Comparison of Digital Water Marking methods

Darshana Mistry
Computer Engineer Department
Gandhinagar Institute Of Technology
Gandhinagar, India

Abstract—**In Digital watermarking, image or video is embedded information data within an insensible form for human visual system but in a way that protects from attacks such as common image processing techniques. Spatial domain(Least significant bit(LSB)) and transform domain (Discrete Cosine Transform(DCT) and Discrete Wavelet Transform(DWT)) methods are used. DWT is best method because of using embedded zero tree wavelet image compression scheme and high frequency sub bands.**

Keyword: Digital watermarking, Leas significant bit, Discrete Cosine Transform, Discrete Wavelet Transform

I. INTRODUCTION

The rapid expansion of the Internet in the past years has rapidly increased the availability of digital data such as audio, images and videos to the public. 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. Some serious work needs to be done in order to maintain the availability of multimedia information but, in the meantime, the industry must come up with ways to protect intellectual property of creators, distributors or simple owners of such data. Of the many approaches possible to protect visual data, digital watermarking is probably the one that has received most interest.

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.

II. BASIC ON WATERMARKING

The increasing amount of applications using digital multimedia technologies has accentuated the need to provide copyright protection to multimedia data. 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. In Figure 1 a general watermarking scheme in order to give an idea of the different operations involved in the process.

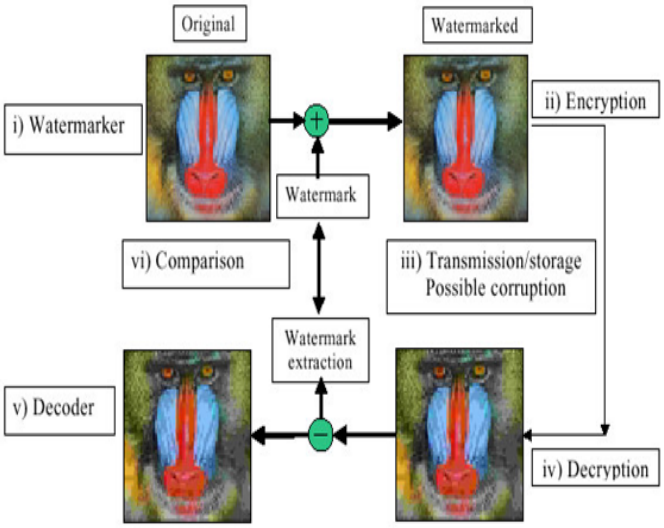


Fig. 1. General Watermarking Scheme

The first distinction that one needs to do in the study of watermarking for digital images is the notion of visible watermarks versus invisible ones. The first ones are used to mark, obviously in a clearly detectable way, a digital image in order to give a general idea of what it looks like while preventing any commercial use of that particular image. The purpose here is to forbid any unauthorized use of an image by adding an obvious identification key, which removes the image's commercial value. On the other hand, invisible watermarks are used for content and/or author identification in order to be able to determine the origin of an image. They can also be used in unauthorized image's copies detection either to prove ownership or to identify a customer. The invisible scheme does not intend to forbid any access to an image but its purpose is to be able to tell if a specified image has been used without the owner's formal consent or if the image has been altered in any way [2].

III. Types Of Digital Watermarking

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[4]. One would refer to the number of pixels over which a pattern repeats (its periodicity) in the spatial domain. Here we use Least Significant bit(LSB)method.

B. *Transform Domain Method*

The produce of high quality watermarked image is by first transforming the original image into the frequency domain by the use of Fourier, Discrete Cosine Transform (DCT) or Discrete Wavelet transforms (DWT) for example. 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.

IV. Least significant Bit

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. The steps to embed watermark image are given below.

A. *Steps of 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 Spatial Domain Watermarking*

This method is comparatively simple, lacks the basic robustness that may be expected in any watermarking applications. It can survive simple operation such as cropping, any addition of noise. However lossy compression is going to defeat the watermark. An even better attack is to set all the LSB bits to '1' fully defeating the watermark at the cost of negligible perceptual impact on the cover object. Furthermore, once the algorithm was discovered, it would be very easy for an intermediate party to alter the watermark.

V. Discrete cosine Transform Watermarking

The DCT allows an image to be broken up into different frequency bands, making it much easier to 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[1].

A. *Steps of DCT watermarking*

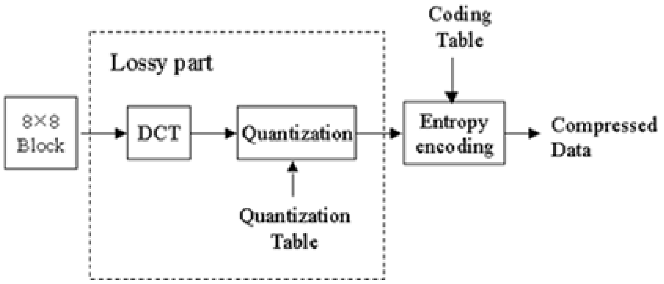


Fig. 2. DCT Watermarking

1) Transforming from the RGB color of the original image into the formation of Gray color

2) To divide the image into 8 × 8 blocks by JPEG standard as below.

3) Transforms original 8 x 8 block into a cosine-frequency domain

a) C(h) = if (h == 0) then 1/sqrt(2) else 1.0

--*C(h) is a auxiliary function used in main function F(u,v)*

b) F(u,v) = ¼ x C(u) x C(v) Σx=0..7 Σy=0..7 Dxy x cos(π(2u + 1)u/16) x cos(π(2y + 1)v/16)

-Gives encoded pixel at row u, column v

-Dxy is original pixel value at row x, column y
-F(u,v) is new matrix value after DCT apply.

B. Extracting Watermarked Image

1) Perform DCT transform on watermarked image and original host image.

2) Substract original host image from watermarked image.

3) Multiply extracted watermark by scaling factor to display.

C. 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 use 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.

VI. Discrete Wavelet Transform Watermarking

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.

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 (i.e. all the bands except the lowest one which is represented by the top left corner in Fig. 3.

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 $\overline{y}$ the ones containing the watermark:

$$\bar{y}_{i,j} = y_{i,j} + \alpha \cdot y_{i,j}{}^{2} \cdot N_{i,j} \qquad (1)$$

$$\bar{y}_{i,j} = y_{i,j} + \alpha \cdot \left| y_{i,j} \right| \cdot N_{i,j} \qquad (2)$$

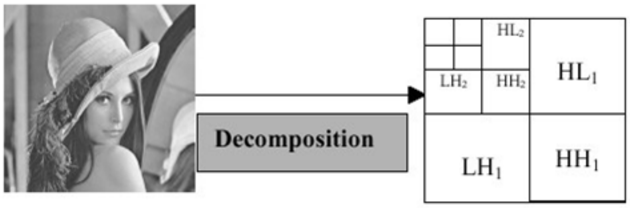


Fig. 3. Resulting Decompose image

4) It must be pointed out that the relations (1) and (2), even though they are mathematically different, have the exact same goal which is to put more weight to the watermark added to high value wavelet coefficients. The parameter alpha is to control the level of the watermark; it is in fact a good way to choose between good transparency or good robustness or a tradeoff between the two. Finally, the two dimension inverse wavelet transform of is computed to form ÿ the watermarked image. ***Fig 4*** *gives a good idea of the main components of the encoder that I have implemented for my project.*

B. Advantages

1) 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, HL etc. Large frequencies in these bands usually indicate edges in an image.

2) The watermarking method robust to wavelet transform 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.

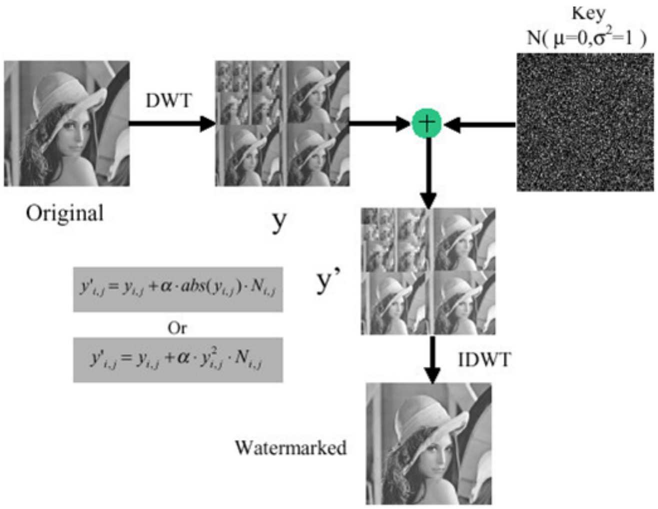

Key
N(μ=0,σ²=1)
DWT
Original
y
y'
$y'_{i,j} = y_{i,j} + \alpha \cdot abs(y_{i,j}) \cdot N_{i,j}$
Or
$y'_{i,j} = y_{i,j} + \alpha \cdot y_{i,j}^2 \cdot N_{i,j}$
IDWT
Watermarked

Fig. 4. Implemented watermarking scheme

VII. Design and implementation

Using of MATLAB 7.0's API. Results are as below:

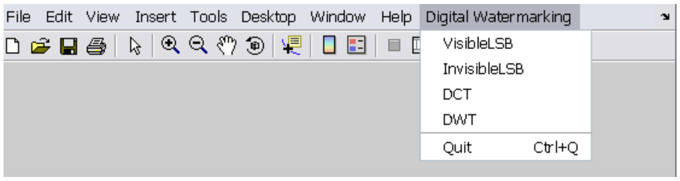

File Edit View Insert Tools Desktop Window Help Digital Watermarking
VisibleLSB
InvisibleLSB
DCT
DWT
Quit Ctrl+Q

Fig. 5. GUI of Digital watermarking

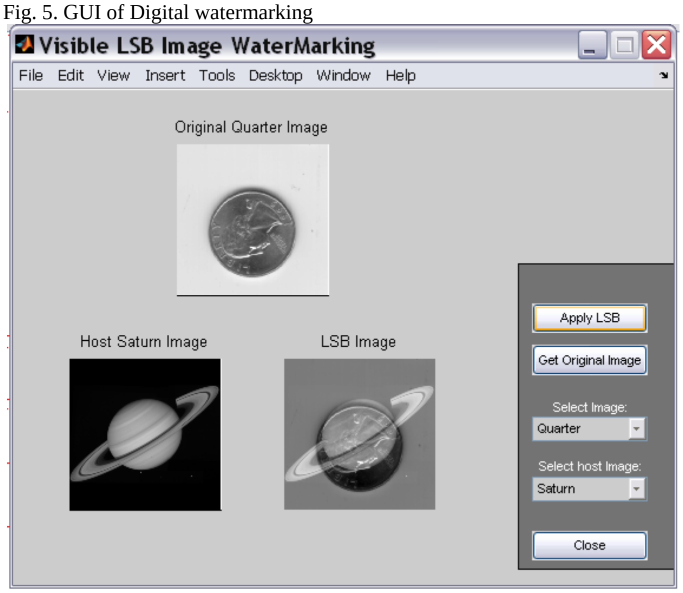


Fig. 6(a) LSB using visible image

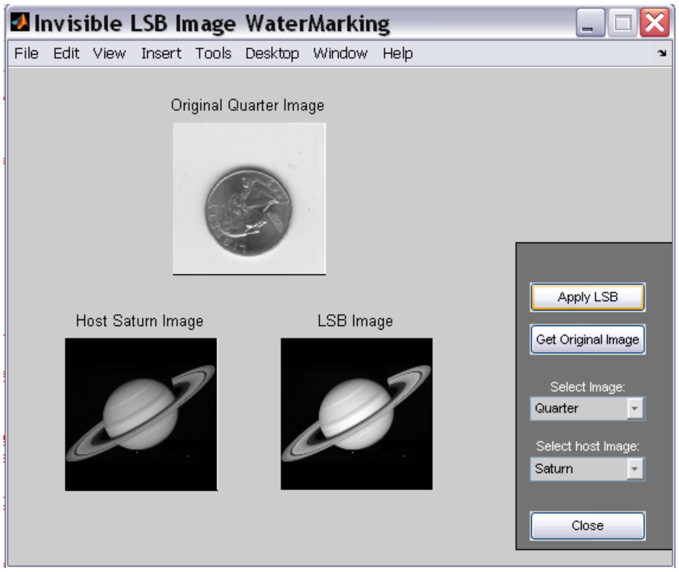
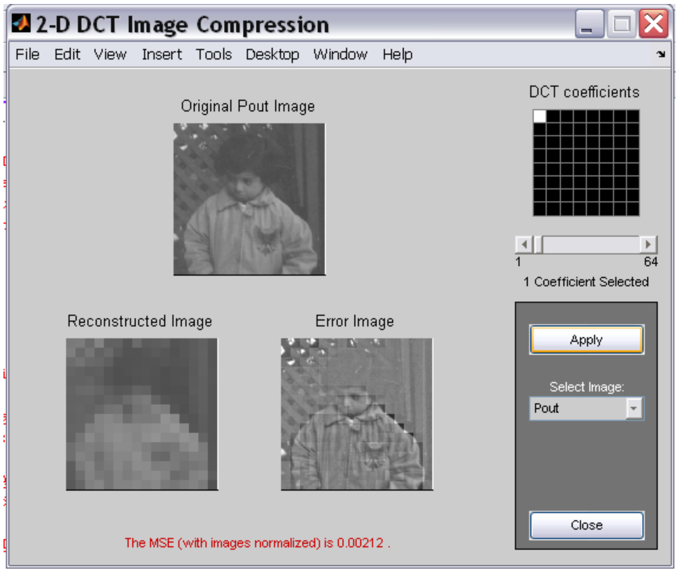
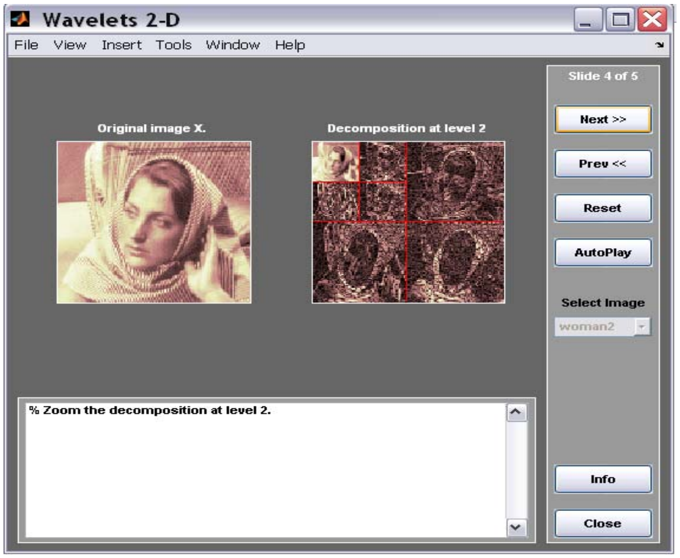


Fig. 6(b). LSB using invisible image



The MSE (with images normalized) is 0.00212 .

Fig. 7. Image is compressed using DCT



% Zoom the decomposition at level 2.

Fig. 8. Image is wavelet using DWT

In LSB, applying of visible image algorithm (Fig. 6(a)) , we can see merge of two images, no intruder can access real image except description. In LSB, applying of invisible image algorithm, we do not see real image, another image is used. So intruder does not take real image.

In DCT method, image is compressed using of number of coefficient of pixels(Fig. 7). If number of coefficient is increased, compressed of image also increased. So it is tough to capture real image.

In DWT method, image is wavelet using wavelet algorithm and high frequency sub band(Fig. 8). So intruder do not get real image except descript of image.

VIII. Conclusion

Digital Image Watermarking can protect image, video, audio from unauthorized person, noise, copyright etc. DCT and DWT 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 and also use JPEG compression method and DWT is used embedded zero-tree wavelet (EZW) image compression scheme and high frequency sub bands as LH,HL,HH etc.

References

[1] Zhao Yuehua, “An image watermark based on Discrete Cosine Transform block classifying” ,

[2] Hye-Joo Lee, Ji-Hwan Park1, and Yuliang Zheng2,” Digital Watermarking Robust Against JPEG Compression”

[3] Xiang-Gen Xia, Charles G. Boncelet and Gonzalo R. Arce. “Wavelet transform based watermark for digital images.”Department of Electrical andComputer Engineering, University of Delaware, Newark, DE 19716

[4] Jashmin K. Shah ECE Department, Temple University, PA 19122, http://astro.temple.edu/~shah

[5] Vallabha VH, “Multiresolution Watermark Based on Wavelet Transform for Digital image.

[6] MATLAB help

AUTHORS PROFILE

Darshana Mistry(ISTE-LM’10). She become a life member ship of ISTE in 2010. Her date of birth is 1st May 1981 in Bharuch. She completed H.S.C from G.S.E.B(Gujarat) in 1998 with 83.67%, B.E.Computer Engineer from S.P.University(V.V.Nagar,Gujarat) with 5.78 CPI in 2002, M.Tech(CSE) from Nirma University(Ahmedabad,Gujarat) with 7.31 CPI in 2009.

She is working as **Coordinator of CE dept., Asst. Professor in Gandhinagar Institute of Technology college, Gandhinagar.** She has 6.8 years experience. She published 1 state level(Gandhinagar, Gujarat, GIT journal,2010), 1national level(Ahmedabad,Gujarat, NUCONE-09-Nirma University,2009), 1 International level paper(V.V.Nagar,Gujarat, ICSSA-09,GCET,2009).