Techniques of Digital Image Watermarking: A Review

Amit Mehto
M.Tech Scholar
Department of ECE
SATI Vidisha, M.P., India

Neelesh Mehra
Assistant Professor
Department of ECE
SATI Vidisha, M.P., India

ABSTRACT
In today's digital word it is very common to distribute digital image as a part of multimedia technology by use of the Internet. Security of this digital data over the Internet is very popular field among researchers. Watermarking is a process that embeds data or watermark inside data such that it cannot be easily accessed by authorized person. Watermarking provides copyright protection of digital data. Digital Image Water marking is a subfield of Digital watermarking, and it concerns with protection of digital image from unauthorized reproduction and modification. In digital watermarking, a secondary image is a watermark and this watermark lied into the host image and provides protection. Different Digital Image watermarking methods have been proposed in this field to maintain content authentication, copyright protection, tamper protection and many other application.

This paper presents a model for digital image watermarking, properties and applications. Moreover, this paper present a survey on different types of digital Image watermarks. This paper reviews different aspects of digital image watermarking for protecting digital data and provide review of digital image watermarking methods named: Least Significant Bit (LSB), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD).

General Terms
Watermarking, Digital Image Watermarking, Copyright protection, Least Significant Bit.

Keywords
Discrete Wavelet Transform, Discrete Cosine Transform, Peak Signal to Noise Ratio.

1. INTRODUCTION
Over the last few years, security of digital data has been a popular topic due to the development of multimedia techniques because of World Wide Web. Rapid development of Internet increases the copyright protection issues for multimedia data. Traditional security mechanisms based on cryptography has its own limitation. The digital watermarking overcomes the limitations of traditional security mechanisms. Digital watermark was first discovered in 1992 by Andrew Tirkel and Charles Osborne [1].Watermark is derived from the German word "Wessmark".

Digital watermarking is the process of adding a watermark on digital images or files without noticeable altering the image itself and verifies the authenticity of the image. It provides proof that it is copyrighted to a particular person and it cannot be owned by third party. It is like a digital signature, which gives the image a sense of ownership or authenticity [2]. Multimedia contents such as text, image, video and audio has been widely used because of rapid development of Internet technology. Now using digital image watermarking humans can easily distribute or access any multimedia data from Internet.

In present, copyright protection of digital data is very important. Copyright provides protection of digital data against duplicate data. In multimedia attackers can easily produce copy of original digital data exactly without quality loss. The main objective of watermarking is not limited to access of the original content, but it also ensures recovery of the embedded data. Figure 1 describes the basic block diagram for embedding watermark into original image. The watermark is embedded into original image using a watermarking algorithm. The process gives a watermarked image. Figure 2 describes extraction process in watermarking. In this process a watermarked is extracted from the watermarked image.

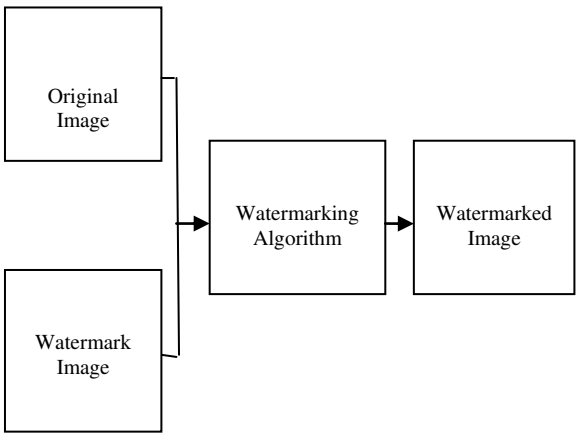


Fig: 1 Embedding algorithm for watermarking

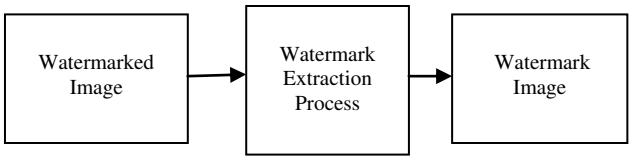


Fig: 2 Extraction process for watermarking

Watermarking can be seen as a special type of steganography. Watermarking is very similar to steganography but the basic difference is that in steganography a secret message is embedded in the image and the image has no relation to the secret message. The digital image is merely used as a cover to hide its existence. In digital watermarking a watermark or digital message is embedded inside another digital data so that the data cannot be easily accessed by third party. The two messages i.e. watermark and original data are related to each other [3]. In past few years, numerous digital watermarking have been proposed, which is based on different sets of criteria. According to the working domain watermarking can be categorized into two types: spatial domain techniques and frequency domain techniques. In Spatial domain, watermark is embedded by changing pixel values of the host image. In Frequency domain, watermark is added to the values of its

transform coefficients. After this perform the inverse transform to get the watermarked image. Frequency domain includes DCT (Digital Cosine Transform), DFT (Digital Fourier Transform), and DWT (Digital Wavelet Transform).

According to the human perception watermarking is of two types, visible and invisible watermarking. A visible logo, which is superimposed on television picture, is an example of visible watermarking. Visible watermark is applicable only for images. On the other hand invisible watermark is hidden inside a multimedia object, which can be extracted by an authorized watermarking algorithm. Figure 3 (a) shows visible and 3 (b) shows invisible watermark image.

Fig: 3(a) Visible watermarked image (b) Invisible watermarked image

This paper is organized as follows. Section 2 is focused on applications of digital image watermarking. Section 3 describes different techniques of digital watermarking. Section 4 describes various properties of image watermarking. Section 5 describes performance metric in digital watermarking. Section 6 describes attacks on system. Section 7 represents results and gives relative comparison of digital image watermarking techniques. Finally section 8 concludes this paper.

2. APPLICATION OF DIGITAL IMAGE WATERMARKING

There are a lot of watermarking applications for images. The applications are as follows [4] [5]:

2.1 Copyright Protection

The copyright content can be inserted as a watermark into the host image. The copyright protection can be used to provide information about ownership authentication of the watermarked image. It gives the evidence to provide information who is the owner of this image [6]. Copyright provides protection of digital data against duplicate data. Copyright information can be embedded as a watermark whenever a new work is produced. This watermark can be used as evidence, if any dispute in ownership of the digital data.

2.2 Fingerprinting

The fingerprints provide information about the legal receiver by embedding information in the image. It associates unique information about each distributed copy of digital data. Watermarking is an appropriate solution for fingerprint application because it is invisible and inseparable from the original data [7]. Prevention of unauthorized copying is done by inserting information about how often an image can be legally copied [8].

2.3 Tamper Detection

If the watermark is modified or destroyed or degraded, this indicates presence of tampering and hence digital content cannot be trusted [9]. Tamper detection can be done with the help of fragile watermarks.

2.4 Medical Application

The medical reports are very important for treatment of the patient. Visible watermarking can be used to print the names of the patients on the X-ray reports and MRI scans. It could create a disaster, if there is a mash up in the reports of two patients [10].

2.5 Broadcast and Publication Monitoring

Digital watermark can also add inside broadcast video and audio. The embedded watermark can also be detected with the help of specialized software and hardware. A visible logo on a corner of television picture is a good example of visible watermark.

2.6 Image and Content Authentication

An image authentication application is used to detect modifications to the image data. A solution called digital signature can be borrowed from cryptography, as a message authentication method. Digital signature represents some kind of summary of the original content. If any part of the original content is tempered or modified, then the signature, will make it possible to detect it. Trustworthy digital camera is one of an example of digital signature method which is used for image authentication [11].

2.7 Convert Communication

The embedded data or watermark can be employed in the transmission of secret message from one person to another or from one computer to another computer, devoid of anyone that a secret message is being transmitted [12]. This application is related to exchange of secret messages which is inserted within an image. In this exchange the hidden data should not give any suspicion that a secret message is inserted into the image.

3. DIFFERENT TECHNIQUES OF DIGITAL WATERMARKING

Watermarking is not a new phenomenon. In this modern era, providing authenticity to digital data is an important issue as most of the world's digital information distributed over the Internet. Digital watermarking is broadly classified into two categories: Spatial Domain techniques and frequency domain techniques. The reviewed watermarking algorithms are classified and described in the following subsections.

3.1 Spatial Domain Techniques

In Spatial domain techniques the watermark is appended inside intensity values. It adds the watermark by changing the pixel values of the host image [13]. This method is characterized by low computational complexity and simplicity. The secret random key, the information associated with the signature and the masking property of the image are the three factors that determine the parameters of spatial domain watermarking algorithm [13].

Commonly used techniques in spatial domain are given below:

3.1.1 Least Significant Bit

Least Significant Bit (LSB) is the frequent used approach in spatial domain. It appends watermarks in the LSB of the

pixels. In LSB large amount of watermark bits can be easily replaced the least significant bits of an image. Least significant bit of an image does not contain visually significant information hence the LSBs can be replaced by watermark image for protection. The LSB is easy to implement and does not create any serious distortion to the image. In LSB an attacker could simply randomize all LSBs hence, it is not very robust against attacks [14].

3.1.2 Salient Point Modification

This method is based on the modification of salient points in the image. Salient points are isolated points in an image [15].

3.2 Frequency Domain Techniques

This technique is more applied as compare to spatial domain technique. In this technique watermark is embedded to the values of its transform coefficients. Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT) are the most commonly used transforms. The DWT and DCT are implemented very effectively in many digital images watermarking techniques. The Human Visual System (HVS) are better captured by the transform coefficients, this is reason to apply watermarking in frequency domain. From past few years Singular Value Decomposition (SVD) is also implementing very effectively in the digital image watermarking scheme.

Al-Haj [16] has been presented a combined DWT-DCT digital image watermarking algorithm. Watermarking is carried out through the embedding of the watermark in the first and second level DWT. Sub-bands of the host image sub-sequenced by the application of DCT on the selected DWT sub-bands.

Commonly used transforms in frequency domain are given below:

3.2.1 Discrete Cosine Transform

Discrete Cosine Transform (DCT) is a transformation function which transforms image from spatial domain to frequency domain. It applies direct transform to entire image or block wise. DCT is same as Discrete Fourier Transform [17]. It converts signal into elementary frequency components [18]. It shows data in terms of frequency domain rather than an amplitude domain. Audio compression method uses one dimensional DCT. The time is the only dimension of interest in audio. Image compression method uses two dimensional DCT. In this method vertical and horizontal dimensions are considered. Equation 1 gives the formula for calculating 2-D DCT and equation 2 gives the formula for inverse 2-D DCT.

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

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

Where $C(u), C(v) = \begin{cases} \sqrt{\frac{1}{N}}, u, v = 0 \\ \sqrt{\frac{2}{N}}, u, v = 1,2 \ldots . N-1 \end{cases}$

In DCT an image is divided into 8x8 block of samples. After this there is a mapping between each of these 8x8 blocks of samples of the original image and the frequency domain. It is shown as a composition of basic DCT functions. This function use appropriately 64 coefficients, and these coefficients represent different horizontal and vertical intensities.Many standardized image, audio, and video compression methods use DCT. DCT has the superiority in reduction of the redundancy of a wide range of signals.

DCT based watermarking methods are robust as compare to spatial domain methods on image processing operation like brightness, low pass filtering and contrast adjustment, blurring etc. However these methods are weak against geometric attacks like cropping, scaling, rotation etc. DCT based watermarking methods are divided into two techniques: Global DCT watermarking and Block based DCT watermarking. In Global DCT the transform is applied to all the parts of the image. However in Block based DCT the transform is applied to a specific part of the image.

Yang et al. has been proposed a DCT domain based removable visible watermarking algorithm [19]. This algorithm defeats illegal removal and resisting compression. It provides protect to the multimedia content. It also ensures high quality of the reconstructed images for authorized persons, or else, low-quality for unauthorized persons by appending the visible watermark. Adaptive scaling and embedding factor scan be determined by the use of a mathematical model which is based on HVS features. Extended version of this method can be applied to other transform domain. Lossless recovery can be easily implemented using Integer transform as it avoids rounding error.

Fangjun Huang et al. have been proposed a hybrid SVD-DCT watermarking method based on LPSNR [20]. This method embedded a digital watermark which combines the singular value decomposition (SVD) and the discrete cosine transform into the host image. More transparency can be easily obtain by embedding, only the singular values (SVs) of a recognized pattern. A part from this, adaptation of LPSNR can easily takes the highest possible robustness without losing the transparency and degrading image quality.

Cox et al. have been proposed an idea to embed watermark by the use of spread spectrum in the discrete cosine transform [21]. This method considers the host image as a communication channel and the watermark as a signal to be transmitted. Spreading with the watermark message is the important part of this method. If an attempt is made to destroy the watermark then the watermarked image will be damaged. This method is not a blind watermarking scheme because the host image is required for watermark extraction. In general, spread-spectrum method can be used to embed the watermarks in wavelet coefficients for images and video [22].

Langelaar et al. has been proposed a method called Optional differential energy watermarking of DCT [23]. It encoded images and video. A block is inserted with a watermark bit by dividing the block into two parts. The block is composes of several 8x8 DCT blocks. An energy difference is produces in the two parts of the same block, and the energy difference is determined by the watermark bit. The method discards the High frequency DCT coefficients in the compressed bit stream. A minimal cut-off index for watermarking, JPEG quantization, and step size are the three parameters in this technique.

3.2.2 Discrete Wavelet Transform

The wavelets are discretely sampled in a discrete wavelet transform (DWT). Wavelets have energy and energy concentrated in time hence it is well suited for the analysis of transient, time- varying signals. Signal processing application, such as in video and audio compression, the simulation of wireless distribution antenna and removal of noise in audio is the major field where DWT is currently used. In DWT robustness can be easily achieved by increasing the strength of the embedded watermark, but this would increase visible distortion of image. However, DWT is much preferred because it provides both a frequency spread of the watermark and a simultaneous spatial localization within an original image.

In one dimensional signal, the DWT has two parts. Part one is low frequency part and part two is high frequency part. The low frequency part is divided into two parts and the same process will continue till the desired level of frequency. The edge components information of the signal contains the high frequency part of the signal.

Now DWT decomposition on an image has four separate parts. The four parts are approximation Image (LL), horizontal (HL), vertical (LH) and diagonal (HH) for detail components. The input signal of DWT decomposition must be multiple of 2n, where, n gives the number of level. DWT has sufficient information and requires less computation time to analyze and synthesize the original signal. Robustness of the watermark can be increase by embedding the watermark data into these four resigns [6]. Figure 4 shows a one dimensional DWT decomposition process.

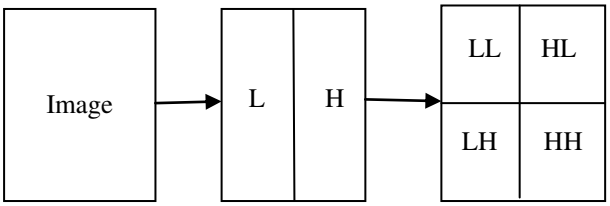


Fig: 4 Single level decomposition using DWT

Shaikh et al. have been proposed a watermarking technology which based on discrete wavelet transformation and embedded a random and a text watermark for testing [24].The watermarks consequently embedded were established to be perceptually non-obstructive on six different gray level images and an mpeg color video. A comparison between the proposed work and an earlier work was carried out and the results were found to be encouraging.

Composition of DWT-SVD method is found to be more robust than the DWT-based method. However, the DWT-SVD method holds the disadvantage of the SVD method and so it is found to be vulnerable against cropping attacks. Hence Jung-Chun Liu et al. has been proposed a method which is the composition of DWT and SVD and it is multi-scale Full-Band Image Watermarking scheme [25]. This method uses the advantages of both DWT and SVD method like robustness against cropping attacks, and robustness against geometric attacks like rotation and scaling and non-geometric attacks respectively. Results show that the multi-scale Full-Band Image which is based on DWT-SVD Watermarking scheme is more robust than the DWT-SVD method.

Abou Ella Hassanien has been proposed a digital watermarking algorithm for copyright protection that based on the concept of modifying frequency coefficients in DWT [26].

3.2.3 Discrete Fourier Transform

Discrete Fourier Transform (DFT) transforms an image from spatial domain to frequency domain. One of the advantages of DFT is that the magnitude and phase of an image in frequency domain can be separated.

The 2D-DFT of an image f(x,y) of size M×N is given by an equation 3 .

$$F(u,v) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)e^{-j2\pi(\frac{ux}{M}+\frac{vy}{N})} \quad (3)$$

Yen-Chung Chiu et al. has been proposed a method for embedding a watermark into a colour image. The embedding is based on coding and synchronization of coefficient-value. Coefficient value is located in the peak locations of the DFT domain [27]. This method embeds the watermark through creation of peaks symmetrically and circularly in the middle frequencies. A part from this, the method uses a combinatorial operation for coding of the peak locations.

In order to create a watermark the positions of the coefficient-value peaks are mapped and identified within a combinatorial operation in the watermark extraction process.

The embedded robust watermark is capable to survive print-and-scan operations. Their method provides protection of image copyright of the owner. Nevertheless, in this watermark embedding technique, the capacity of a normalize image is not enough for hiding a common logo image.

3.2.4 Singular Value Decomposition

Singular Value Decomposition (SVD) gives numeric analysis of linear algebra. SVD is used in many applications of image processing. SVD decomposes a matrix with a little truncate error according to the equation 4 [28].

$$A = USV^T \quad (4)$$

Where A represents the original matrix, U and V represents orthogonal matrices with dimensions M x M and N x N respectively, S represents diagonal matrix of the Eigen values of A and T represents matrix transposition.

R. Liu and T. Tan have been represents the decomposition of the cover image. To get the equation 5 using the scale coefficient α for adding watermark is given by [29]:

$$S + \alpha W = U_W S_W \quad (5)$$

Multiplying matrices U, S_W and V^T result in the marked image A_w:

$$A_W = US_W V^T \quad (6)$$

This is possible due to the high stability of singular value of SVD.

Chin-Chen Chang et al. have been proposed a watermarking scheme based on the SVD domain [30]. Watermark embedding is done by U matrix of SVD. In other words, watermark
embedding is done by calculating the absolute difference between the two rows of U matrix. The positive relationships between the rows of U and V matrices that are preserved after JPEG
compression is explored by this method.

Ghazy et al. have been proposed an approach [31]. In this the cover image is divided into blocks and the SVD applied to each block. In this approach the dimension of watermark must be equal to the block size and a copy of the watermark must be embedded in each block. This technique increases

watermark robustness and provide protection against many kinds of attacks.

Singular values show the algebraic properties of an image

[32]. Singular values contain the geometric and algebraic invariance to some extent. Singular values contain the following properties [28]:

3.2.4.1 Property 1 (SVD)

If $\in R^{m\times n}$, then there exist orthogonal matrices $U = [u_{1,\ldots\ldots,}u_m] \in R^{m\times n}$ and $V = [v_1, \ldots, v_m] \in R^{m\times n}$ such that $U^T AV = diag(\sigma_1, \ldots., \sigma_p)$.where $p = \min(m, n)$, $\sigma_1 \geq \sigma_2 \ldots \sigma_p \geq 0. \sigma_i, i = 1,2, \ldots p$ are the singular value of A. The singular values are the square roots of the Eigen values $\varphi_i of\ AA^H\ or\ A^H A$, that is $\sigma_i = \sqrt{\varphi_i}$.

3.2.4.2 Property 2 (The Scaling Property)

If the singular values of $A^{m\times n}$ are $\sigma_1, \sigma_2, \ldots, \sigma_k$ the singular values of $\alpha * A^{m\times n}$are $\sigma_1^*, \sigma_2^*, .., \sigma_k^*$ then$|\alpha|(\sigma_1, \sigma_2, \ldots \sigma_k) = (\sigma_1^*, \sigma_2^*, \ldots \sigma_k^*)$.

3.2.4.3 Property 3 (The Rotation invariant Property)

If P is a unitary and rotating matrix, the singular values of PA (rotated matrix) are the same as those of A.

3.2.4.4 Property 4 (The Stability of SV)

The stability of singular value represents that, whenever there is a little disturbance with matrix A, the variation of its singular value is not greater than 2-norm of disturbance matrix. 2-norm is equal to the largest singular value of the matrix.

3.2.4.5 Property 5 (The Translation invariance property)

The original image A and its rows or columns interchanged image have the same singular values.

3.2.4.6 Property 6 (The Transposition invariance property)

If $AA^T u = \varphi^2 u$ then $A^T AV = \varphi^2 v$, so that A and A^T have same singular values.

Due to the above mentioned properties, the watermark can be retrieved effectively from the attacked watermarked image. Hence the above mentioned properties of SVD are very much desirable in image watermarking.

SVD technique is considered as a powerful methods for robust image watermarking [33] and [34]. SVD has the attributes:

1. SVD can be applied on both rectangular and square matrices.
2. SVD obtains both non-symmetric and one-way properties, which cannot be preserved using DFT or DCT.
3. Digital image has stable Singular value (SV). The SVs remain unchanged when disturbances are applied to an image.
4. Intrinsic algebraic properties of a digital image can easily be represented by SVs.

Chandra et al. have been proposed a method based on the SVD of both the host image and visual watermark [35]. Scaling factor and the SVs of the watermark are multiplied and then added to the SVs of the host image. The attacks used in this method are low pass filter and JPEG. However this method is non-blind in nature.

4. PROPERTIES OF WATERMARKING

Watermarking systems have number of properties [36], [37]. Requirements of the system decide the relative importance of each property. The properties presented here are related to watermark embedded, watermark detector, or both.

4.1 Fidelity

It can be define as a perceptual similarity among the watermarked and un-watermarked works at the point at which they are presented to a customer [37]. It can also be defined as a measure of imperceptibility of watermark. Watermarking reduces commercial value of the watermark image so it should not introduce visible distortion to watermark image.

4.2 Effectiveness

It defines the probability that the message in a watermarked image will be correctly detected. Ideally the effectiveness probability should be 1.

4.3 Data Payload

Data payload can also call as capacity of watermarking. It can be define as maximum amount of information that can be hidden without degrading image quality. Data payload evolution can be done by the amount of hidden data. This property describes how much amount of data should be added inside the image as a watermark so that it can be successfully detected during extraction process.

4.4 Robustness

Robustness is a property that can stand against piracy attacks or image processing. It means that the piracy attacks should not affect the embedded watermark. In a watermarked image there should be an invisible watermark as a backup, if the visible watermark is removed during an attack. The invisible watermark is added to the source image while the visible watermark is inserted into it. Therefore, in this way a dual watermarked image can be created by inserting a watermark within a watermark. There is another method of developing robust watermarking. This method adds watermark at more than one position in the source image. If one or two watermarks are removed then the other is there.

4.5 False Positive Rate

It can be define as an identification of a watermark from a cover work which does not contain one in reality. A false positive rate, defines number of false positives that can be anticipate happening in a given number of runs of the detector.

4.6 False Positive Rate

It is very important and desirable property. A watermark should be secret and only be accessible by authorized persons. If an unauthorized person wants to access the watermark then it must be undetected. Cryptographic keys are normally used to achieve the watermark. In general, every user has the details of a digital watermark algorithm. For embedding and extracting process a watermark signal with a special number is used. This special number is used for confirmation of legal owner of the digital data. Hence security is a major concern. Watermark systems use three types of keys: private-key, public-key and detection-key. In general, the anti-reverse engineering research algorithm should not be able to remove watermark.

4.7 Computational Complexity

Computational complexity describes the efficiency and cost of the algorithm in terms of time and space used by algorithm, so it should be at a reasonable cost [38]. Computational complexity describes the amount of time watermarking algorithm takes to encode and decode. Computational complexity is needed to ensure security and validity of watermark. Conversely, real-time applications necessitate both speed and efficiency.

5. PERFORMANCE PARAMETERS USED IN IMAGE WATERMARKING

This paper considers performance metrics to calculate the performance of watermarked image. The performance metrics are Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE) and Signal to Noise Ratio (SNR).

5.1 Mean Square Error (MSE)

It is measured by an average squared difference between reference image and watermarked image. It is measured by the formula given below.

$$MSE = \frac{1}{XY}\left[\sum_{i=1}^{x}\sum_{j=1}^{y}\left(c(i,j) - e(i,j)\right)^2\right] \quad (7)$$

Where,

X and Y are height of the image.

c (i, j) is the pixel value of the cover image.

e (i, j) is the pixel value of the embed image.

5.2 Peak Signal to Noise Ratio (PSNR)

It measures the degradation in the watermarked image with respect to host image. To measure the quality of a watermarked image, the peak signal to noise ratio is used. It is measured by the formula given below:

$$PSNR = 10\log_{10}\frac{max^2}{MSR} \quad (8)$$

5.3 Signal to Noise Ratio (SNR)

It measures the signal strength relative to the background noise. It is measured by the formula given below:

$$SNR = 10\log_{10}\frac{P_{signal}}{P_{noise}} \quad (9)$$

Where,

P_{signal} measures the signal strength relative to P_{noise} (the background noise).

6. ATTACKS ON WATERMARKING

Transmission media are not perfect. It can cause impairments in the signal. These impairments implies in a damaged content. Attacks can be categorized as intentional or accidental [39]. Intentional attacks use all available resources to modify or destroy the watermark. It makes it impossible to detect it. The methods used in intentional attacks are: signal processing techniques, cryptanalysis, and stag analysis. Whereas accidental attacks are inevitable. In every image transmission noise can cause distortions. A part from these types, there are other types of attacks called estimation based attacks. In estimation based attacks, estimates of either the watermark data or the original object can be obtained using stochastic methods. Estimation based attacks can be categorized as removal, protocol, or de synchronization depending on the method uses for estimation [40].

6.1 Removal and Interference Attacks

Removal attacks causes removal of the watermark content from the watermarked object. Such attacks target the fact that the watermark is usually an additional noise signal present inside the host signal.

In the other hand, interference attacks are those which adds noise to the watermarked object. Examples are: lossy compression, remodulation, quantization, collusion, de noising, and averaging and noise storm.

6.2 Geometric Attacks

Geometric attacks manipulate the watermarked image in such a way that the detector cannot find the watermark content. Affine transforms such as rotation, translation and scaling are included in this type of attack. Line/column removal, cropping and Warping are also included in this family of attacks. One more example of geometric attack is the mosaic attack. In this mosaic attack, first the watermark image is divided into several parts and then rearranged by use of HTML code. Detector will fail to provide desired results in the Constructed watermark image. Local pixel jittering is an example of spatial domain geometric attack. Geometric attacks are specific to images and videos.

6.3 Cryptographic Attacks

Removal and geometric, do not break the security mechanism of the watermarking algorithm. But, cryptographic attacks crack the security of the watermarking algorithm. For example, finding the secrete watermarking key using exhaustive brute force method. One more example of cryptographic attack is the oracle attack [41]. In the oracle attack, the attacker creates a non-watermarked object when a public watermark detector device is available.

6.4 Protocol Attacks

These types of attacks target the loopholes in the watermarking concept. One example of such attack is the IBM attack [42]. The IBM attack is also known as the deadlock attack, fake-original attack or inversion attack. This attack inserted one or several additional watermarks such that it is ambiguous to detect which one is original watermark. In some attacks, a fake original object is created that gives the same results as original object through the detection process. These types of attacks are called as inversion attacks.

Hartung et al. [43] also classified watermarking attacks in the given classes:

6.5 Simple Attacks

Simple attacks change the contents of the host image without doing anything to watermark location. Examples are: Wavelet-based compression, noise addition, conversion to analog and cropping.

6.6 Disabling Attacks

It breaks the correlation between the watermark and the host image. This makes extraction impossible. Examples are: Insertion of pixels, geometric distortions, cropping and rotation.

6.7 Ambiguity Attacks

These types of attacks confuse the receptor by inserting a fake watermark. Fake watermark makes it impossible to discover which one was the original watermark in the host image.

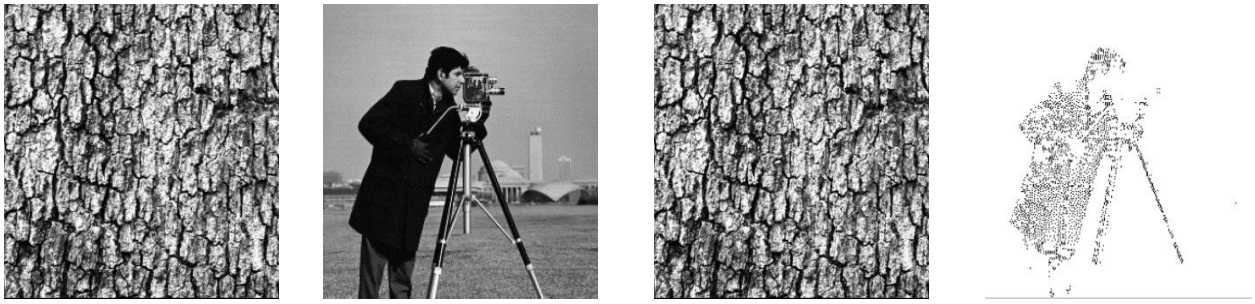
7. EXPERIMENTAL RESULTS

The experiments have been performed with the software MATLAB R2013a version. Experiments have been done with

a 512×512 "smooth", "texture", "edge" as the gray scale original host image, and a 256×256 grey-scale image as watermark image. In the experiment, the original images, watermark image, watermarked image and recovered watermark image quality show by figures. Figure 5 shows LSB watermarked result images. Figure 6 shows DCT watermarked result images. Figure 7 shows DWT watermarked result images. Figure 8 shows DWT-SVD watermarked result images. Figure 9 shows DCT-SVD watermarked result images. Table 1, 2 and 3 show parameter values of smooth image watermarking, texture image watermarking and edge image watermarking for different watermarking techniques respectively.

Original Image **Watermark Image** **Watermarked Image** **Recovered Image**

(a) LSB Watermarking Using Smooth Images



Original Image **Watermark Image** **Watermarked Image** **Recovered Image**

(b) LSB Watermarking Using Texture Images

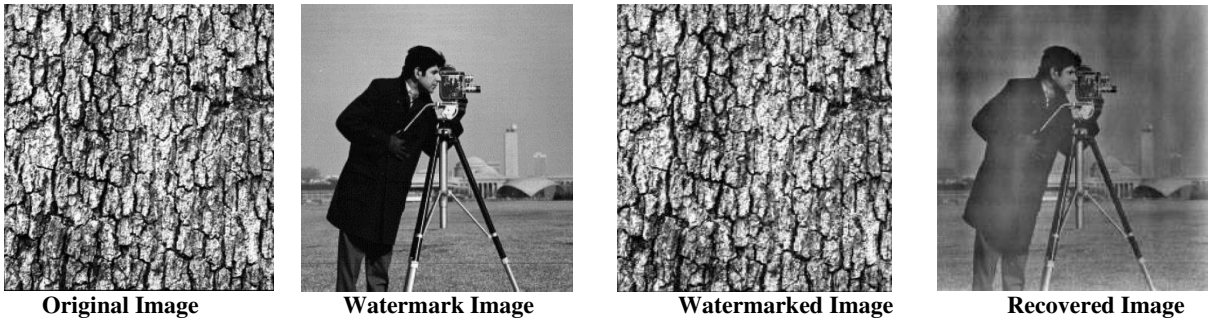
Original Image **Watermark Image** **Watermarked Image** **Recovered Image**

(c) LSB Watermarking Using Edged Images

Fig.5: LSB Watermarking Result Images

Original Image **Watermarked Image** **Recovered Image**

(a) DCT Watermarking Using Smooth Images



Original Image **Watermark Image** **Watermarked Image** **Recovered Image**

(b) DCT Watermarking Using Texture Images

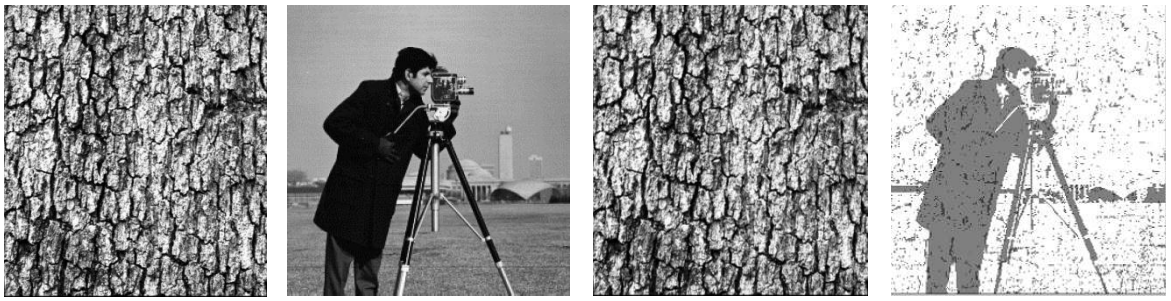
Original Image **Watermark Image** **Watermarked Image** **Recovered Image**

(c) DCT Watermarking Using Edges Images

Fig.6: DCT Watermarking Result Images

Original Image **Watermark Image** **Watermarked Image** **Recovered Image**

(a)DWT Watermarking Using Smooth Images



Original Image **Watermark Image** **Watermarked Image** **Recovered Image**

(b)DWT Watermarking Using Texture Images

Original Image **Watermark Image** **Watermarked Image** **Recovered Image**

(c)DWT Watermarking Using Edges Images

Fig.7: DWT Watermarking Result Images

Original Image Watermark Image Watermarked Image Recovered Image

(a) DWT-SVD Watermarking Using Smooth Images

Original Image Watermark Image Watermarked Image Recovered Image

(b) DWT-SVD Watermarking Using Texture Images

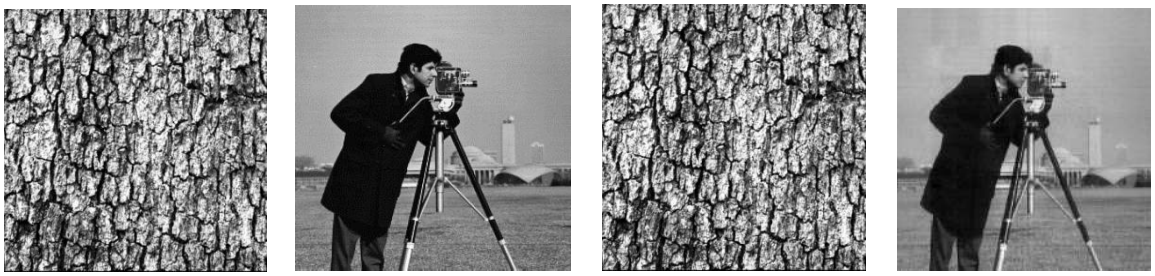
Original Image Watermark Image Watermarked Image Recovered Image

(c)DWT-SVD Watermarking Using Edges Images

Fig. 8: DWT-SVD Watermarking Result Images

Original Image Watermark Image Watermarked Image Recovered Image

(a) DCT-SVD Watermarking Using Smooth Images



Original Image Watermark Image Watermarked Image Recovered Image

(b) DCT-SVD Watermarking Using Texture Images

Original Image **Watermark Image** **Watermarked Image** **Recovered Image**

(c) DCT-SVD Watermarking Using Edges Images

Fig. 9: DCT-SVD Watermarking Result Images

Table 1. The parameter values of smooth image watermarking

Techniques	PSNR	MSE	SNR
LSB	61.9084	0.0419	54.3300
DCT	39.2481	7.7316	33.5916
DWT	46.1285	1.5857	40.4717
DWT-SVD	51.5199	0.4582	45.8631
DCT-SVD	45.5042	1.8309	39.8474

Table 2. The parameter values of texture image watermarking

Techniques	PSNR	MSE	SNR
LSB	51.1591	0.4979	46.4157
DCT	39.7547	6.8803	35.0113
DWT	46.5482	1.5273	41.5482
DWT-SVD	51.4562	0.4650	46.7127
DCT-SVD	45.6655	1.7641	40.9220

Table 3. The parameter values of edge image watermarking

Techniques	PSNR	MSE	SNR
LSB	51.1213	0.5023	48.3383
DCT	39.1998	7.8182	34.4167
DWT	46.5482	1.5273	41.5482
DWT-SVD	51.6070	0.4491	48.8239
DCT-SVD	45.2120	1.9583	42.4289

After applying the some different types of attacks in watermarked images the parameter values have changed. The tables show the change in parameters values. Attacks apply in different techniques, watermarked image and results is shown in tables. Table 4, 5, 6, 7 and 8 show LSB watermarking attacks results, DCT watermarking attacks results, DWT watermarking attacks results, DWT-SVD watermarking attacks results and DCT-SVD watermarking attacks results respectively.

Table 1. LSB watermarking attacks results

LSB Watermarking	MSE	PSNR	SNR
Watermarked Image	0.4994	51.1465	45.4897
JPEG Attack Image	5.7041e+03	10.5689	4.9122
PSNR Attack Image	6.3588e+03	10.0970	4.4403
NOISE Attack Image	9.3493e+03	8.4230	2.7662
CROP Attack Image	3.5300e+03	12.6531	6.9820
ROT Attack Image	1.0442e+04	7.9429	2.2656

Table 2. DCT watermarking attacks results

DCT watermarking	MSE	PSNR	SNR
Watermarked Image	7.7316	39.2481	33.5916
JPEG Attack Image	174.0594	25.7238	20.0670
PSNR Attack Image	5.0877	41.0656	35.4088
NOISE Attack Image	9.3433e+03	8.4258	2.7690
CROP Attack Image	3.5220e+03	12.6630	6.9919
ROT Attack Image	1.0442e+03	7.9450	2.2678

Table 3. DWT watermarking attacks results

DWT Watermarking	MSE	PSNR	SNR
Watermarked Image	1.5857	46.1285	40.4717
JPEG Attack Image	170.7504	25.8072	20.1504

PSNR Attack Image	1.5857	46.1285	40.4717
NOISE Attack Image	9.3571e+03	8.4194	2.7626
CROP Attack Image	3.5228e+03	12.6619	6.9909
ROT Attack Image	1.0436e+04	7.9454	2.2681

Table 7. DWT-SVD watermarking attacks results

DWT-SVD Watermarking	MSE	PSNR	SNR
Watermarked Image	0.4491	51.6070	48.8239
JPEG Attack Image	186.0601	25.4343	19.7775
PSNR Attack Image	169.4566	25.8402	20.1834
NOISE Attack Image	1.4896e+04	6.4002	0.7434
CROP Attack Image	9.9112e+03	8.1695	2.5128
ROT Attack Image	9.6225e+03	8.2979	2.6412

Table 8. DCT-SVD watermarking attacks results

DCT-SVD Watermarking	MSE	PSNR	SNR
Watermarked Image	1.8309	45.5042	39.8474
JPEG Attack Image	218.2684	24.7409	19.0841
PSNR Attack Image	201.5666	25.0866	19.4298
NOISE Attack Image	1.4897e+04	6.3997	0.7430
CROP Attack Image	1.0169e+04	8.0581	2.4013
ROT Attack Image	9.6714e+03	8.2759	2.6191

When apply attacks in watermarked images all the parameters value are decreases as compared to original watermarked image. So that attacks degrade the watermarked images and also affect recovered watermark.

8. CONCLUSION

Watermarking is process of embedding a watermark inside the data. In this paper, different watermarking algorithms which are based on spatial domain and frequency domain have been reviewed and compared with attacks to find out what effects after attacking watermarked images. This paper gives a view for the categories of attacks against the security of the digital watermarking schemes.This paper concludes that digital watermarking technique is very impressive and has its own beauty of research. It provides authentication of image and other digital data and gives protection against attacks.

In future, this work will be extended to improve the performance parameters value using robust watermark image.

9. REFERENCES

[1] Schyndel, R. G., Tirkel, A. and Osborne, C. F. "A Digital Watermark", in proceedings of IEEE International conference on Image Processing, ICIP-1994, pp. 86-90.

[2] Er-Hsien Fu, "Literature Survey on Digital Image Watermarking", EE381K-Multidimensional Signal Processing August 1998.

[3] Hartung F. and Kutter M., Katzenbeisser S. and Fabien A. P. Petitcolas, editors, "Information Hiding Techniques for Steganography and Digital watermarking" , Artech House, 2000 .

[4] Su G. M., "An Overview of Transparent and Robust Digital Image Watermarking", 2001.

[5] Seitz, J., "Digital Watermarking for Digital Media", Information Science Publishing, 2005.

[6] Liu, J. and Hi, X., "A review study on Digital Watermarking". In proceeding of International Conference on Information and Communication Technologies, 2005.

[7] Kougianos E., Mohanty, S. P. and Mahapatra R. N. "Hardware assisted watermarking for multimedia" Computers and Electrical Engineering Volume 35 Issue 2, 2009 339- 358.

[8] Rawat K. S. et. Al, "Digital watermarking scheme for authorization against copying or piracy of color image", Indian Journal of Computer Science and Engineering, Vol. 1 No. 4, pp. 295-300.

[9] Fridrich, J., "Image watermarking for tamper detection," in proceedings of IEEE Int. Conf. Image Processing, Chicago, IL, Oct. 1998, pp. 404-408

[10] Coatrieux, G., Lecornu, L., Roux, C., Sankur, B. "A Review of Digital Image Watermarking in Health Care".

[11] Muharemagic E. and Furht B. "A Survey of Watermarking Techniques and Applications" 2001.

[12] Katzenbeisser S. and Petitcolas F.A.P., "Information Hiding Technique for Steganography and Digital Watermarking", Aetech House, UK 2000.

[13] Megalingam, R. K., Nair, M. M., Srikumar, R. Balasubramanian, V. K., Sarmaand, V. and Sarma V. "Performance Comparison of Novel, Robust Spatial Domain Digital Image Watermarking with the Conventional Frequency Domain Watermarking Techniques", in proceeding of IEEE International Conference on Signal Acquisition and Processing 2010, pp. 349- 353

[14] Singh, P., and Chadha, R. S., "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT), Vol. 2, No. 9, March 2013, pp. 165-175.

[15] Wu, C.H. and Cathey, R., "Digital Watermarking: A Comparative Overview of Several Digital Watermarking Schemes" 2002.

[16] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science, Vol. 3, No. 9, 2007, pp. 740-746.

[17] Lang, J., Sun, J. Y., and Yang, W. Y., "A Digital Watermarking Algorithm Based on Discrete Fractional Fourier Transformation" in proceeding of International Conference on Computer Science and Service System August 2012, pp. 691 – 694.

[18] Wu, C. and Hsieh, W., "Digital watermarking using zero tree of DCT", IEEE Trans. Consumer Electronics, vol. 46, No. 1, 2000, pp. 87-94.

[19] Yang, Y., Sun, X., Yang, H., and Li, C. T. "A Removable Visible Image Watermarking Algorithm in DCT Domain," Journal of Electronic Imaging, Vol. 17, No. 3, July-September 2008, pp. 033008-1 ~ 033008-11.

[20] Huang, F., and Guan, Z. H. "A Hybrid SVD-DCT Watermarking Method Based on LPSNR", Pattern Recognition Letters, Vol. 25, No. 15, November 2004, pp. 1769-1775.

[21] Cox, I. J., Kilian, J., Leighton, F. T. and Shamoon, T., "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, Vol. 6, January 1997, pp. 1673–1687.

[22] Zhu, W., Xiong, Z. and Zhang, Y.Q., "Multi Resolution Watermarking for Images and Video", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 9, June 1999, pp.545–550.

[23] Langelaar, G.C. and Langendijk, R.L., "Optional Differential Energy Watermarking of DCT Encoded Images and Video", IEEE Transactions on Image Processing, vol. 10, January 2001, pp. 148-158.

[24] Shaikh, M. S. and Dote, Y. "A Watermarking Scheme For Digital Images Using Multilevel Wavelet Decomposition", Malaysian Journal of Computer Science, Vol. 16 No. 1, June 2003, pp. 24-36.

[25] Liu, J. C. Lin, C. H., Kuo L. C. and Chang, J. C. "Robust Multi-scale Full-Band Image Watermarking for Copyright Protection", Lecture Notes in Computer Science, Springer Berlin, Heidelberg, Vol. 4570, 2007, pp. 176-184.

[26] Hassanien, A. E., "A Copyright Protection using Watermarking Algorithm", ACM Journal Informatica, Vol. 17, No. 2, April 2006, pp. 187-198.

[27] Chiu Y. C. and Tsai, W. H. "Copyright Protection against Print-and-Scan Operations by Watermarking for Color Images Using Coding and Synchronization of Peak Locations in Frequency Domain", Journal of Information Science And Engineering, Vol. 22, 2006, pp. 483-496.

[28] Singh, Y. S., Devi, B. P. and Singh K. M., "A Review of Different Techniques on Digital Image Watermarking Scheme" International Journal of Engineering Research, Vol.2, No.3, July 2013, pp.193-199.

[29] Liu, R. and Tan, T. "An SVD-based Watermarking Scheme for Protecting Rightful Ownership", IEEE Trans. Multimedia, Vol. 4, No. 1, 2002, pp. 121-128, 2002.

[30] Chang, C. C., Tsai, P., and Lin, C. C. "SVD based Digital Image Watermarking Scheme", Pattern Recognition Letters 26, 2005, pp. 1577-1586.

[31] Ghazy, R.A., El-fishawy, N.A., Hadhoud, M.M., Dessouky, M.I., El-Samie, F.E.A., "An Efficient Block-by-Block SVD-based Image Watermarking Scheme", National Radio Science Conference, 2007, pp. 1-9.

[32] Shieh, J. M., Lou D. C. and Chang, M. C., "A Semi-blind Digital Watermarking Scheme Based on Singular Value Decomposition", Computer Standards and Interfaces Vol. 28 No. 4, 2006, pp. 428-440.

[33] Hsieh, C. and Tsou, P. "Blind Cepstrum Domain Audio Watermarking Based on Time Energy Features", in proceeding of 4th International Conference on Digital Signal Processing, 2004, pp. 705-708.

[34] Vladimir, B., and Rao, K. E. "An Efficient Implementation of the Forward and Inverse MDCT in MPEG Audio Coding", IEEE Signal Processing Letters, Vol. 8, No. 2, 2005, pp. 48-51.

[35] Chandra, D.V.S., "Digital Image Watermarking Using Singular Value Decomposition", in proceedings of 45th IEEE Midwest Symposium on Circuits and Systems, Tulsa, UK, August 2002, pp. 264-267.

[36] Cox I. J., Miller, M. L. and Bloom J. A., "Digital Watermarking", Morgan Kaufmann Publishers, USA, 2002.

[37] Katzenbeisser S. and Petitcolas F.A.P., "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, UK, 2000.

[38] Pan, J. S., Huang, H. C., Jain L. C., and Fang, W. C. "Intelligent Multimedia Data Hiding", in Springer, 2004

[39] Liu J. and He, X. "A Review Study on Digital Watermarking", in proceeding of 1st International Conference on Information and Communication Technologies, 2005, pp. 337-341.

[40] Friedman, G.L., "The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image", in proceeding of IEEE Transaction on Consumer Electronics, Vol. 39, No. 4, November 1993, pp. 905-910.

[41] Coatrieux, G., Lecornu, L., Roux, C., Sankur, B., "A Review of Digital Image Watermarking Health Care".

[42] Hartung, F., Su., J. K. and Girod, B. "Spread Spectrum Watermarking: Malicious attacks and counterattacks", 1999, pp. 147-158.

[43] Katzenbeisser S. and Petitcolas F.A.P., "Information Hiding Techniques for Steganography and Digital Watermarking", Aetech House, UK, 2000.