Visible and Invisible Image Watermarking

Bindu Reddy
Dept. of Electronics and Telecommunication
F.C.R.I.T, Vashi,
Mumbai, India

Anita Jadhav
Dept. of Electronics and Telecommunication
F.C.R.I.T, Vashi,
Mumbai, India

***Abstract*— Watermarking is the process of hiding a predefined pattern or any information into multimedia like image, audio or video in a way that quality of multimedia is preserved. Predefined pattern or any type of information represents identity of an author or owner. Watermarking can be done by using various techniques like least Significant Bit (LSB), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) techniques either in visible or invisible way. In this paper, we have implemented image watermarking using Discrete Cosine Transform, Least Significant bit modification, and Discrete Wavelet Transform. In which we understood that DWT technique is fast and less complicated as compared to DCT and LSB bits replacement with 1-bit the distortion observed was low and negligible respectively.**

Keywords*— *Discrete cosine transforms, Discrete wavelet transform, Least significant bit.

I. INTRODUCTION

Watermarking is the method to embed digital information into the original signal [1]. Information has become an important strategic resource as social development. With the technology of Internet developing rapidly, people can easily spread copy, store and process multimedia message such as images, sound, video and text. However, this also leads to a problem of transmission security of multimedia information and copyright protection of digital information. These are mainly manifested in the follows: data files transmitted are easily destroyed and altered through Internet [2]. Digital watermark basically deals with information which is to be embedded in the signal. In other words, difference between cover signal and watermarked signal is digital watermark. Embedding, attacking and detection are the three steps which make a Watermarking system. Input of watermarking system is any signal in form of image, audio or video which is then used for further process. The first step in any watermarking system is to embed data into the host signal. Watermarked signal will be produced by embedding procedure. Now, the watermarked signal is usually transmitted to an individual. If the modification is made by that individual then, it is called as an attack. In copyright protection application, the phrase attack arises. In which, other individuals may try to take out the digital watermark through some amendment. Lossy compression, adding noise or cropping image or video is some possible amendments made by third parties. The last step of a watermarking system is detection. In this step, extraction takes place which is an algorithm applied to the signal which is been used to get back the watermark from the attacked signal. If signal was unchanged during transmission, and if watermark is still present then it may be extracted back by detection procedure. There are various digital watermarking applications

in which robust watermarking includes the extraction algorithm which will produce watermark properly even if the changes are made. The extraction algorithm will not produce watermark properly if the changes are made such type of a watermarking is called as fragile watermarking [3]-[4]. In original signal and watermarked signal there will be no perceptible difference. It is difficult to remove the watermark without damaging the original signal. Digital watermarking technology is mainly applied for copyright protection, operation tracking or piracy tracking, image authentication and copy control [2].

II. TYPES OF WATERMARKING

Various types of watermarking techniques having different applications are given below:

- Robust & Fragile Watermarking: In robust watermarking, if the changes are made to the watermarked image or video which will not change the watermark but in fragile watermarking technique watermarked content is changed which will change or destroy watermark.
- Visible & Transparent Watermarking: watermarking is said to be visible when the content is visible to human eye whereas transparent watermarks are also known as invisible watermarks, in which the content is not visible to human eye.
- Public & Private Watermarking: To detect the watermark, users are authorized in public watermarking whereas in private watermarking users of the content are not authorized to detect the watermark.
- Asymmetric & Symmetric Watermarking: Different keys used for detecting and embedding in asymmetric watermarking whereas in symmetric watermarking same keys are used for embedding and detecting.

III. CLASSIFICATION OF IMAGE WATERMARKING

There are various techniques used to hide any information in images and are classified as:

A. Discrete cosine transform

Signal which is transformed from spatial to frequency representation is done by discrete cosine transform. There are various applications which include DCT technique. Application from spectral methods to lossy compression of images or audio which includes DCTs. Discrete Fourier transform consists of DCT because DFT includes sine as well as cosine. For applications such as compression, cosine function turns out to be more capable. Whereas the cosines express a exacting choice of boundary conditions for differential equation [6]. DCT works either in one-dimensional or two-dimensional which is a separable linear transformation. Two-dimensional DCT is equivalent to one-dimensional performed along a single dimension followed by one-dimensional in the other dimension. [5].

The equation of two dimensional (N by M image) DCT is given by the below equation:

$$F(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}}\left(\frac{2}{M}\right)^{\frac{1}{2}}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1} c(i).c(j).\cos\left[\frac{\pi v}{2M}(2j+1)\right].f(i,j) \quad (1)$$

The resultant inverse 2D- DCT transform is simple by $F^{-1}(u, \mathrm{v})$.

Where,

$$c(\epsilon) = \begin{cases} \frac{1}{\sqrt{2}} & for \quad \epsilon = 0 \\ 1 & otherwise \end{cases} \quad (2)$$

As a real transform, Discrete Cosine Transform (DCT) transforms real data into real spectrum and therefore avoids the problem of redundancy.

1) Algorithm proposed for DCT Gray image watermarking

a) Watermark embedding process consists of 256×256 image that is original image.
b) Dividing original image into 8×8 and then take DCT of each block.
c) The watermark 128×128 image is divided into 8×8 blocks and then taking DCT of each block.
d) Replacing the watermark image at bottom right of original image which is visible watermarking and taking IDCT to obtain watermarked image.

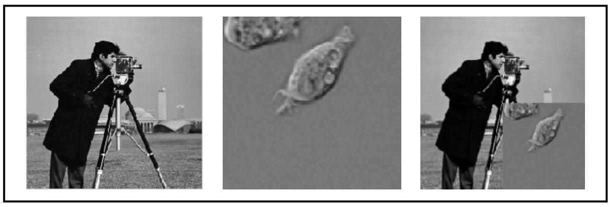


Fig. 1.DCT method_Test1: (a) Original image (b) watermark image (c) watermarked image

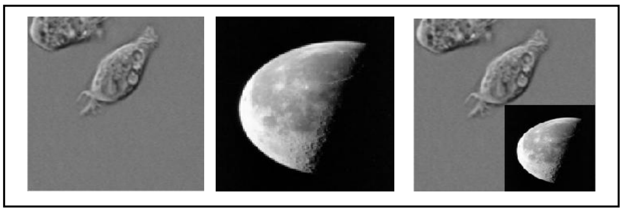


Fig. 2.DCT method_Test2: (a) Original image (b) watermark image (c) watermarked image

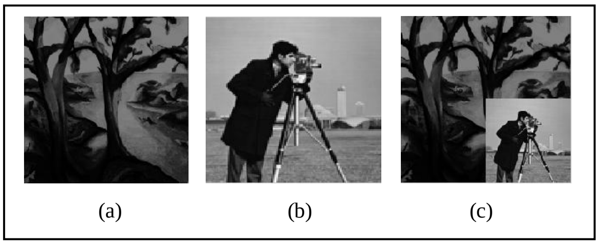


Fig. 3.DCT method_Test3: (a) Original image (b) watermark image (c) watermarked image

B. Discrete wavelet transform

In numerical analysis and functional analysis, a DWT is any wavelet transform for which the wavelets are discretely sampled. Fourier transform can capture only frequency information whereas, wavelet transform has an advantage over Fourier transform because it can capture both frequency and time that is location information. The essential idea of DWT is to separate frequency detail, which is multi-resolution decomposition. There are several time of decomposition. Single level decomposition can divide the main image into four sub graph related as the size of the quarter. The four sub graphs gives low frequency approximate and three detailed sub graphs. Three detailed sub graphs include horizontal, vertical and diagonal direction high frequency details. In the wavelet transform domain, high frequency parts represent detailed information of image's edge, shape and texture and so on. Embedding watermarking in these places cannot be easily detected as people are not easily conscious of it. But after processing, it has poor stability. Most energy of image is centralized in low frequency. Low frequency coefficients are nearly unchanged [5].

LL	**HL**
LH	**HH**

Fig. 4. One level DWT

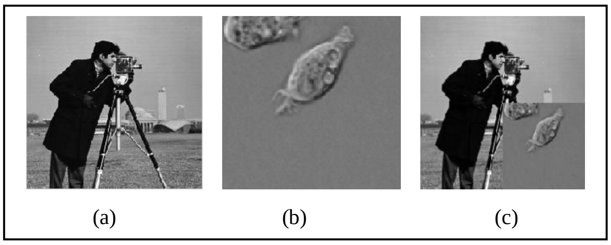
The resulting two-dimensional array of coefficients contains four bands of data, each labeled as LL (low-low), HL (high-low), LH (low-high) and HH (high-high). The LL band can be decomposed once again in the same manner, thereby producing even more sub bands.

1) Algorithm proposed for DWT Gray image watermarking

a) Watermark embedding process consists of decomposing original 256×256 image into 1-level sub bands using DWT which generate Four sub bands (LL, LH, HL, HH).

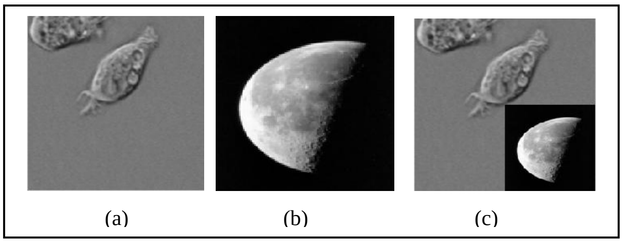
b) The Watermark 128×128 image divided into 1-level sub bands using DWT which generate Four sub-bands (LL, LH, HL, HH).

c) Replacing the watermark image at bottom right of original image which is visible watermarking and taking IDWT to obtain watermarked image.



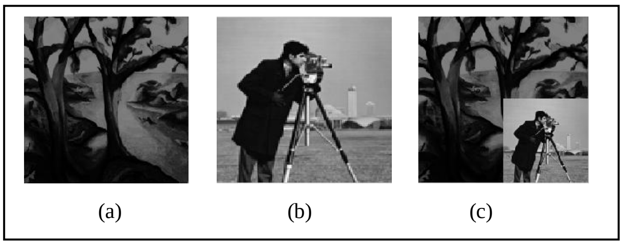
(a) (b) (c)

Fig. 5.DWT method_Test1: (a) Original image (b) watermark image (c) watermarked image



(a) (b) (c)

Fig. 6.DWT method_Test2: (a) Original image (b) watermark image (c) watermarked image



(a) (b) (c)

Fig. 7. DWT method_Test3: (a) Original image (b) watermark image (c) watermarked image

TABLE 1.COMPARSION OF DCT AND DWT DEPENDING ON THEIR ELAPSED TIME

Test images	**Original size**	**Watermark size**	**Elapsed time(secs)**	
			DCT	*DWT*
Test_1	63.7KB	30.3KB	134.056	52.207
Test_2	30.3KB	179KB	98.898	24.273
Test_3	179KB	63.7KB	89.712	22.728

C. *Least significant bit modification*

A new digital watermarking algorithm using least significant bit is introduced. This technique is based on the substitution of LSB plane of the cover image with the given watermark image. LSB is used because of its little effect on the image. In a digital image, information can be inserted directly into every bit of image information or the more busy areas of an image can be calculated so as to hide such messages in less perceptible parts of an image. An example of the less predictable or less perceptible is Least Significant Bit insertion. In LSB technique, cover image is converted to binary image and the least significant bits of the binary image are changed by bits of watermark image. These changes cannot be perceived by the human visibility system. However, a passive attacker can easily extract the changed bits, since it has performed very simple operation. Despite being a simple method, LSB substitution suffers from many drawbacks. Although it can survive transformations like cropping, any addition of undesirable noise or lossy compression but a more sophisticated attack that could simply set the LSB bits of each pixel to one can fully defeat the Watermark with negligible impact on the cover object. Once the algorithm is known to a hacker, the embedded watermark could be easily modified by him/her without any difficulty. LSB substitution however has lots of drawbacks. For e.g.

Pixel Value of Image: 11001010 00110101 00011010…

Watermark: 1 1 1…

Watermarked Image: 11001011 00110101 00011011…

1) *Algorithm proposed for LSB Modification*

a) Watermark Embedding Process consists of 256×256 image i.e. original image, which is converted to binary image.

b) Now, Watermark image 128×128 image is also converted to binary image.

c) Replacing the first 2 rows of watermark image into last column of original image that is 1-bit LSB replacement.

d) Display the image.

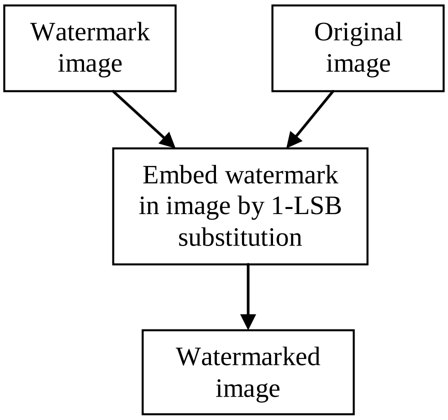


Fig. 8. Algorithm for LSB subsitution

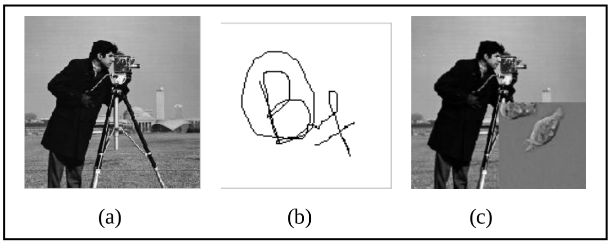


Fig. 9. LSB method_Test1: (a) Original image (b) watermark image (c) watermarked image

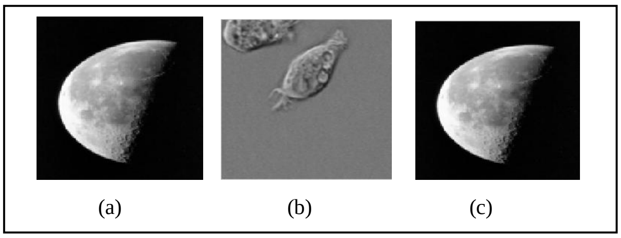


Fig. 10. LSB method_Test2: (a) Original image (b) watermark image (c) watermarked image

IV. CONCLUSION

To simulate results we have used MATLAB @R2009b. A visible watermarking technique has been proposed in the DCT and DWT domain. For image watermarking the DWT technique is fast and less complicated as compared to DCT. For 1 column LSB bits replaced the distortion observed was low and negligible respectively. The distortion observed by replacing 3 LSB bits with original image was visible. Hence, replacing 3 LSB bits would not be a good choice.

REFERENCES

[1] Yu Wei, Yanling Hao and Yushen Li "Multipurpose digital watermarking Algorithm of color image" *in Proceedings of the 2009 IEEE International Conference on Mechatronics and Automation* August 9 - 12, Changchun, China.

[2] Amit Joshi, Vivekanand Mishra1and R. M. Patrikar "Real Time Implementation of Digital Watermarking Algorithm for Image and

[3] Video Application" *in Sardar Vallabhai National Institute of Technology* Surat, india.

[4] Kamrul Hasan Talukder and Koichi Harda, "Discrete wavelet transform for image compression and a model of parallel image compression scheme for formal verification", *in Proceedings of the world congress of engineering,* 2007 vol1,WCE2007,July2-4,2007,London,U.K.

[5] http://en.wikipedia.org/wiki/Digital_watermarking.

[6] Roop Singh, Rekha Gupta "Digital Image Watermarking by using DWT and DCT and comparison based on MSE and PSNR", IEEE, Feb 2012.

[7] Navnidhi Chaturvedi and Dr.S.J.Basha,"comparision of digital image watermarking methods DWT and DWT-DCT on the basis of PSNR" *in International Journal of Innovative Research in Science, Engineering and Technology* Vol. 1, Issue2,December2012.

[8] http://www.cs.cf.ac.uk/Dave/Multimedia/node231.html.

[9] Abdullah Bamatraf, Rosziati Ibrahim and Mohd. Najib Mohd. Salleh," A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit "*in Journal of Computing*, Volume 3, Issue 4, April 2011,ISSN 2151-9617.

[10] Puneet Kr Sharma and Rajni," Analysis of image watermarking using least significant bit algorithm" *in International Journal of Information Sciences and Techniques (IJIST)*, Vol.2, No.4, July 2012