

# A REVIEW FOR DIGITAL IMAGE WATERMARKING TECHNIQUES

Priyanka Bharti ,  
<sup>1</sup>M.Tech Scholar, R.C.E.W ,  
 Jaipur, Rajasthan, India,  
 priyankabharti.eca@gmail.com,

Roshan,  
 Assistant professor,  
 R.C.E.W , Jaipur, Rajasthan, India,

**Abstract :-** Security of multimedia data has a great significance for internet as it provides ease of distribution, duplication & manipulating the data of multimedia format. The field of digital watermarking hides the sensitive original data to protect it from copying & its distribution. This document conducts evaluation over present techniques of digitized watermarking. In the field of digitized watermarking, sensitive data is invaded to protect the rights of ownership of multimedia information over the consideration of domains such as spatial or transform or wavelets. The techniques of spatial domain are implemented over pixels in a straight manner & domain of frequency is implemented over transforms coefficients of a picture. The assessment expands the important methodologies in spatial & transform domain and concentrates over disadvantages & advantages of the technology.

**Keywords:** Digital watermarking, Spatial domain, Least Significant Bit (LSB), Frequency domain, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT) .

## I. INTRODUCTION

Processing of digital images is a field that is developing over fast rate along several implemented applications in the field of engineering & computer science. It is considered to be an important research area as the methodologies are implemented in various applications such as medical visualization, enhancing the image, enforcement of law, restoration of image, artistic effects & digitized watermarking for the security measures. Processing of digitized images has got several advantageous attributes in contrast to processing of analogue images. Digitized image processing accomplish variance of computer functions over digitized images for several applications such as quality of image Digital image processing is accomplishing variant computer operations like improvising quality of image, filtration of noise from images. An image of digital format [1] presents 2-D image in the form of a finite group having digital value termed as elements of picture or pixels. Hence, processing a digitized image by making use of digital computer that is termed as processing of digital image.

The technique based over digitized communication such as internet relates to several issues of privacy concerns & securing the information. The methods for security are needed as there is illegal access to information without any permission. Hence, there is a need for protecting the information in the world of internet. To ensure security of digitized information, several methods such as decryption, encryption, steganography, cryptography & digitized watermarking. In this document, various digitized watermarking techniques are suggested. The digitized watermarking is an application for processing of digital images.

The digital watermarking is an application of the digital image processing.

The process of digitized watermarking is the process for hiding the information. There are several methodologies to hide the information that are of video, text, audio & image format. Generally, the technique of digitized watermarking is for invading some supplementary & secret information in a cover picture that can further be extracted or identified for several uses such as identification of owner, authentication, protection of content & protecting copyright etc. At some moments, factor of scaling is applied for indulging the watermark in a cover picture. The digitized watermarking can be applied for purpose of securing the digitized media & also protection of information for access of illegal users & giving the right of ownership of the digitized content. A cardinal feature of digitized watermarking is calculated in terms of imperceptibility & robustness in contrast to several attacks or general manipulation of image such as scaling, rotation, compression, cropping & filtering etc. The scale of measuring performance of algorithms for watermarking is dependent over robustness of invaded watermark contrasting different attacks. The digitized watermarking is the methodology that is applied for enhancing the right of owner over a picture by replacement of a signal of lower level straightly in the picture. Digitized watermarking technique is implemented for proofing it from temperament & authentication [2].

The field of digitized watermarking is growing at a faster pace & is implemented in several applications with a successful implementation. The digitized watermarking is implemented in numerous techniques of processing an image. The goal of each application is to furnish a level of security for content of digital form. The applications for digitized watermarking are Broadcast Monitoring [3], Digital Fingerprinting [4], Transaction Tracking [5], Copyright Protection [6], Temper Detection [7], Data Hiding [8] & Content Authentication [9] etc.

Each of the technique of digitized watermarking is comprised of two algorithms: one is considered as embedment algorithm, & the second as detecting algorithm. The two processes work in a same fashion for every method of watermarking. A process of embedding a watermark is demonstrated in the figure 1 where watermark is invaded in cover picture by applying the embedment algorithm. The process for recognizing the watermark is demonstrated in figure 2 where detection algorithm is used for revering the watermark.

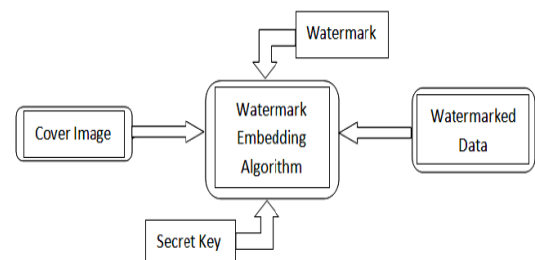


Figure 1. Watermark Embedding Process

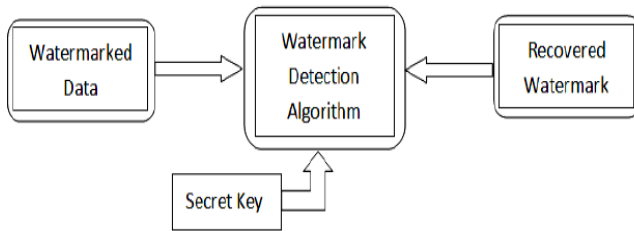


Figure 2. Watermark Detection Process

## II. DIGITAL IMAGE WATERMARKING WORKING

The technique of digital watermarking is implemented in the processing of digital signals for incorporating the information that is hidden in the form of multimedia data. The data invaded cannot be visualized while a précised extractor or detector is observed & the information is extracted. This technique can use the images with digital format to invade the hidden data that is embedded with an image with a watermark & the images with a watermark have more robustness confronting the attacks. The different levels of digitized watermarking are demonstrated in the figure 3. Generally, functioning of watermarking of digitized images is segmented into three levels [10]:

### A. Embedding Stage

This stage is the initial stage where a watermark is invaded in the actual picture by applying the algorithm for embedding & a hidden key. Then the image incorporated with a watermark is produced. Therefore, the watermarked picture is relayed on the network.

### B. Distortion/Attack Stage

In the given stage, transmission of data takes place over whole network. In a case, either some noise is incorporated along the images that are having watermarks or else some attacks were executed over images having a watermark. Hence, data with a watermark is either converted or eliminated.

### C. Detection/Retrieval Stage

In detection stage, a definite detector helps in recognizing a watermark by implementing an algorithm for detection & applying a hidden key. Adding up to this, it is able to identify the noise as well.

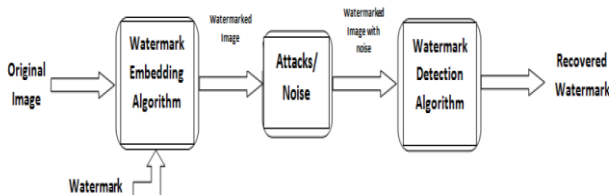


Figure 3. Stages in Digital Image Watermarking

## III. DIGITAL IMAGE WATERMARKING TECHNIQUES

In the domain of digitized watermarking, watermarking of digital images has got fascination of research community for two causes: first cause is that it is easily available & the other one is that it relays lot of

information with redundancy that can be implemented for invading watermarks [11]. Digitized watermarking is comprised of several methodologies for securing the digitized details. The whole of techniques of watermarking the digitized images performs operation in two of the domains that is either transform or spatial domain. The methods in spatial domain function over pixels in straightforward manner. The watermark is indulged by transforming the values of pixels. The techniques of LSB are generally implemented techniques of spatial domain. The watermark is invaded by techniques of transform domain by varying the coefficients of transform domain. The generally implemented techniques of transform domain are DFT, DCT & DWT. By attaining the imperceptibility & robustness, techniques of transform domain work in an effective manner in contrast to methodologies of spatial domain. These two domains are further defined along their implemented methods.

### A. Least Significant Bit (LSB)

The LSB is considered to be the basic methodology of spatial domain watermarking for indulging a watermark in the LSBs of pixels which are randomly chosen for a cover picture. An illustration of the LSB watermarking [12]:

```

Image:
10010101 00111011 11001101 01010101....
Watermark:
           1       0       1       0....
Watermarked Image:
10010101 00111010 11001101 01010100....
  
```

The steps taken for embedding a watermark in the real image by applying LSB [13]:

- 1) Conversion of RGB to the gray scale image.
- 2) Creating twice precision for a picture.
- 3) Shifting MSB (most significant bits) to LSB (least significant bits) of the watermarked pictures.
- 4) Making the LSB of hosted picture to zero.
- 5) Adding the shifted version (as in step 3) of watermarked pictures to the modified version (step 4).

The main lead of this methodology is that it can be easily executed over the pictures. Further, it furnishes transparency for higher perceptual frequency. Further, the watermark is indulged by making use of LSB; there is no effect over quality of the image. The major issue associated to the technique of LSB is that it has bad robustness for function of processing the signals as by this method, it is easy to eliminate the watermark any type of attack over processing of signals. It don't possess vulnerability with respect to attacks & noise but it has much imperceptibility.

### B. Limitations of spatial domain watermarking

The watermarking in the spatial domain is basic in contrast to watermarking implemented in transform domain. The main limitation is the term of robustness in watermarking of spatial domain. It is able to deal with the basic functions such as indulging the noise & cropping.

Other restraint over transformation in spatial domain is that it doesn't permit consecutive processing for enhancing robustness in watermark.

**C. Transform Domain Watermarking**

The watermarking in the domain of transformation has got much success in contrast to the watermarking performed in spatial domain. By the watermarking in transform domain, picture is presented in the type of frequency. By the techniques of watermarking in transform domain, initially the actual image is transformed through a predefined transformation. Further, watermark is invaded in transformed picture or either in coefficients in transformation. At last, inverse transform is implemented for obtaining a picture with watermark [14]. The generally implemented techniques in transform domain are DCT, DFT & DWT.

**D. Discrete Cosine Transform**

The DCT is applied for processing of signals. It leads to transformation of spatial to frequency domain. DCT is implemented over several regions such as recognition of pattern, compression of data & each field of processing the image. Watermarking in DCT has higher robustness in contrast to the methods of watermarking implemented in spatial domain. The main steps of the DCT are [11]:

- 1) Segmentation of the picture in block of 8 \* 8 sizes that doesn't overlaps.
- 2) Implementing forwarded DCT to every block.
- 3) Implementing criteria for selecting the block such as HVS.
- 4) Implementing criteria for selecting the coefficients like highest.
- 5) Invading a watermark by transforming the chosen co-efficient.
- 6) Implementing IDCT (inverse-DCT) transform over every block.

In the DCT, the information of a watermark is invaded by dividing the picture in different bands of frequency. As per the figure 4, constituent of the block with minimal frequency is denoted, in which the component having higher frequency is presented by FH while FM signifies the component with middle frequency that is selected for selecting the position for embedding. The DCT incorporates a better level of robustness in contrast to several attacks for processing the signals by choosing the components of domain that is perceptually signified.

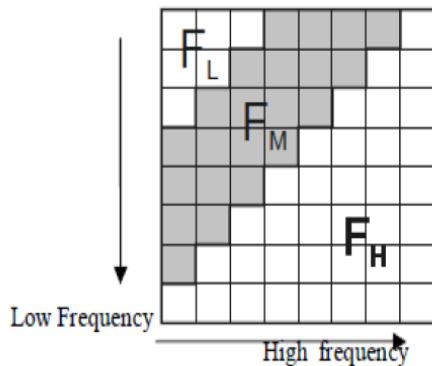


Figure 4. Discrete Cosine Transform Region

By the characterization of DFT (Discrete Fourier Transform), DCT turns the edge of picture for transforming the image as a component of even function. It is considered as a basic linear transformation executed over technology of processing the digitized signals. A 2D-DCT (two dimensional discrete cosine transform) is presented as:

$$F(jk) = a(j)a(k)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} f(mn)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right] \dots(1)$$

The associated inverse transformation (either it is 2DIDCT) is given as:

$$F(mn) = \sum_{m=0}^{N-1}\sum_{n=0}^{N-1} a(j)a(k)F(jk)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right] \dots(2)$$

**E. Discrete Wavelet Transform**

DWT of an image generates multiple resolution presentation of a picture. This presentation of multi resolution furnishes a basic layout to interpret the generation of an image. The DWT evaluates the signal over multi-resolution. The picture is disintegrated by the DWT in quadrants with higher & lower frequency. The frequency with a low quadrant get splinted into two more segments with lower & higher values of frequency and this process goes on till the time complete signal get decomposed thoroughly.

A DWT transform a 2-D picture into four segments: first part is the lower frequency in the real image, the top right corner accumulates the details of the picture, a bottom left corner is comprised of vertical information of the real image, and the bottom side right corner accumulates the higher frequency in the real images. The coefficients with lower value of frequency have higher robustness for indulging a watermark as it is comprised of a bit more data related to the actual picture [2]. The reconstruction of the actual picture from disintegrated image is executed by the IDWT [16].

The DWTs are of scalable form. The DWT are mainly implemented in the watermarking of images of digital format as it has better spatial localization & techniques of multiple resolutions. This fine spatial localization characteristic is easy to for recognizing area in cover picture where watermark get indulged very efficiently.

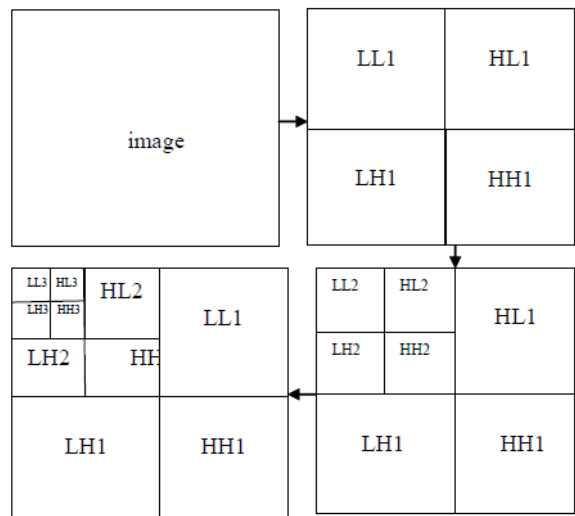


Fig 5:- discrete wavelet decomposition

**F. Discrete Fourier Transform**

DFT (Discrete Fourier Transform) provides robustness in contrast to attacks falling over the geometry parameters like cropping, rotation, translation, scaling etc. DFT helps in disintegration of a picture in cosine & sine format. The methodologies for watermarking constituted over DFT are segregated into two forms: first one is the direct embedment & the second one is embedment on the basis of template.

As per the method of direct embedment, watermark is invaded by varying the magnitude of DFT & coefficients of phase. The method of embedding based over template indulged the theory of templates. The template is considered as a design that is indulged in the domain of DFT for making estimation over factor of transformation. In a process where the image went under the transformation, the image is resynchronized by searching the template & a detector is implemented for extracting the invaded watermark of spread spectrum [11]. The DFT is implemented for the signals of digital format, discrete-time  $f(x)$  & periodicity. The DCT is implemented for a signal that is of period  $M$  that is described as [1]:

$$F(u) = \sum_{x=0}^{M-1} f(x) e^{-\frac{j2\pi ux}{M}} \dots (3)$$

The IDFT (inverse Discrete Fourier Transform) is given as:

$$f(x) = \frac{1}{M} \sum_{u=0}^{M-1} F(u) e^{\frac{j2\pi ux}{M}} \dots (4)$$

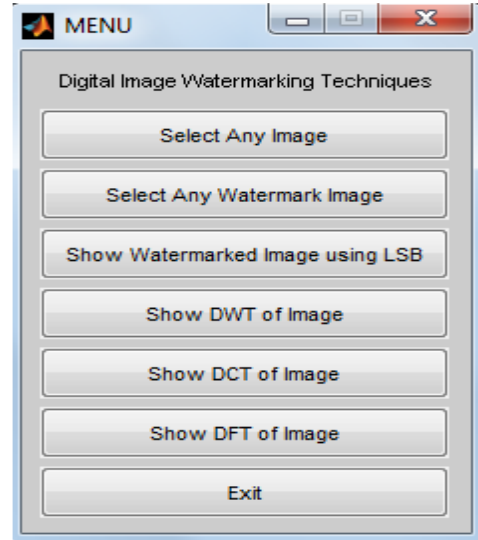
**IV. EXPERIMENTAL RESULTS**

This portion presents the outcomes of experiments carried over watermarking methods in the images of digital format in the MATLAB. The method of watermarking performs in two domains called as: transform & spatial domain. The outcomes generated by the cardinal techniques in spatial domain and also for transform domain are demonstrated below. By the outcomes, initially a GUI is implemented that holds the presentation for outcomes in a very effective manner & implement the very important techniques of spatial & transform domain that are developed.

The techniques are assessed on the picture provided as sample; if it is a RGB or grayscale image having any dimensions and further an image that is watermarked is invaded into the originally chosen picture. After the implementation of technique of LSB in spatial domain, an image with a watermark is produced. In the LSB, a picture with a watermark is incorporated in the least significant bits of the actual picture. At many times techniques like DWT, DCT & DFT of transform domain are implemented to perform functions such as image processing compression pattern identification etc. Further, a transformed picture is produced by implementing the transform domain.

A GUI for methods of watermarking in an image of digital format is presented in Figure 6 (a). In figure (b) the actual chosen image is presented. In figure (c) the selected image with a watermark is displayed. In figure (d) Image having watermark invaded through LSB that belongs to spatial domain. In figure (e) DWT transformation of the real picture is shown. The DWT helps in transforming the picture into

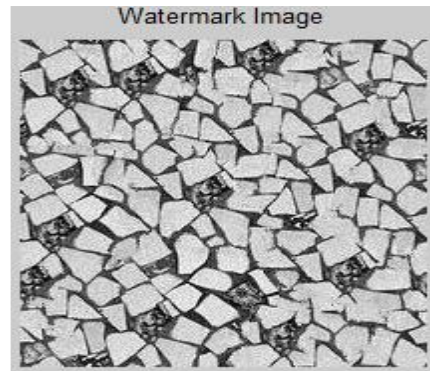
several resolutions. In figure (f) DCT transform of the picture is shown. The DCT leads to transformation of picture in multiple bands of frequency. In figure (g) the DFT transform of the real picture is shown. The DFT leads to transformation of image in cosine & sine format.



a) GUI of Digital Image Watermarking Techniques



b) Original Image

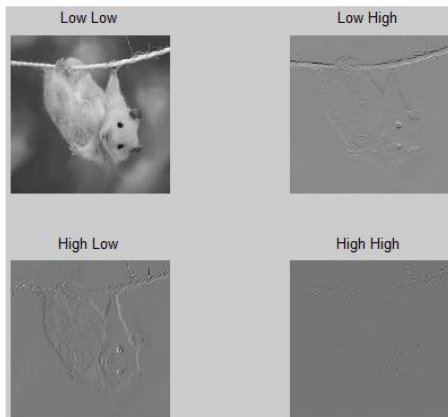


c) Watermark Image

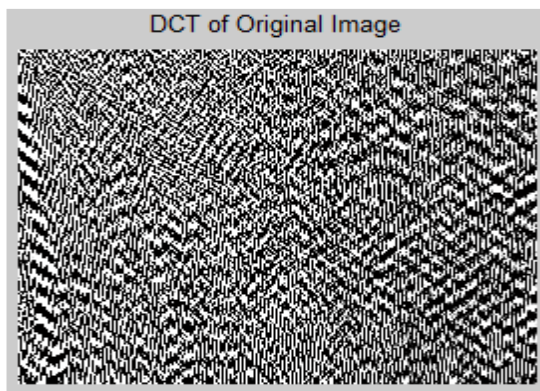




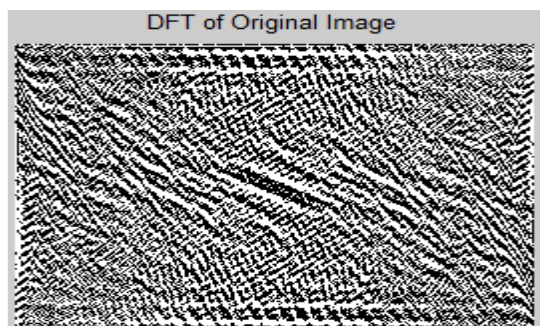
d) Watermarked Image using LSB



e) DWT of Original Image



f) DCT of Original Image.



g) 1-DFT of Original Image

Figure 6. Output Images by use different methodology

## V. CONCLUSION

The technique of digital watermarking is considered to be of very much importance for giving security to media files in digital format over internet. In this document, evaluation is carried over various methods formed over spatial domain (LSB) & transform domain (DWT, DCT & DFT). This analysis presents the strengths & weakness of watermarking techniques.

The field of digital watermarking is still considered as a challenge incorporated with a lot of interesting points, as it don't help in stopping the distribution or copying & is not helpful in dealing with every kind of attack. A future point is developing a genuine robust, secure & transparent watermarking methodology for different forms of media that indulge video, images & audio.

## REFERENCES

- [1] G. Rafael, C. Gonzalez and R. E. Woods, "Digital Image Processing", Third Edition, (2008).
- [2] N. Tiwari, M. k. Ramaiya and Monika Sharma, "Digital watermarking using DWT and DES", IEEE (2013).
- [3] L. Li and X. Li, "Watermarking Protocol for Broadcast Monitoring", International Conference on E business and E-Government (ICEE) (2010).
- [4] D. Zhang, S. Xu, Y. Wang, J. Zhang and Y. Li, "A Digital Fingerprinting Scheme of Digital Image". International Conference on Computational Intelligence and Software Engineerin (CISE) (2010).
- [5] S. Emmanuel, A. P. Vinod, D. Rajan and C.K. Heng, "An Authentication Watermarking Scheme with Transaction Tracking Enabled", Digital Ecosystem and Technologies Conference, 2007.DEST'07 Inaugural IEEE-IES.
- [6] Y.-C. Wang and J.-f. Niu, "Research on Digital Content Copyright Protection System", IEEE International Conference on Network Infrastructure and Digital Content, 2009. IC-NIDC (2009).
- [7] S.-L. Hsieh, C.-P. Yeh and I.-J. Tsai, "An Image Copyright Protection Scheme with Tamper Detection Capability", Symposia and Workshops on Ubiquitous, Autonomic and trusted Computing, 2009.UIC-ATC'09
- [8] Z. Ni, Y.Q. Shi, N. Ansari, W. Su, Q. Sun and X. Lin, "Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication", IEEE Transactions on Circuits and Systems for Video Technology, vol. 18, no. 4.
- [9] J. Zhu, Q. Wei, J. Xiao and Y. Wang, "A Fragile Software Watermarking Algorithm for Content Authentication", IEEE Youth Conference on Information, Computing and Telecommunication, 2009.YC-ICT'09.
- [10] L. Robert and T. Shanmugapriya, "A Study on Digital Watermarking Techniques", International Journal of Recent Trends in Engineering, vol. 1, no. 2, (2009) May.
- [11] V. M. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).
- [12] N. Chandrakar and J. Bagga, "Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of computer Application Technology and Research, vol. 2, no. 2, (2013), pp. 126-130.
- [13] D. Mistry, "Comparison of Digital Watermarking Methods" (IJCSE) International Journal on Computer Science and Engineering, vol. 02, no. 09, (2010), pp. 2805-2909.

- [14] F. Daraee and S. Mozaffari, "Watermarking in binary document images using fractal codes", Pattern Recognition Letter (2013).
- [15] S. A. Khayam, "Discrete Cosine Transform (DCT): Theory and Application".
- [16] S. S. Gonge and J. W. Bakal, "Robust Digital Watermarking Techniques by Using DCT and Spread Spectrum", International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084, vol. 1, no. 2, (2013).
- [17] B. Sridhar and C. Arun, "A Wavelet based Image Watermarking Technique using Image Sharing Method", IEEE (2013).
- [18] K. Deb, Md. S. Al-Seraj, Md. M. Hoque and Md. I. H. Sarkar, "Combined DWT-DCT Based Digital Image Watermarking Technique for Copyright Protection", International Conference on Electrical and Computer Engineering, (2012) December 20-22.
- [19] C. -L. Liu, "A Tutorial of the Wavelet Transform", (2010) February 23.