

# Digital Watermarking Methods in Spatial Domain and Transform Domain

Nilay B. Mistry<sup>1</sup> Dhruv Dave<sup>2</sup>

<sup>1</sup>Research Scholar, <sup>2</sup>Professor, Department of Computer Engineering

<sup>1,2</sup>KSV University, Gandhinagar, India

**Abstract**--- The ease of digital media modification and dissemination necessitates content protection beyond encryption. Information hidden as digital watermarks in multimedia i.e. text, image, video, audio enables protection mechanism in decrypted contents. In a way that protects from attacks several common image processing techniques are used in Spatial Domain and Transform Domain. In Spatial Domain Least Significant Bit(LSB) is used and in Transform domain Discrete Cosine Transform(DCT) & Discrete Wavelet Transform(DWT) are used. Among these DWT is best method due because of using embedded zero tree wavelet image compression scheme and high frequency sub bands.

**Keyword:** Digital watermarking, LSB, DCT, DWT

## I. INTRODUCTION

Nowadays the increases use of the Internet has rapidly increased the availability of digital data i.e. images, audio, videos & texts to the end users. We all want to protect our images from unauthorized use, but at the same time, we don't want to do anything to detract from the visual appearance, since that is the whole point of posting the work in the first place. As we have witnessed in the past few months, the problem of protecting multimedia information becomes more and more important and a lot of copyright owners are concerned about protecting any illegal duplication of their data or work[1]. For that some serious work needs to be done to protect and maintain the multimedia data of creators, distributors or simple users. Among the many approaches available to protect multimedia information, "Digital Watermarking" is probably the best suitable in order to its robustness.

The idea of robust watermarking of images is to embed information data within the image with an insensible form for human visual system but in a way that protects from attacks such as common image processing operations. The goal is to produce an image that looks exactly the same to a human eye but still allows its positive identification in comparison with the owner's key if necessary[1].

## II. FUNDAMENTALS OF WATERMARKING

Digital Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video or audio. Digital watermarking technology makes use of the fact that the human eye has only a limited ability to observe differences. Minor modifications in the colour values of an image are subconsciously corrected by the eye, so that the observer does not notice any difference. 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.

A digital watermark can be described as a visible or preferably invisible identification code that is permanently embedded in the data. It means that it remains present within the data after any decryption process. A general definition can be given: "Hiding of a secret message or information within an ordinary message and the extraction of it at its destination." Complementary to encryption, it allows some protection of the data after decryption. As we know, encryption procedure aims at protecting the image (or other kind of data) during its transmission. Once decrypted, the image is not protected anymore.

By adding watermark, we add a certain degree of protection to the image (or to the information that it contains) even after the decryption process has taken place. The goal is to embed some information in the image without affecting its visual content. In the copyright protection context, watermarking is used to add a key in the multimedia data that authenticates the legal copyright holder and that cannot be manipulated or removed without impairing the data in a way that removes any commercial value [1]. The encoding and decoding is shown in following figures.

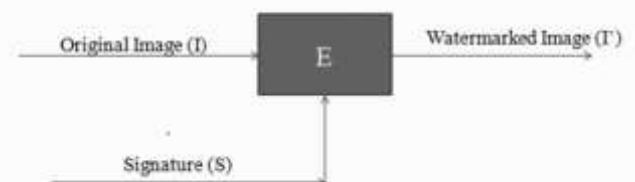


Fig. 1: Encoding of Watermark



Fig. 2: Decoding of Watermark

### A. Classification of Watermark

- 1) According to Human Perception
  - 1) Visible Watermarking
  - 2) Invisible Watermarking
- 2) According to Working Domain
  - 1) Spatial Domain
  - 2) Transform(Frequency) Domain
- 3) According to Robustness
  - 1) Fragile

- 1) Semi-Fragile
- 2) Robust
- 4) According to types of Documents
  - 1) Text
  - 2) Audio
  - 3) Video
  - 4) Image

### III. TYPES OF WATERMARKING ACCORDING TO WORKING DOMAIN

#### A. Spatial Domain Method

The *spatial domain* is the normal image space, in which a change in position in I directly projects to a change in position in space. Distances in I (in pixels) correspond to real distances (e.g. in meters) in space. This concept is used most often when discussing the frequency with which image values change, that is, over how many pixels does a cycle of periodically repeating intensity variations occur[2].

$$g(x_i) = \sum_j \alpha_j x_j \quad (1)$$

The spatial Domain image processing is manipulating or changing an image representing an object in space to enhance the image for a given application. One way in which images are processed is to look at the neighbourhood around the pixel or that you wish to manipulate. The neighbourhood around pixel is made up of the surrounding pixels depending on how we define neighbourhood. In general, the neighbourhood of  $i$  is the set of all  $j$  such that  $j$  is a neighbour of  $i$ . The value of a pixel  $x_i$ , with a sum of all  $j$  such that  $j$  is in the neighbourhood of  $i$  ( $N_i$ ) is given by: eq. 1.

#### B. Transform Domain Method (Frequency)

The producer of high quality watermarked image is by first transforming the original image into the frequency domain by use of Fourier, Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT). Each of these transform has its own characteristics and represents the image in different ways [2]. With this technique, the marks are not added to the intensities of the image but to the values of its transform coefficients. Then inverse transforming the marked coefficients forms the watermarked image. The use of frequency based transforms allows the direct understanding of the content of the image; therefore, characteristics of the human visual system (HVS) can be taken into account more easily when it is time to decide the intensity and position of the watermarks to be applied to a given image [1].

##### 1) Different Frequency Domain mathematical transforms:

- 1) Fourier Series – repetitive signals, oscillating systems
- 2) Fourier Transform – non repetitive signals, transients
- 3) Laplace transform – electronic circuits and control systems
- 4) Z transform – discrete signals, digital signal processing

### IV. LEAST SIGNIFICANT BIT (LSB)

One of the simplest technique in digital watermarking is in spatial domain using the two dimensional array of pixels in the container image to hold hidden data using the least significant bits (LSB) method. Note that the human eyes are not very attuned to small variance in color and therefore processing of small difference in the LSB will not noticeable [1].

If data is encoded to only the last two significant bits (which are the first and second LSB) of each color component it is most likely not going to be detectable; the human retina becomes the limiting factor in viewing pictures. For the sake of this example only the least significant bit of each pixel will be used for embedding information. If the pixel value is 138 which is the value 1000110 in binary and the watermark bit is 1, the value of the pixel will be 1000111 in binary which is 139 in decimal. In this example we change the underline pixel [3].

#### A. Algorithm for Least Significant Bit

- 1) Convert RGB image to gray scale image.
- 2) Make double precision for image.
- 3) Shift most significant bits to low significant bits of watermark image.
- 4) Make least significant bits of host image to zero
- 5) Add shifted version (step 3) of watermarked image to modified (step 4) host image.

#### B. Limitations of Least Significant Bit

This method is comparatively simple and easy to implement but it lacks the Robustness that we may expect in any watermarking method to protect out digital data. It can survive with certain attacks like Cropping, Adding Noise and JPEG Compression in the watermarked images. Furthermore, once the algorithm was discovered, it would be very easy for an intermediate party to alter the watermark.

### V. DESCRETE COSINE TRANSFORM (DCT)

JPEG's lossy encoding tends to be more frugal with the gray-scale part of an image and to be more frivolous with the color. DCT separates images into parts of different frequencies where less important frequencies are discarded through quantization and important frequencies are used to retrieve the image during decompression [4].

The DCT allows an image to be broken up into different frequency bands, embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they have minimized they avoid the most visual important parts of the image (low frequency) without over-exposing themselves to removal through compression and noise attacks [5].

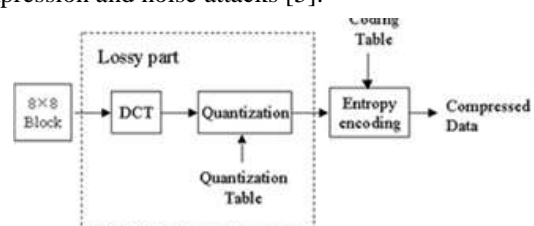


Fig. 3: DCT Watermarking [1]

### A. Steps in DCT to Encode the image

Step 1. The image is broken into N\*N blocks of pixels. Here N may be 4, 8, 16, etc.

Step 2. Working from left to right, top to bottom, the DCT is applied to each block.

Step 3. Each block's elements are compressed through quantization means dividing by some specific value.

Step 4. The array of compressed blocks that constitute the image is stored in a drastically reduced amount of space.[6]

### B. Steps in DCT to Decode the image

Step 1. Load compressed image from disk

Step 2. Image is broken into N\*N blocks of pixels.

Step 3. Each block is de-quantized by applying reverse process of quantization.

Step 4. Now apply inverse DCT on each block. And combine these blocks into an image which is identical to the original image.

### C. Comparative Advantages

- 1) DCT domain watermarking is comparatively much better than the spatial domain encoding since DCT domain watermarking can survive against the attacks such as noising, compression, sharpening, and filtering.
- 2) It uses JPEG compression method to apply DCT watermarking as a parameter. One may use different parameters related to image processing, and these parameters might provide equal or even stronger robustness against various attacks based on image processing.
- 3) Discrete cosine transform (DCT), where pseudo-random sequences, such as M sequences, are added to the DCT at the middle frequencies as signatures. [1]

## VI. DISCRETE WAVELET TRANSFORM (DWT)

The basic idea in the DWT for a one dimensional signal is the following. A signal is split into two parts, usually high frequencies and low frequencies. The edge components of the signal are largely to the high frequency part. The low frequency part is split again into two parts of high and low frequencies. This process is continued an arbitrary number of times, which is usually determined by the application at hand[1].

The DWT decomposes input image into four components namely LL, HL, LH and HH where the first letter corresponds to applying either a low pass frequency operation or high pass frequency operation to the rows, and the second letter refers to the filter applied to the columns. The lowest resolution level LL consists of the approximation part of the original image. The remaining three resolution levels consist of the detail parts and give the vertical high (LH), horizontal high (HL) and high (HH) frequencies[7].

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 decomposes 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 [8]. The three-level DWT decomposition is shown in Fig. 4.

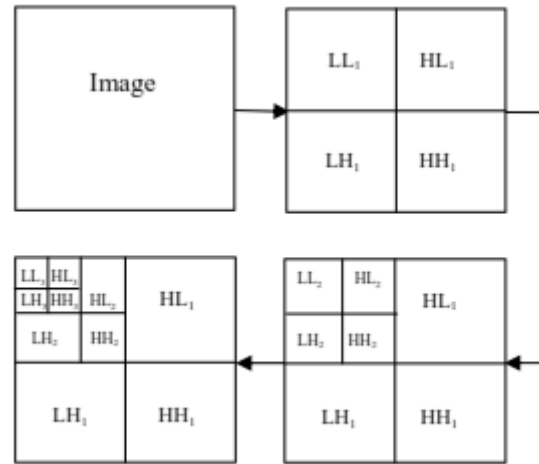


Fig. 4: 3-Level Discrete Wavelet Decomposition [8]

### A. Steps of DWT Watermarking

- (1) The first part of the watermarking process is, of course, the encoder. The first step is to decompose the image into four frequency bands using first resolutions of Haar wavelets at first level. In second level, decompose image into seven frequency bands using second resolutions of Haar wavelets. At three level, decompose image into ten frequency bands using third resolutions of Haar wavelets and so on.
- (2) The next operation is to add a pseudo random sequence N, in fact a Gaussian distribution of mean zero and variance one, to the coefficients of the medium and high frequency bands.
- (3) The normal distribution is used because it has been proven to be quite robust to collusive attacks. In order to weight the watermark according to the magnitude of the wavelet coefficients, we used one of the two following relations between the original coefficients y and y the ones containing the watermark:

$$\bar{y}_{i,j} = y_{i,j} + \alpha \cdot y_{i,j}^2 \cdot N_{i,j} \quad (2)$$

$$\bar{y}_{i,j} = y_{i,j} + \alpha \cdot |y_{i,j}| \cdot N_{i,j} \quad (3)$$

### B. Advantages of DWT

The watermarking method has multi resolution characteristics and is hierarchical. It is usually true that the human eyes are not sensitive to the small changes in edges and textures of an image but are very sensitive to the small changes in the smooth parts of an image. With the DWT, the edges and textures are usually to the high frequency sub bands, such as HH, LH, and HL etc. Large frequencies in these bands usually indicate edges in an image [1].

(2) The watermarking method robust to wavelet transforms based image compressions, such as the embedded zero-tree wavelet (EZW) image compression scheme, and as well as

to other common image distortions, such as additive noise, rescaling/stretching, and half toning. This is advantage over DCT[1].

## VII. CONCLUSION

This paper gives the overview of digital watermarking methods in Spatial Domain and Transform Domain. By these methods we can protect our digital data i.e. image, audio, video, text from unauthorized person, remove noise and gives copyright protection. By studying, we conclude that DCT and DWT domain methods are comparatively robust than Spatial Domain. Again DCT domain watermarking can survive against noising, compression, filtering, sharpening which can be removing by DWT domain methods. So, 3-level DWT wavelet transform method is better.

## REFERENCES

- [1] Dharshna Mistry, "Comparison of Digital Water Marking methods," (IJCSE) International Journal on Computer Science and Engineering, Vol. 02, No. 09, 2010, 2905-2909
- [2] Kiratpreet Singh Dhaliwal, Rajneet Kaur, "Comparative study of single watermarking to multiple watermarking over a color image," International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2 Issue 2 March 2013
- [3] Abdullah Bamatraf, Rosziati Ibrahim & Mohd. Najib Mohd. Salleh, "A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit," Journal of Computing, Vol. 3 Issue 4 April 2011
- [4] N. Ahmed, T. Natarajan, and K. R. Rao, "Discrete cosine transform," IEEE Trans. On Computers, vol. C-23, pp. 90-93,1974.
- [5] Zhao Yuehua, "An image watermark based on Discrete Cosine Transform block classifying"
- [6] Anilkumar Katharotiya, Swati Patel & Mahesh Goyani, "Comparative Analysis between DCT & DWT Techniques of Image Compression," Journal of Information Engineering and Applications, Vol 1, No.2, 2011
- [7] Chirag Sharma & Deepak Prashar, "DWT Based Robust Technique of Watermarking Applied on Digital Images," International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-2, May 2012
- [8] Nikita Kashyap & G.R.Sinha, "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)," I.J.Modern Education and Computer Science, 2012.03.07