International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 5, May 2017)

A Review on Watermarking Techniques for Encryption

Isha Arora[1], Pardeep Sandhu[2]
[1]M. Tech scholar, ECE Department, Guru Nanak Institute of Technology, Haryana, India
[2]A. P., ECE Department, Guru Nanak Institute of Technology, Haryana, India

Abstract: **Digital watermarking is protection provider for multimedia contents over internet. Now day's very sensitive information pass through network, so the protection for that information is necessary. So as audio, video, images protection we need to protect the image. Image watermarking is a process to hide digital data into image. So due to this way of encryption we can avoid any other person to access data. The main advantage of watermarking is that a user can send data over internet with a faith that no one cannot forge or access its personal. There are so many techniques for watermarking exists in market. In this paper our focus on watermarking concept and compare results of watermarking techniques which already exist.**

Keywords: **- watermarking, DCT, DWT, SVD, and LSB**

I. INTRODUCTION

Enhancement in document for security purpose is required when that document transfer over internet. For that enhancement in document there is a technique that is known as watermarking. Some types of seal or image add with text of document that indicates that information is confidential. The watermark feature in Word is a definite asset for intermediate to advanced users of Word. Text needs full security for a good level because in major websites contents are like paper, legal document, letter, SMS etc. exist. Digital watermarking is a process in which information hide in form of image, audio, video etc. at the receiving side this information is extract that called decryption process. For authentication and identification this information extracted. So they have to protect the data from outside world for illegal accessing of information. So to protect data from illegal authorities there exist many methods like cryptography, watermarking, steganography. Encryption and decryption process of data follow in steganography. In case of encryption data is encrypted and outside world or third parties cannot access it. Then on receiver side after decrypting there is no any provision to protect data from replications. So encryption exists on sender side and decryption exists on receiver side in steganography.

Watermarking technique have been developed in past to protect the data from illegal copies, any forgery with data or prevent copyright.

This technique is proposed for English language text either in use textual or image watermark. There are many ways to forgery with data as like insertion, deletion or recorded a copy of data. The available watermarking techniques are not robust against random tampering forgery (mixing, removing or reordering of pixels). Watermarks composed of both image and text make the text secure and has better robustness [1]. Text document watermarking is shown in figure 1.

Figure 1 Hidden of text in image

In this figure we add text in image that is not possible to find out data. Attacker confuse at this point is this only image or image with text.

Generally two forms of digital watermarking available in market like: visible (perceptible) and invisible (imperceptible). In visible watermarking, watermarks are embedded in such a way that they are visible when the content is viewed. Invisible watermarks are not possible to see but maintain of original from watermark is possible with an accurate decoding technique.

II. WATERMARKING BASED ON DCT

In processing of signal, Discrete Cosine Transform (DCT) is commonly performed as transform function. It transforms a signal from spatial domain to frequency domain. Due to good response, it has been performed in JPEG standard for image compression and decompression. DCT has been implemented in many areas such as data compression, pattern recognition, and image processing, and so on. The DCT transform and its inverse manner can be explained as follows:

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 5, May 2017)

$$F(u,v) = \frac{4C(u)C(v)}{n^2}\sum_{j=0}^{n=1}\sum_{k=0}^{n=1} f(j,k)\cos[\frac{(2j+1)u\pi}{2n}]\cos[\frac{(2k+1)v\pi}{2n}]$$

$$f(j,k) = \sum_{u=0}^{n=1}\sum_{v=0}^{n=1} C(u)C(v)F(u,v)\cos[\frac{(2j+1)u\pi}{2n}]\cos[\frac{(2k+1)v\pi}{2n}]$$

Where C (w) $=\frac{1}{\sqrt{2}}$

When w=0

$C(w) = 1$ when $w = 1, 2, 3 \ldots n-1$

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 8´8 components [2].

Frequency components of DCT block should be high frequency, because of the heavy quantization of coefficients during JPEG compression.

Hence it is better to embed the watermark in mid or high frequency DCT components. If the embedding factor M is chosen small, embedding the watermark in lowest frequency components will be more desirable, because these components are the ones that are least likely to be quantized in JPEG compression. The flow chart of the algorithm is shown in figure 2.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 5, May 2017)

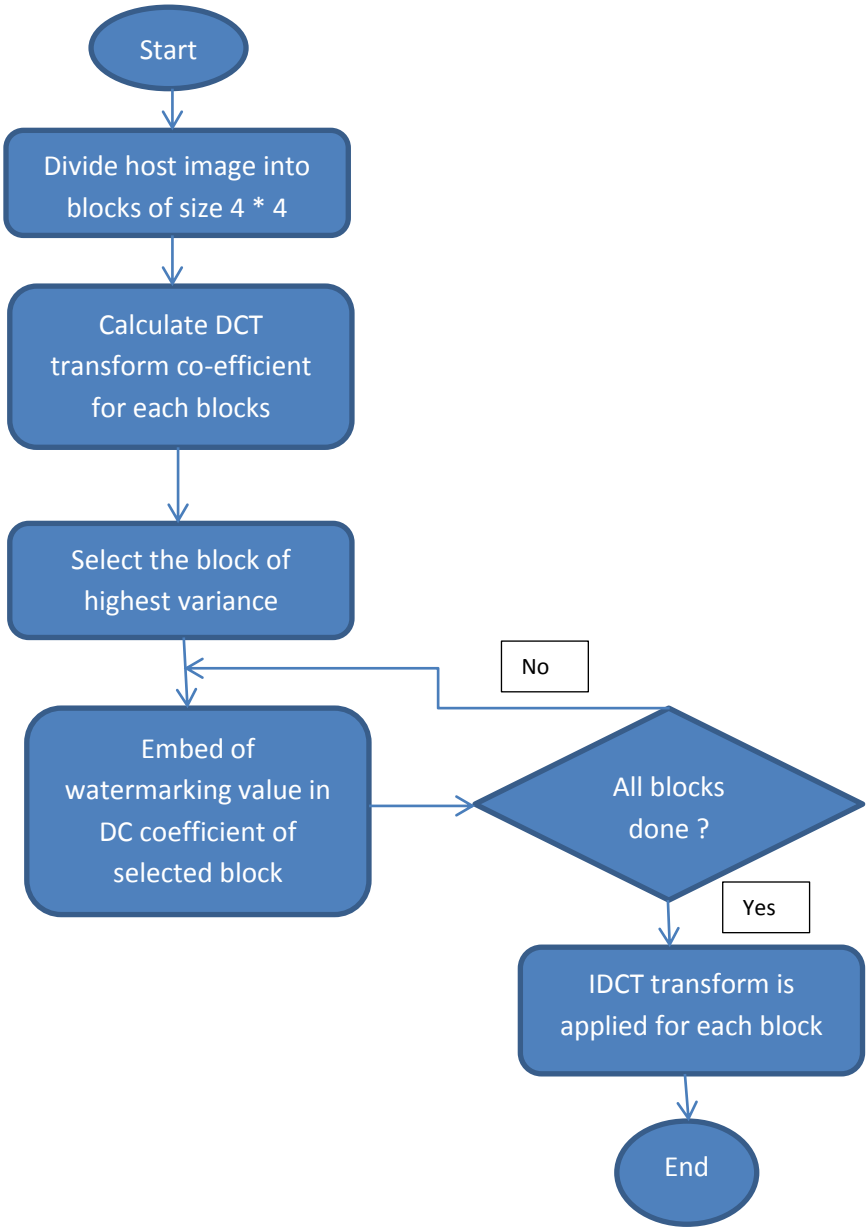

Figure 2: The DCT algorithm flow chart

III. WATERMARKING BASED ON DWT

Wavelet domain is a promising domain for watermark embedding. Wavelet refers to small waves. Discrete Wavelet Transform is based on small waves of limited duration and varying frequency [3].

This is a frequency domain technique in which firstly cover image is transformed into frequency domain and then its frequency coefficients are modified in accordance with the transformed coefficients of the watermark and watermarked image is obtained which is very much robust.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 5, May 2017)

DWT decomposes image hierarchically, providing both spatial and frequency description of the image. Then the image is decomposing in three directions i.e. vertical, horizontal and diagonal in results to separate different components name as LL, HL, LH, and HH. Here letter L and H refers to applying either low pass frequency operation or high pass frequency operations to the rows and the second letter refers to the filter applied to the columns of the cover image [4]. As shown in figure 3

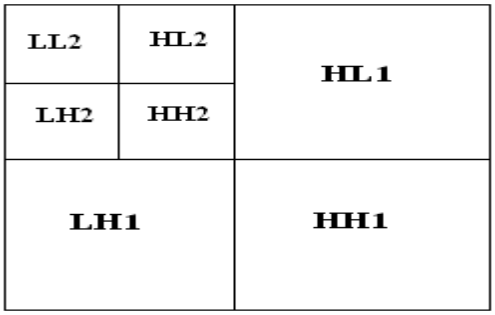

Figure3 Two-level DWT

Algorithm for carrying out DWT: **Step1**. By using DWT, we decompose the original image in some sub-bands, **Step2**. In this step our work is to choose a Sub-band for embedding watermark that should be most suitable, **Step3**. The Wavelet coefficients of the selected sub-band are modified according to the watermark image. **Step4**. After embedding watermark, watermarked image is obtained.

IV. Other Techniques

Exclude DCT and DWT there exist many other techniques for watermarking as following: -

a) Singular Value Decomposition (SVD)

Singular Value Decomposition transform is a linear algebra transform which is used for factorization of a real or complex matrix with numerous applications in various fields of image processing [5]. As a digital image can be represented in a matrix form with its entries giving the intensity value of each pixel in the image, SVD of an image M with dimensions m x m is given by:

$$M=USV^T$$

Where, U and V are orthogonal matrices and S known as singular matrix is a diagonal matrix carrying non-negative singular values of matrix M.

There are two main properties of SVD to employ in digital watermarking schemes [6]:

1. Quality of image does not affect by Small variations in singular values
2. Singular values of an image have high stability so; they do not change after various attacks.

b) Least Significant BIT (LSB)

This is invisible digital watermarking technique, in which we each 8-bit pixel's least significant bit is overwritten with a bit from the watermark. 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. To demonstrate, assume the image uses a 24-bit RGB color model (Figure 4). The first image pixel has a teal green color (0x008080), while the first watermark byte is 0xDC. First, we divide the image pixel into its constituent bytes of red, green, and blue.as shown in figure 4.

0x008080 => r: 0x00, g: 0x80, b: 0x80

Then we divide the watermark byte into pairs of bits. Next we embed each bit pair into bits 1 and 0 of each color byte. So the red byte (0x00) becomes 0x03, the green byte (0x80) becomes 0x81, and the blue byte (0x80) becomes 0x83. We then use these modified bytes to recolor the image pixel. The new pixel color, however, seems to be the same teal color (Figure 4).

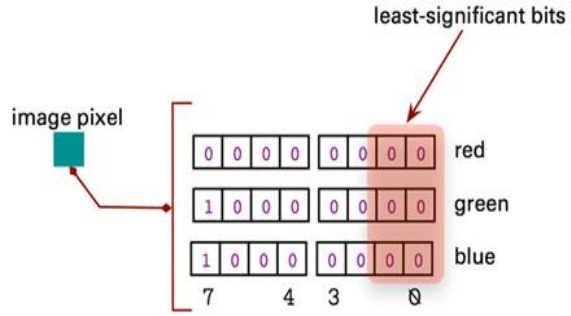

Fig. 4 Example of LSB

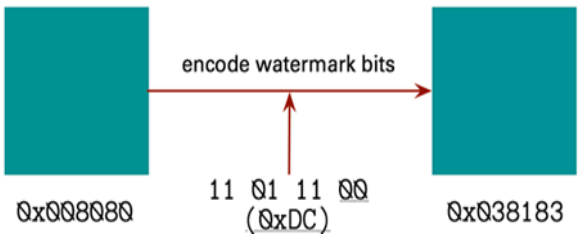

Figure 4 Encoding of watermark bits

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 5, May 2017)

V. COMPARITIVE RESULT

Comparative result of DCT and DWT need GUI first of all.

So they develop DCT GUI and DWT GUI as shown in fig 5.1 and fig 5.2:

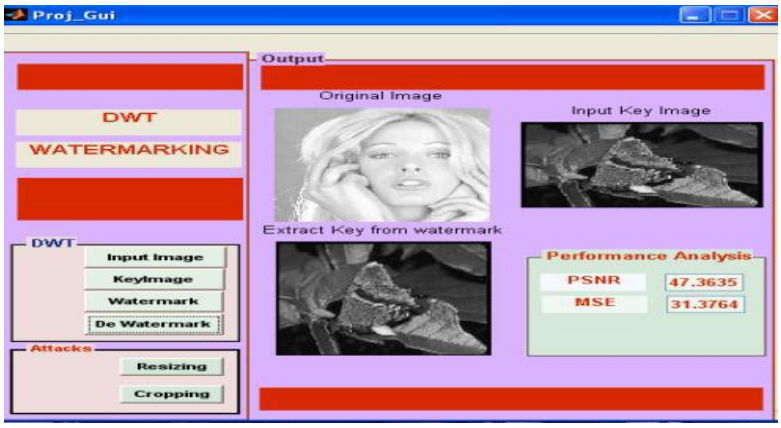

Figure 5.1 GUI for DWT Based Watermarking

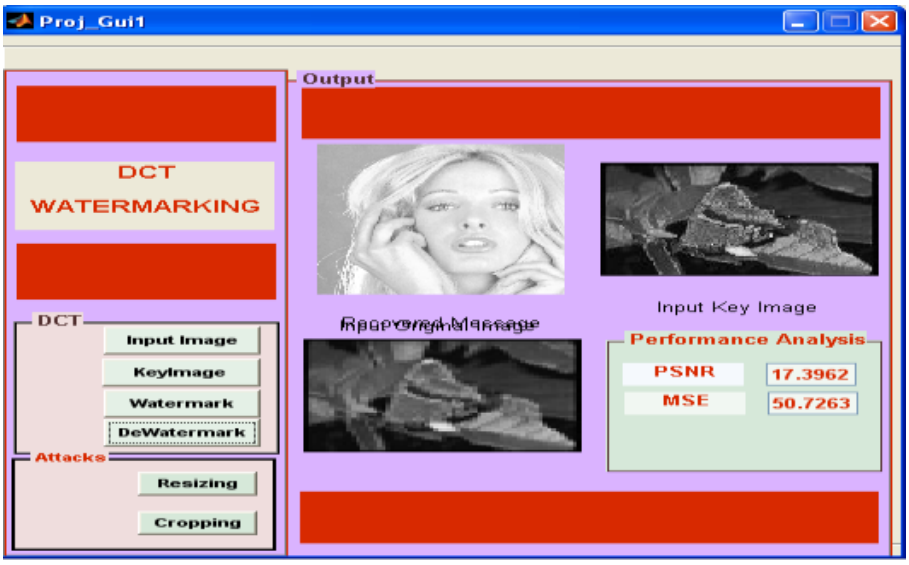

Figure5.2 GUI for DCT Based Watermarking

There is evolution of results on the basis of three images as shown in GUI. Table I show results for imperceptibility

Original image	Key image	PSNR in DWT	PSNR in DCT
SPLASH	0.jpg	91.5	49.02
GIRL	0.jpg	91.5	35.57
MANDRILL	0.jpg	91.5	49.02

So with graph presentation comparison between both techniques can be discussed very well.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 5, May 2017)

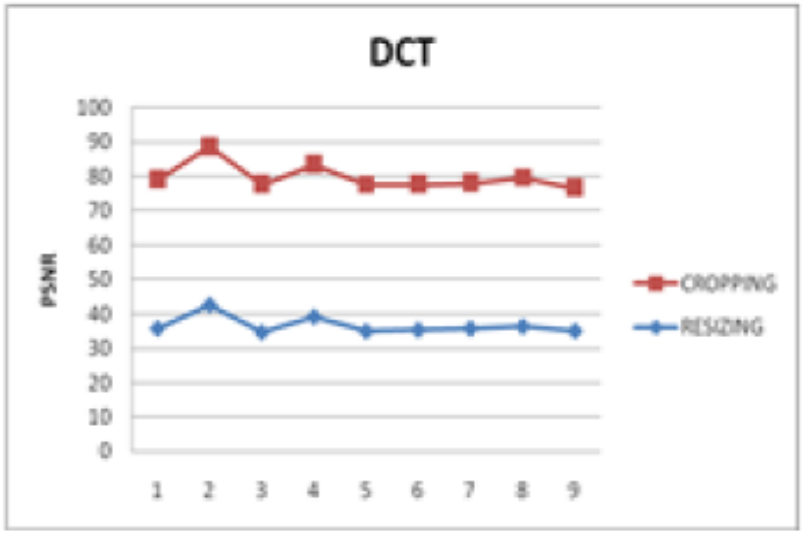

Figure 5.3 PSNR value of DCT with Cropping & Resizing

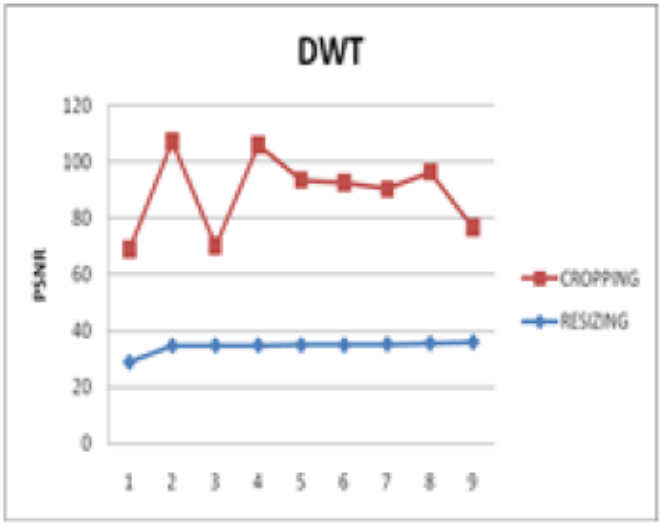

Figure 5.4 PSNR value of DWT with Cropping & Resizing

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 5, May 2017)

Figure 5.3 and figure 5.4 shows the results of DCT and DWT to find PSNR value of the basis of cropping and resizing.

VI. Factors For Marked Image Quality Measure

Many factors are available to measure marked-image quality such as peak-signal to noise ratio (PSNR) and bit correct ratio (BCR). PSNR used to evaluate the imperceptibility of the watermarked-image. PSNR can be found by equation (1) and the robustness of the watermarking measured by BCR using equation (3).

$$PSNR = 10 * log_{10}(\frac{255^2}{MSE})(db) \quad (1)$$

$$MSE = \frac{1}{M*N}\sum_{i=0}^{M}\sum_{j=0}^{N}(I_B(i,j) - I_H(i,j))^2 \quad (2)$$

$$BCR = \left(1 - \frac{\sum_{i=0}^{M}\sum_{j=0}^{N} I_B(i,j)\ \theta\ I_H(i,j)}{M*N}\right) * 100\% \quad (3)$$

Where IH and IB stand for the marked-image and the base-image, respectively, M and N represent dimensions of IH and IB images, and MSE is the Mean Square Error. For imperceptible watermarking, the marked-image should look as similar as the base-image, thus the MSE between the two images in equation (2) should be as small as possible. From equation (1), the higher value of the PSNR leads to less imperceptibility of the marked-image.

VII. Problem Statement

In spatial domain the watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. This type of watermarking is called single level. In LSB we simply shift the bit that exists on least significant due to which attacker can easily guess the method. To prevent this type of attack we need to provide some complexity in it. Other issue is created about robustness. So to keep in mind these issues, we try to think a proposed technique that will robust by nature and difficult to forgery due to its complexity.

VIII. Conclusion

With study of water marking techniques it is described that recent work in text watermarking is that used technique invisible and some aspects for human visual system.

Comparison of existing technique DCT and DWT have done of basis of some parameter like cropping and resizing. The watermark's imperceptibility obtained more in DWT as compare to DCT. From the results and graphs shown above a conclusion arise that DWT work robust in cropping and resizing as compared to DCT. After all the study of recent techniques it found that we need to design a hybrid approach that can handle the issues.

REFERENCES

[1] Jaseena K.U., Anita John," Text Watermarking using Combined Image and Text for Authentication and Protection", International Journal of Computer Applications (0975 – 8887) Volume 20– No.4, April 2011.

[2] Wen Yuan Chen and Shih Yuan Huang," Digital Watermarking Using DCT Transformation", Digital Watermarking Using DCT Transformation.

[3] Chunlin Song, SudSudirman, MadjidMerabti, "Recent Advances and Classification of Watermarking Techniques in Digital Images", ISBN: 978-1-902560-22-9 © 2009 PGNet

[4] M. MohamedSathik, S. S. Sujatha, "A Novel DWT Based Invisible Watermarking Technique for Digital Images", International Arab Journal of e-Technology, Vol 2, no. 3, pp. 167-173, January 2012.

[5] Manjunath. M, Prof. Siddappaji, "A New Robust Semi blind Watermarking Using Block DCT and SVD", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), pp. 193-197, 2012.

[6] L. Demanet, " Curvelets, wave atoms, and wave equations", Ph.D. thesis, Caltech, 2006.