algorithm. Another very important region is the detection region, which is the region containing all the possible images from which a watermark can be successfully extracted using a watermark detection algorithm. Lastly, the region of acceptable fidelity contains all the possible images resulting from the embedding of a message into an un-watermarked image, which essentially looks identical to the original image. The embedding region for a given watermarking system should ideally lie inside the intersection of the detection region and the region of acceptable fidelity, in order to produce successfully detected watermarks that do not alter the image quality very much.

An example of a geometric model can be seen in Figure 2. Here we can see that if mean square error (MSE) is used as a measure of fidelity, the region of acceptable fidelity would be an n-dimensional sphere centered on the original un-watermarked image, with a radius defined by the largest MSE we are willing to accept for images with acceptable fidelity. The detection region for a detection algorithm based on linear correlation would be defined as a half space, based on the threshold used to decide whether an image has a watermark embedded or not. Note that the diagram is merely a projection of an n-dimensional space into a 2d space.

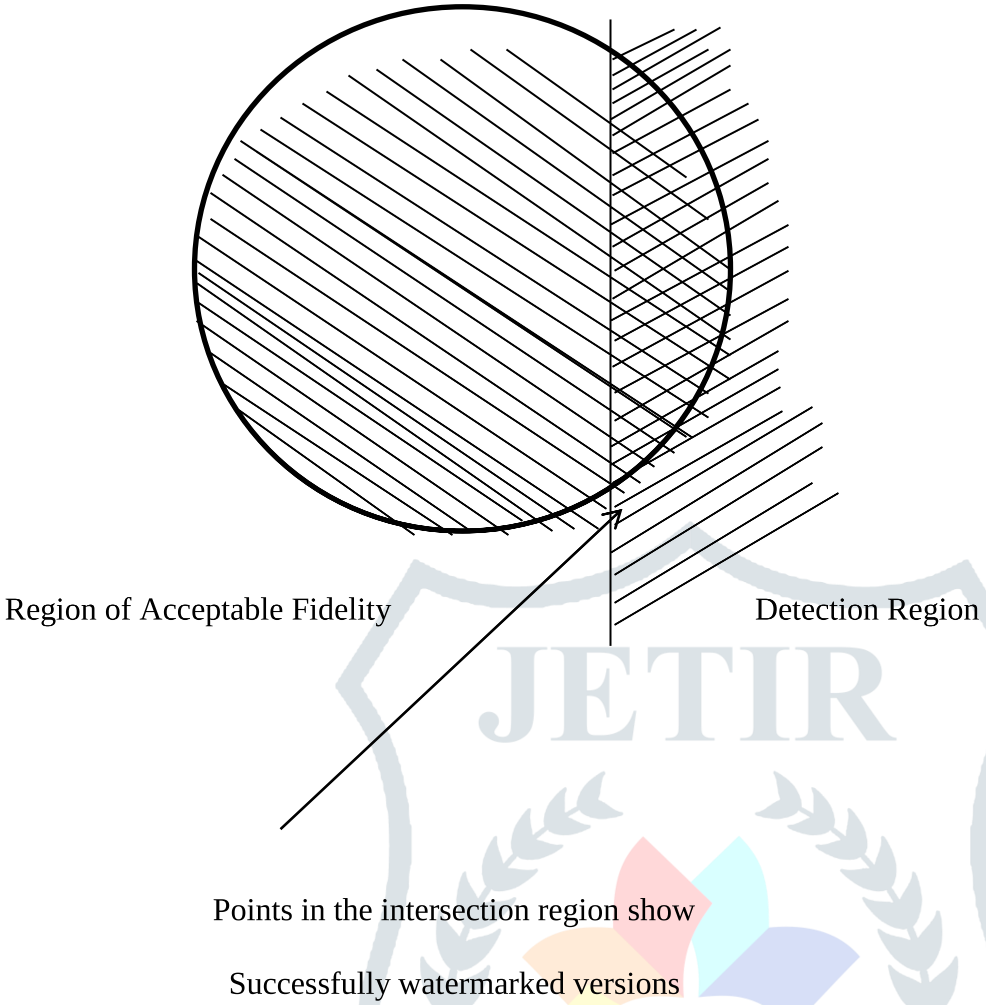
Region of Acceptable Fidelity
Detection Region
Points in the intersection region show
Successfully watermarked versions

Figure 2: The region of acceptable fidelity

When thinking about complex watermarking systems, it is sometimes more useful to consider a projection of the media space into a possibly lower-dimension marking space in which the watermarking then takes place as usual. This projection can be handled more easily by computers because of the smaller number of vector elements and can be possibly expressed by block-based watermarking algorithms which separate images into blocks instead of operating on a pixel basis. As described earlier, some communication-based watermarking models do not take advantage of the channel side-information. In this kind of models, the image is simply considered as another form of channel noise that distorts the message during its transmission. This can be seen in Figure 3. The watermark embedder encodes a message using a watermark encoder and a key. This is then added to the original image and transmitted over the communication channel which adds some noise. The watermark detector at the other end receives the noisy watermarked image and tries to decode the original image using a key.

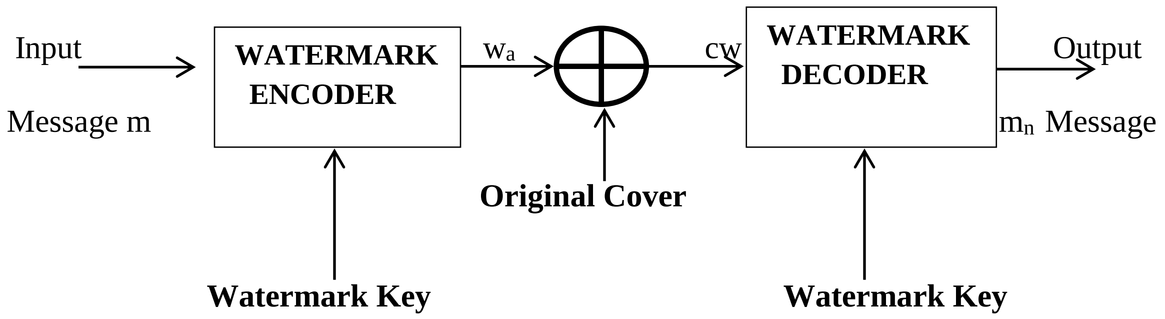

Figure 3: Watermarking Steps

3.3 Blind embedding and linear correlation detection

This system is an example of blind embedding, which does not exploit the original image statistics to embed a message in an image. The detection is done using linear correlation. This system is a 1-bit watermarking system, in other words it only embeds one bit (a 1 or 0) inside the cover image. The algorithm for the embedder and the detector is as follows:

2.3.1 Embedder:

1. Choose a random reference pattern. This is simply an array with the same dimensions as the original image, whose elements are drawn from a random Gaussian distribution in the interval [-1, 1]. The watermarking key is the seed that is used to initiate the pseudo-random number generator that creates the random reference pattern.
2. Calculate a message pattern depending on whether we are embedding a 1 or a 0. For a 1, leave the random reference pattern as it is. For a 0, take its negative to get the message pattern.
3. Scale the message pattern by a constant α which is used to control the embedding strength. For higher values of α we have more robust embedding, at the expense of losing image quality. The value used at the initial experiment was α = 1.
4. Add the scaled message pattern to the original image to get the watermarked image.

3.3.2 Detector:

1. Calculate the linear correlation between the watermarked image that was received and the initial reference pattern that can be recreated using the initial seed which acted as the watermarking key.

2. Decide what the watermark message was, according to the result of the correlation. If the linear correlation value was above a threshold, we say that the message was a 1. If the linear correlation was below the negative of the threshold we say that the message was a 0. If the linear correlation was between the negative and the positive threshold we say that no message was embedded.

An example of the embedding process can be seen in Figure 4. The top left image is the original image, the bottom left image is the reference pattern and the watermarked image resulting from embedding a 1, with α=1, is seen on the right. As we can see, there is no perceptual difference between the original and the watermarked image.

3.3.3 Watermark Extraction:

The Watermark Extraction process is almost the opposite of the detection process. The Watermarked image is passed through the key algorithm and the embedded watermark is retrieved from it.

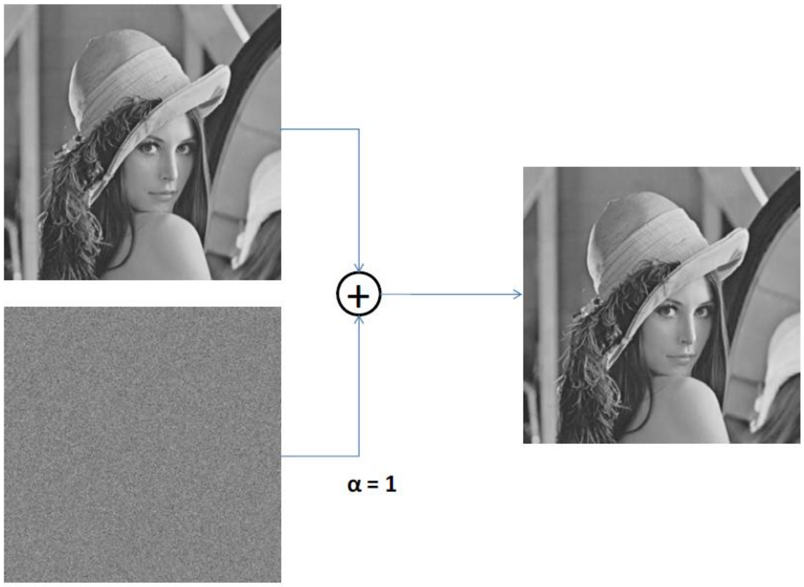

Figure 4: Watermark Embedding

3.4 Spatial Domain Watermarking

There are many algorithms using original data, such as video, image, audio, and text, to hide specific information like logos or personal signatures in a spatial domain. In other words, if the original data is an image, processing would be into the pixel values without changing the data into another domain. The widest and simplest method in spatial domain is Least Significant Bit (LSB), which is replacing the first bit in each pixel by information that intends to hide.

3.4.1 Least Significant Bit Watermarking

LSB is the one of the oldest and simplest algorithms that allows users to hide their information using spatial domain. The human eye cannot recognize the difference that occurs in the two first bits in each pixel. In other words, the change in the least significant bit does not affect the image's quality. 24-bit images have three LSB because each RGB channel has its own LSB. This provides users with more storage capacity to embed the information that is necessary to hide. For example, two pixels of an RGB image color will provide six bits for watermarking. To encode a message (100111) in RGB image needs two LSB pixels.

RGB Pixel 1 (R: 00010101 G: 11001100 B: 11101100)
RGB Pixel2 (R: 11011111 G: 00010001 B: 11001001)
To hide the same message (100111) in a gray-scale image six LSB pixels are needed.
Pixel1: 10010101 Pixel2: 00001100 Pixel3: 11001000
Pixel4: 10011111 Pixel5: 00010001 Pixel6: 11001011

3.4.2 Frequency Domain Watermarking

This is also called transform domain, because the original data changes from spatial to frequency domain. The most common frequency methods are Discrete Fourier Transformation (DFT), Discrete Wavelet Transformation (DWT), and Discrete Cosine Transformation (DCT). For example, an 8-bit image with a 256 by 256 resolution can be transformed into frequency watermarking using DWT. The result of this processing would be four small images, each of them with a 128 by 128 resolution. Moreover, four images will have different frequency ranges from low to high because each of them has different coefficients for others. The main advantage of using frequency domain watermarking is that it is robust for many kinds of signal manipulations when sending data via the Internet. Also, it resists of many noises that attack embedded information.

3.4.2 Discrete Cosine Transform

The DCT is a very popular transform function used in signal processing. It transforms a signal from spatial domain to frequency domain. Due to good performance, it has been used in JPEG standard for image compression. DCT has been applied in many fields such as data compression, pattern recognition, image processing, and so on.
The DCT transform and its inverse manner can be expressed as follows:

$$X_C(k_1,k_2) \triangleq \sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1} 4x(n_1,n_2)\cos\frac{\pi k_1}{2N_1}(2n_1+1)\cos\frac{\pi k_2}{2N_2}(2n_2+1), \quad 1$$

For, $(k_1,k_2)\in[0,N_1-1]x[0,N_2-1], Otherwise, X_C(k_1,k_2)\triangleq 0.$

As an image transformed by the DCT, it is usually divided into non-overlapped m x m block. In general, a block always consists of 8x8 components. The block coefficients are shown in figure 5. The left-top coefficient is the DC value while the others stand for AC components. The zigzag scanning permutation is implied the energy distribution from high to low as well as from low frequency to high frequency with the same manner.

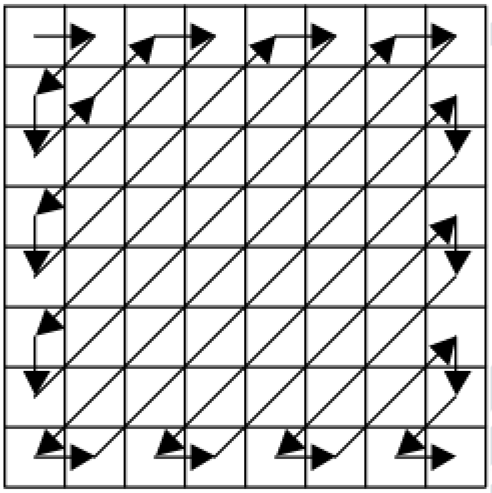

Figure 5: DCT block Coefficient and Zigzag

The human eyes are more sensitive to noise in lower-frequency band than higher frequency. The energy of natural image is concentrated in the lower frequency range. The watermark hidden in the higher frequency band might be discarded after a lossy compression. Therefore, the watermark is always embedded in the lower-band range of the host image that transformed by DCT is perfect selection. The lower-band coefficients of DCT block are described as in Figure 6.

	1	5	6				
2	4	7					
3	8						

Figure 6: 8 lower band coefficients

3.4.3 Discrete Wavelet Transform

It is a tool to transform the signal or data from one domain which is a spatial to another domain which is a frequency. In the frequency domain the signal splits into the two half one of them is high frequency and another is low frequency. Then each of them is going to divide again into high and low frequency that four different parts of signal. Four parts or sub bands of decomposed signal are LL, LH, HL and HH frequencies which are low-low, low-high, high-low and high-high frequencies. Low frequency is the same of original signal and other parts are more details of signal they are not exact data as original one, so we can change or remove depends on the technique that we using. The reconstruction process is the opposite of decomposition process that means the four bands of divided data have to be mixed again to recover the original data. Sometimes we do more than one level of decomposition depends on the algorithm that we use. Low-low frequency band will be used in case we do second decomposition. In case of reconstruction the last level of decomposition will used first which is an exact opposite direction. DWT is the multi resolution description of an image the decoding can be processed sequentially from a low resolution to the higher resolution. In this the low frequency signals are located in the frequency domain while high frequency signals are located in the pixel domain. Wavelets have their energy concentrated in time and are well suited for the analysis of the transient, time varying signals. The 2D wavelet transform decomposes an image into lower resolution approximation image (LL) as well as horizontal(HL),vertical(LH) and diagonal(HH) detail components. The perceptible watermark should be embedded in the low frequency region while the imperceptible watermark should be embedded in the high frequency region. Figure 7 shows the architecture of the watermarking model based on digital watermarking. In this the discrete wavelet transform is applied to the original image and the watermark separately. After this the watermark is embedded in the image using the alpha blending technique. For the recovery of the watermark and the original image the IDWT(Inverse Discrete Wavelet Transform) is applied to the watermarked image and the both images are recovered.

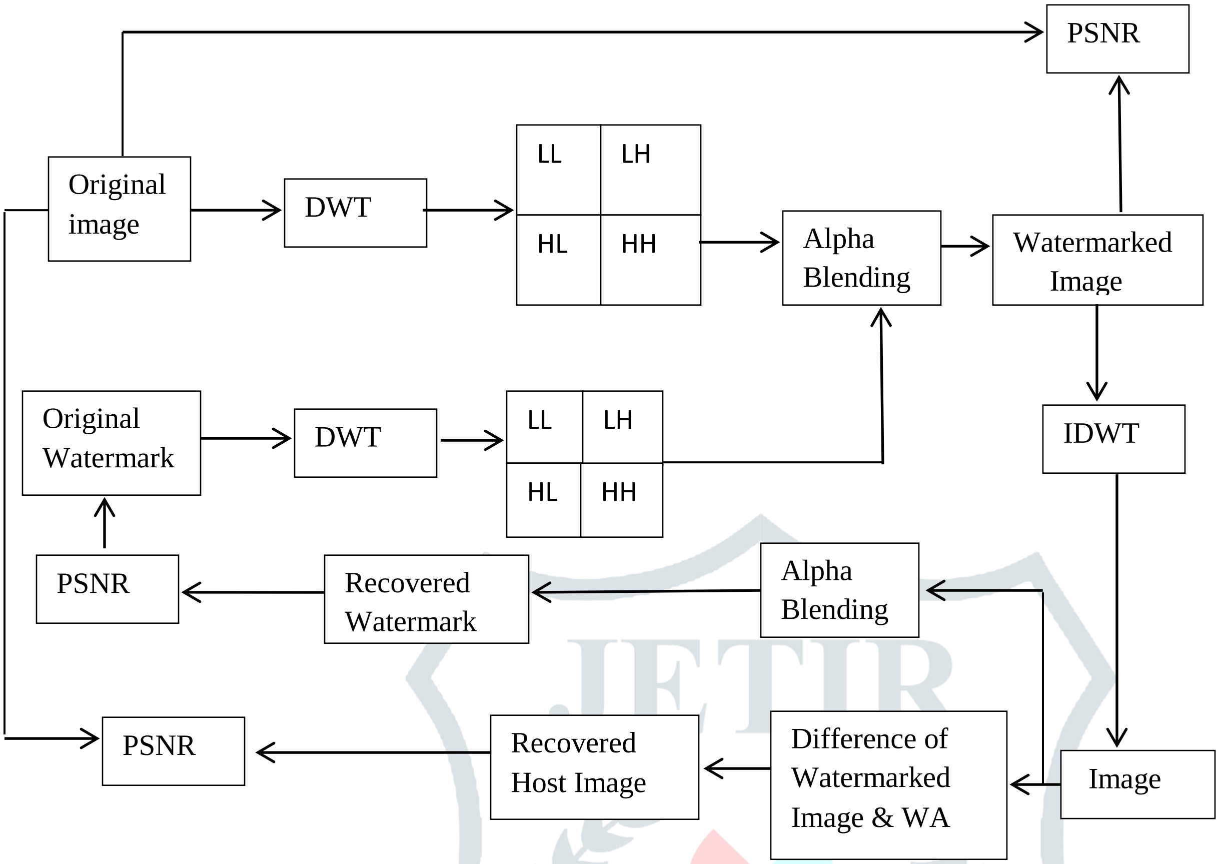

Figure 7: Architecture of DWT base Watermarking Technique

Watermark Embedding: In this process firstly the gray scale host image is taken and 2D DWT (Discrete Wavelet Transform) is applied to the image which decomposes image into four components low frequency approximation, high frequency diagonal, low frequency horizontal, low frequency vertical components. In the same manner DWT is also applied to the watermark image which is to be embedded in the host image. The wavelet used here is the wavelets of daubechies. The technique used here for inserting the watermark is alpha blending. In this technique the decomposed components of the host image and the watermark which are obtained by applying DWT to both the images are multiplied by a scaling factor and are added. During the embedding process the size of the watermark should be smaller than the host image but the frame size of both the images should be made equal. Since the watermark embedded in this paper is perceptible in nature or visible, it is embedded in the low frequency approximation component of the host image.

Alpha blending:

According to the formula of the alpha blending the watermarked image is given by:

$$WMI=k*(LL1)+q*(WM1) \qquad 2$$

WMI=Watermarked image

LL1=low frequency approximation of the original image WM1=Watermark. k, q-Scaling factors for the original image and watermark respectively.

Watermark Extraction: In this process the steps applied in the embedding process are applied in the reverse manner. The Inverse discrete wavelet transform is applied is applied to the watermarked image .Now the result obtained is subtracted from the watermarked image and in this way the host image is recovered. The watermark is recovered from the watermarked image by using the formula of the alpha blending.

Alpha blending

$$RW= (WMI - k*LL1) \qquad 3$$

RW=Recovered watermark, LL1=Low frequency approximation of the original image, WMI=Watermarked image.

REFERENCES

[1] Srinivasa Rao Chalamala and Krishna Rao Kakkirala,"Local Binary Patterns for Digital ImageWatermarking", 015 Third International Conference on Artificial Intelligence, Modelling and Simulation 978-1-4673-8675-3/15 $31.00 © 2015 IEEE 2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation.

[2] Jun-Dong Chang, Bo-Hung Chen, and Chwei-Shyong Tsai,"LBP-based Fragile Watermarking Scheme for Image Tamper Detection and Recovery",IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) - February 25-26 , Kaohsiung , Taiwan.

[3] Heng Zhang, Chengyou Wang, and Xiao Zhou,"An Improved Secure Semi-fragile Watermarking Based on LBP and Arnold Transform", Journal of Information Processing System.

[4] Dipesh Agrawal and Samidha Diwedi Sharma," Analysis of Random Bit Image Steganography Techniques", International Journal of Computer Applications (0975 – 8887)International Conference on Recent Trends in engineering & Technology – 2013.

[5]Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt,"Digital Image Steganography: Survey and Analysis of Current Methods", Signal Processing, Volume 90, Issue 3, March 2010, Pages: 727-752\

[6]. Anil Kumar and Rohini Sharma,"A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique",International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 7, July 2013.

[7]. Ramadhan Mstafa and Christian Bach,"Information Hiding in Images Using Steganography Techniques",2013 ASEE Northeast Section Conference, Norwich University, March 14-16, 2013.