A Review on Digital Image Watermarking Techniques

Article *in* International Journal of Image, Graphics and Signal Processing · April 2017

DOI: 10.5815/ijigsp.2017.04.07

CITATIONS
10

READS
1,186

2 authors:

Anuja Dixit
Indian Institute of Technology (ISM) Dhanbad
9 PUBLICATIONS **26** CITATIONS
SEE PROFILE

Rahul Dixit
Indian Institute of Information Technology Pune
26 PUBLICATIONS **94** CITATIONS
SEE PROFILE

I.J. Image, Graphics and Signal Processing, **2017, 4, 56-66**
Published Online April 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2017.04.07

A Review on Digital Image Watermarking Techniques

Anuja Dixit
Madhav Institute of Technology & Science, Gwalior, 474005, India
Email: anu2010cse1@gmail.com

Rahul Dixit
National Institute of Technology, Rourkela, 769001, India
Email: rahul2012ism@gmail.com

Abstract—Nowadays, Multimedia security [1] is a major issue. Images, video, audio, text files are losing their credibility day by day as they can be distorted or manipulated by using several tools. Ensuring the authenticity [2] and integrity of digital media is a major issue. The manipulation made by forgery tools are so smoothly done that we don't even suspect that forgery may be involved in digital content. Multimedia data is facing several issues related to illegal distribution, duplication and manipulation of information conveyed by them. The digital watermarking [3] technique plays an important role in protecting digital content. In this paper, On the basis of their operating principles different watermarking techniques are categorized [4]. Attacks, applications and requirements [5] related to watermarking techniques are also discussed. Different watermarking techniques proposed by researchers for protecting copyrights of digital media are presented which are based on spatial and frequency domain. Frequency domain are getting much more attention due to use of wavelets which have high degree of resemblance to human visual system. In digital watermarking, secret information is embedded with original data for maintaining ownership rights of the digital content. Spatial domain watermarking techniques work over pixel characteristics and frequency domain watermarks concerned about different transformations that can be used with digital content. Imperceptibility, robustness, security, complexity and capacity are some requirements of the digital watermarking which completely depends on the algorithm used for watermarking.

Index Terms—Copyright protection, Cryptography, Digital image watermarking, Discrete Cosine Transform, Discrete Fourier Transform, Discrete Wavelet Transform, Fragile, Frequency domain, Image processing, Ownership, Robust, Security, Singular Value Decomposition, Spatial domain.

I. INTRODUCTION

Digital images are used for various purposes. Nowadays, we cannot think about the world without images. We go through several images in a day which are available at various places like TV, magazines, websites, newspaper, books etc. Digital image processing [6] has its several applications over analogue image processing. Several operations [7] such as enhancing quality of image, filtering noise, segmentation, restoration can be performed over digital images. A digital image can be defined as two dimensional image having finite number of digital values also known as picture elements or pixels.

Digital data is facing several issues related to privacy and security [8] of data. Efficient security techniques are needed to prevent illegal use of data permission. Due to speedy development of technology versatile software are available which can perform changes in digital media efficiently. These changes are not noticeable. Due to such situations multimedia data is no longer believable. It is highly recommended to secure multimedia data present over internet. To deliver security to digital data several techniques are used such as cryptography [9], encryption, decryption, steganography and digital watermarking. In this paper digital watermarking techniques are discussed.

Digital watermarking is an integral part of digital image processing. Digital watermarking is one of the most effective technique for hiding information. Several watermarking techniques are offered to conceal the secret information in form of digital data such as text, audio and video. Digital watermarking is provides facility to attach secret data in cover image which could be afterward used for extraction or detection for several uses like identification of owner [10], copyright protection, authentication and content protection etc. Requirements which should be fulfilled by watermarking techniques are discussed in section 2. Applications of watermarking are depicted in section 3. General watermarking techniques are keyed out in section 4. Related work in field of Digital watermarking techniques is elaborated in section 5. Categories of watermarking techniques are discoursed in section 6. Several attacks on watermarking techniques are keyed out in section 7. Section 8, depicts performance analysis metrics. Finally, this paper is concluded in section 9.

II. Prerequisites of Watermarking

Watermark should satisfy several requirements [11] as shown in figure (1). Watermark should be capable of resisting malicious attacks, to prevail common distortions and not to be easily empathized. Watermark should be able to adjust with other coexisting watermarks and should not be too much complex for insertion or deletion. An image watermark should satisfy following properties.

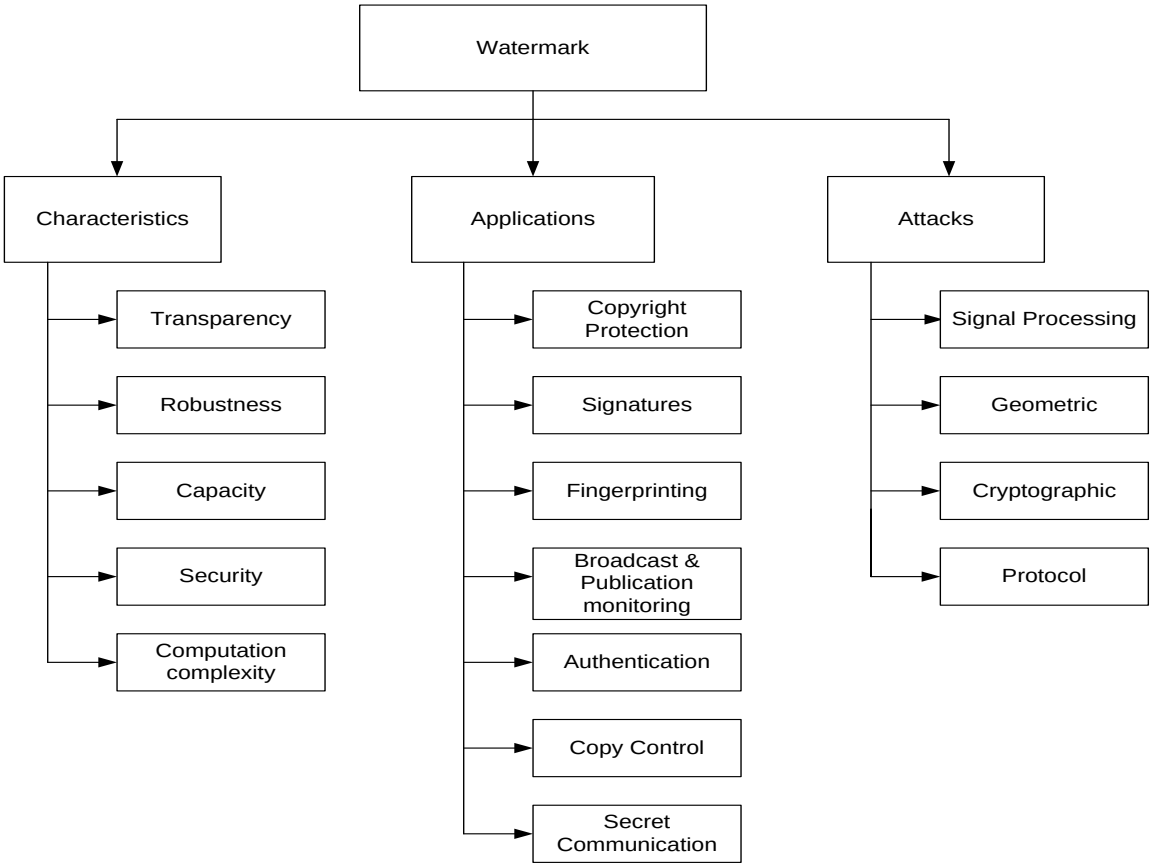

Fig.1. Characteristics, applications and attacks related to watermarking.

- *Transparency:* When watermark is embedded in image it should not distort the quality of the image or the message conveyed in image. Embedded watermarks should be perceptually invisible. Cover work of watermark versions and original image should be perceptually similar. End user should not be able to observe any visual discrepancy. In some cases it is observed that imperceptibility is compromised to obtain high degree of robustness and to reduce expenditure.
- *Robustness:* Watermarks should be able to resist against various attacks. These attacks could be geometrical or non-geometrical [12]. Elimination or manipulation of watermarks should be impossible if they are tampered without sufficient knowledge of embedding process related to specific fields.
- *Capacity:* A suitable amount of information has to be attached to images. This embedded information in watermarked image is known as data payload. Bits encoded in watermark for a unit of time or work is characterized as data payload. The number of bits encoded [13] in watermarking and image information should make an adequate amount of combination for figured application.
- *Security:* Watermarks should be secured using secret keys so that they cannot be altered without specific knowledge of the secret key. Watermarks should be highly secured to protest all attempts of addition, deletion and updation used by unauthorized persons.
- *Computational complexity:* Time taken by watermarking algorithms in encoding and decoding is referred to as computational complexity. To establish the security arrangements and watermark validity high computational complexity is required. For real-time applications efficiency and speed are of great importance.

III. Applications of Watermarking

Digital watermarking has several applications [14]. Applications are classified in following categories using general consent on digital watermarking techniques.

- *Copyright protection*: It is one of the most important application of watermarking techniques. The sole purpose of this application is to detect the original owner of the digital media so that other parties can be restricted to make alterations in the original content without permissions. This application should make sure that no other information can be attached or altered without resulting in significant change in digital media.
- *Signatures:* The owner of the content is recognized through watermarks. This application may be exploited by potential user to take control from authentic owner of legal rights for copying or publishing the data.

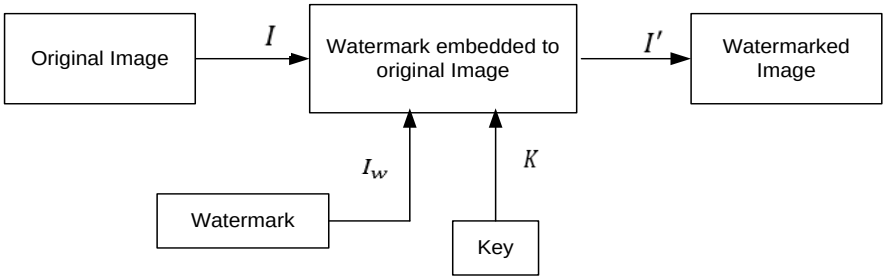

Fig.2. Process of watermark embedding.

- *Fingerprinting*: Watermarks can be used to identify the buyers of content. This application is highly useful in finding the origin of illegal copies [15] of digital media.
- *Broadcast and publication monitoring*: Using signature technique the owner of the content is detected but in broadcast and publication monitoring technique possible computer networks, television and radio broadcast, and other distribution channels are monitored using automated systems. Using this application content is monitored when and where it appears.
- *Authentication:* Watermark is used for encoding the information to conclude that the content is original.
- *Copy control:* Watermark consists information related to rules and regulations of usage and copying which are enforced by content owner. Most of the times, these rules are undemanding rules such as "this content cannot be replicated" or "this content can be copied, but no consequent replica can be made of that copy".
- *Secret communication:* Watermarks can also be used for secret communication [16]. The signals are embedded in transmission of secret information from one place to another.

IV. General Watermarking Stages

Watermark embedding can be represented using (1). If 'I' is an original image and watermark 'I_w' is provided then watermarked image can be shown using following equation.

$$I^{'} = I + \gamma . I_w \tag{1}$$

The operational flowchart of watermark embedding process is shown in figure (2). Original image 'I' and watermark 'I_w' enter into a system, γ is a scaling factor. An optional secret key or public key can be applied to guide the operation. The output of this complete process is a watermarked image I'. Embedded watermarks can be extracted using different ways. Original image can be used to compare and detecting the watermark known as non-blind watermark [17]. Correlation measure are also used to find the watermark known as blind watermarking. In non-blind watermarking, embedded watermark can be extracted using (2).

$$I_w = (I^{'} - I) / \gamma \tag{2}$$

In second method of watermarking extraction (known as blind watermarking) similarity measures are used as shown in figure (3).

Similarity between original and extracted watermarks can be calculated using correlation-based method. Equation (3) can be used for calculating watermark similarity measure. Generally, the extracted watermark I_w' is not identical to the original watermark I_w. Equation (3) calculates the similarity between I_w and I_w' as shown following.

$$sum(I_w, I_w^{'}) = \frac{I_w^{'}.I_w}{\sqrt{I_w^{'}.I_w}} \tag{3}$$

For declaring whether I_w and I_w' match, sim (I_w, I_w') should be greater than predefined threshold $'T'$.

V. Digital Image Watermarking Techniques

Digital watermarking comprises various techniques to protect the digital content from unauthorized access and modifications performed over them. Watermarking techniques can be divided in two main categories spatial and transform domain. In spatial domain directly functions are performed over pixels. Watermarks are embedded in spatial domain [18] by altering pixel values.

In spatial domain LSB technique is mainly used for modification. Transform domain techniques used for watermarking mainly focus over alteration of transform domain coefficient. In case of transform domain DCT, DWT, DFT are the most widely used techniques for watermarking. To obtain robustness and security transform domain techniques are much more effectual than spatial domain watermarking techniques.

A. Spatial Domain Watermarking

Spatial domain shows image as combination of pixels. Pixels intensity and color value of some specific pixels are modified to attach watermark. The spatial domain techniques are less time consuming. These techniques possess less complexity. Each operation performed in spatial domain technique is very simple. Computational speed is high in these techniques but these are less robust to attacks. In LSB technique [19], watermarks are embedded in least significant bits of arbitrarily selected pixels of cover image. The prime advantage of this technique is that it can easily be performed over images. When using LSB technique, watermarks are embedded quality of image does not get affected. The main limitation of LSB method is that it is not robust to common signal processing operations hence watermarks can be easily depleted due to signal processing attacks. Spatial domain watermarking techniques can withstand against simple attacks like cropping and addition of noise.

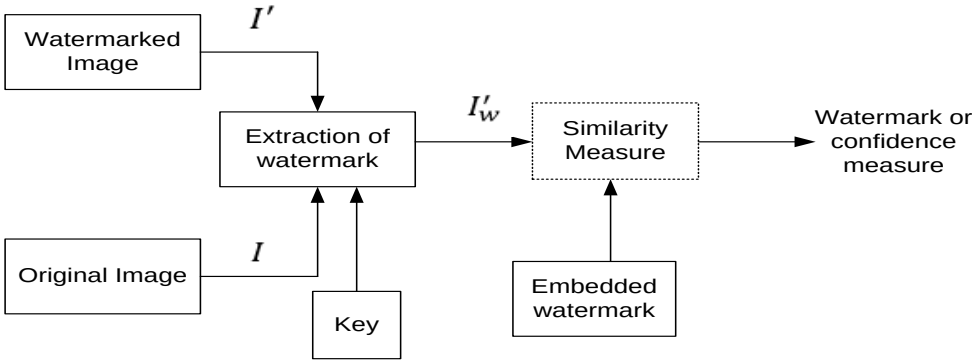

Fig.3. Extraction and detection of watermark.

B. Transform Domain Watermarking

In such techniques, watermarks are not directly embedded to the cover image. At first, cover image is transformed and then watermarks are embedded to coefficient of transformed image. To extract original signal, inverse transform is computed for manipulated coefficients. In case of transform domain [20], where embedding of watermark is performed in transformed coefficients are robust against attacks such as JPEG compression. Transform domain algorithms are useful in robust watermarking to assure the flexibility of watermark to popular signal processing attacks. There are various transform domain watermarking techniques like Discrete wavelet Transform (DWT), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Singular Value Decomposition (SVD). These methods render higher imperceptibility, effective robustness to image alterations and signal processing attacks. The cost of computation for transform based watermarking methods is more than spatial domain based methods.

- *Discrete Cosine Transform Based Watermarking Technique*

DCT is used for obtaining frequency domain signal from time domain signal. When DCT [21] is applied over an image, a two-dimensional matrix of coefficients is achieved. DCT is used in several disciplines such as data compression, pattern recognition and various areas of image processing. In DCT based approach, image is divided in non-overlapping blocks of specific fixed dimension. DCT is applied over each of the block of the image. Block selection criteria is applied to extract blocks of higher importance such as HVS. Coefficients are selected corresponding to chosen blocks. Low frequency components which are highly important, situated at left most corner of the coefficient matrix. High frequency components are present at right most corner of the matrix. DCT is used for fractioning image into pseudo frequency bands. Most often, watermarks are embedded in middle frequency subbands. If watermarks are embedded between high frequency components then such approach is less effective against attacks but it can efficaciously hide the watermarks. Watermarks are inserted into coefficients of image by modifying them smoothly. After above steps, Inverse DCT is applied over blocks of image.

The DCT for one dimensional succession of length N can be computed using (4)

$$c(u) = \alpha(u)\sum_{x=0}^{N-1} f(x)\cos\left[\frac{(2x+1)u\pi}{2N}\right] \quad (4)$$

Where u = 0, 1, 2, 3,……., N-1. Inverse DCT transformation for one dimensional sequence can be calculated using (5)

$$f(x)=\sum_{u=0}^{N-1}\alpha(u)c(u)\cos\left[\frac{(2x+1)u\pi}{2N}\right] \quad (5)$$

For above equations $\alpha(u)$ can be defined as shown in (6)

$$\alpha(u)=\begin{Bmatrix}\sqrt{\frac{1}{N}}, u=0\\ \sqrt{\frac{2}{N}}, u\neq 0\end{Bmatrix} \quad (6)$$

When DCT is applied over block of image, two kind of coefficients (AC and DC) [22] are achieved. Only one DC coefficient is present in coefficient matrix and others are AC coefficients. DCT can be defined for two-dimensional transformation as shown in (7)

$$c(u,v)=\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (7)$$

Where u, v= 0,1,2,3……., N-1. $\propto(u)$ and $\alpha(v)$ can be defined as shown in (6). Inverse transformation corresponding to two dimensional DCT can be computed using (8).

$$f(x,y)=\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(v)\alpha(u)c(u,v)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (8)$$

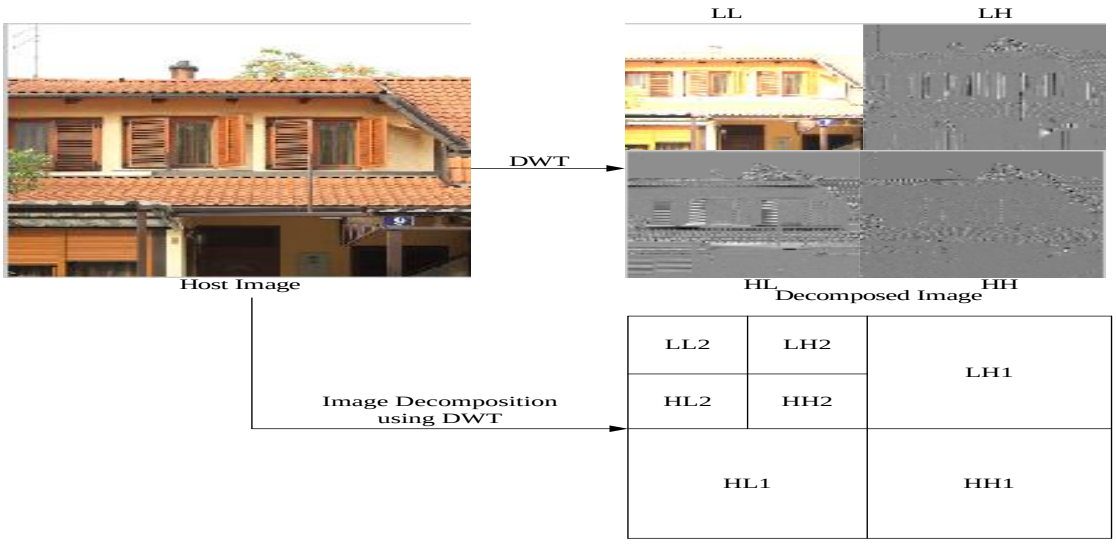

Fig.4. Decomposition of image using DWT.

DCT technique is strong enough to withstand against various kinds of attacks like filtering, cropping, sharpening and noising. DCT has excellent computational efficiency. For bit rate reduction, DCT provides improved performance.

- *Discrete Wavelet Transform Based Watermarking Technique*

DWT is helpful in producing multiresolution view of an image. The multiresolution representation renders a framework to understand image information. DWT [23] provides an efficient way to observe signals at multiple resolution. DWT decomposes image in high frequency and low frequency components. Further, low frequency components are decomposed recursively until desired result is obtained. When DWT is applied over image, image decomposed in four subbands as shown in figure (4). Four subbands LL, LH, HL and HH contains approximation, vertical data, horizontal data and diagonal details present in the image respectively. Low frequency components of the image that are mainly present in approximation subband which is suitable for embedding watermark because approximation subband contain maximum information related to original image. The original image is obtained back by using Inverse Discrete Wavelet Transform (IDWT). DWT provides scaling facility. DWT is one of the most used technique in watermarking because of its outstanding spatial localization and multiresolution feature. The spatial localization property can be utilized for identifying section in the cover image at which watermark is effectively embedded.

When DWT is applied over image it gets decomposed in four non-overlapping multiresolution coefficient sets. The coefficients can be shown using following equations.

$$Z_{LL}^{K}=\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}m(x)m(y)z_{LL}^{K-1}(2u-x)(2v-y) \quad (9)$$

$$Z_{LH}^{K}=\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}m(x)n(y)Z_{LL}^{K-1}(2u-x)(2v-y) \quad (10)$$

$$Z_{HL}^{K} = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} n(x)m(y)Z_{LL}^{K-1}(2u-x)(2v-y) \quad (11)$$

$$Z_{HH}^{K} = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} n(x)n(y)Z_{LL}^{K-1}(2u-x)(2v-y) \quad (12)$$

Where K is the level of the decomposition. m(x) and n(y) are the impulsive response. DWT provides improved visual image quality than DCT. DWT provides much better localization as compared to DCT. DWT realizes functioning of HVS more accurately as compared to DCT. DWT is able to support multi resolution description of host image. Image can be shown at different level of resolution varying from low resolution to high resolution. The disadvantage of DWT is that computational cost is high also time involved in computation is also high.

- *Discrete Fourier Transform Based Watermarking Technique*

DFT is one of the most commonly used techniques in image processing. It offers pure frequency domain analysis. DFT [24] can withstand against several kind of attacks like cropping, rotation, translation, scaling etc. When DFT is applied over an image, it get decomposed in sine and cosine forms. Watermark embedding techniques based on DFT are divided in two categories: Direct embedding and Template based embedding. In case of direct embedding techniques, DFT magnitude and phase coefficients are modified to embed watermark. Concept of templates is used in template based techniques. Transformation factor is estimated using DFT domain which consists template structure. To synchronize the image, template is searched during image transformation. Detector is used for extracting embedded spread spectrum watermark. DFT can be used for periodic as well as digital signals or discrete-time function. DFT can be calculated using (13) where period is M:

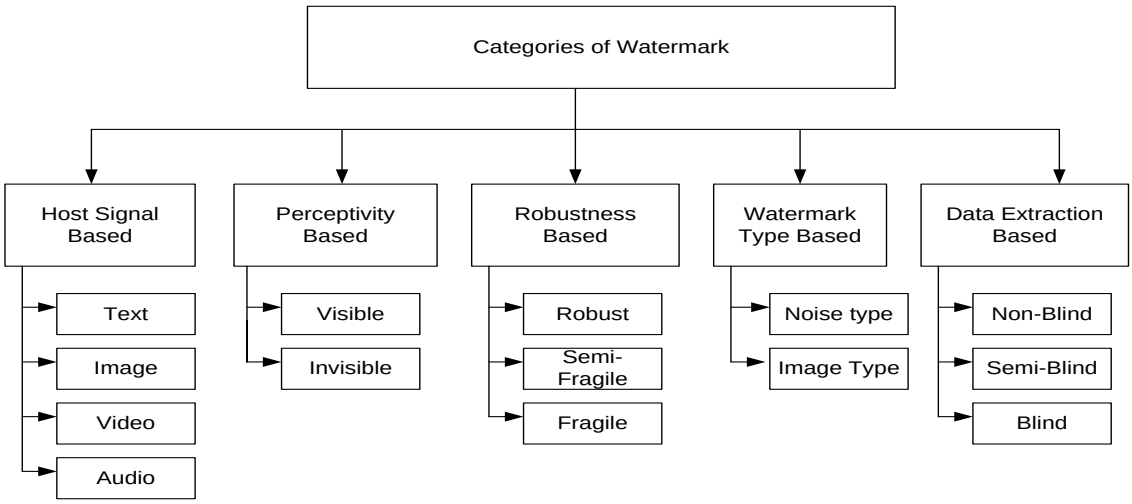

Fig.5. Categories of watermarks.

$$F(u) = \sum_{x=0}^{M-1} f(x)e^{\frac{-j2\pi ux}{M}} \quad (13)$$

Inverse Discrete Fourier Transform (IDFT) can be calculated using (14)

$$f(x) = \frac{1}{M}\sum_{u=0}^{M-1} F(u)e\frac{-j2\pi ux}{M} \quad (14)$$

Where *u, x = 0, 1, 2,....., M-1.* Equations (15) and (16) shows computational formula for one dimensional DFT. Forward and inverse discrete transform with period M are infinitely periodic.

$$F(u) = F(U + kM) \quad (15)$$

$$f(x) = f(x + kM) \quad (16)$$

In case of DFT, image is considered as complex valued. DFT represents image in form of phase and magnitude. One of the most important component of DFT is low frequency component often known as central component. DFT can be helpful in dealing with cropping attacks which leads to blurring of spectrum. If the watermarks are embedded in magnitude part, no synchronization is required. If scaling is performed over image, extracted signals are amplified. These signals can be discovered using correlation coefficient. DFT is invariant to rotation, scaling and translation hence, DFT can recuperate from geometric attacks. It is difficult to recover geometric distortions in case of DWT and DFT. Drawback of using DFT approach for watermarking is that the output produced from DFT is complex valued. In case of complex value, computation is complicated and requires high frequency rate. This technique is unable to produce positioning information in the space-time domain. Fourier transform is not able to render frequency information in

case of partial time quantum. To overtake such kind of inadequacies, fourier transform is substituted with DCT and DWT. These techniques consists higher characteristics of fourier transform and also overcome some of its limitations.

- *Singular value Decomposition Based Watermarking Technique*

Singular value decomposition is used for dimensionality reduction. It is originated from linear algebra. When SVD [25] is applied over a matrix '*A*' it get decomposed in three matrices. '*A*' produces '*U*' which is orthogonal matrix, Transpose of another matrix '*V*' and '*S*' which shows a diagonal matrix with singular values as diagonal elements. SVD is able to transform correlated variables into set of uncorrelated variables so that the various relationships among original data can be exposed clearly. A digital image can be defined as a matrix with nonnegative scalar entries. Let '*A*' is an image with size $m \times n$. Using SVD image can be shown in decomposed form as shown in (17)

$$A = USV^T \tag{17}$$

Where, orthonormal eigenvectors of AA^T are the columns of matrix '*U*'. Orthonormal vectors of A^TA used as the columns for '*V*'. *S* shows a diagonal matrix. *S* includes the square roots of eigen values from either '*U*' or '*V*' in descending order. If it is considered that matrix '*A*' has rank '*r*' ($r \leq \min(m,n)$) then a relation can be established between the elements of diagonal matrix *'S'* as shown in (18)

$$\sigma_1 \geq \sigma_2 \geq \sigma_3 ....., \sigma_r \geq \sigma_{r+1} \geq \sigma_{r+2} ..... \geq \sigma_n \geq 0 \tag{18}$$

$$A = \sum_{k=1}^{r} \sigma_k u_k v_k^T \tag{19}$$

Where, σ_k shows k^{th} singular value. u_k and v_k represents the k^{th} eigen vector of matrices '*U*' and '*V*' respectively. SVD scheme is highly robust. The singular values produced using SVD are practicable for conservation of substantial amount of watermark which is supplied by the owner and it cannot be excerpted from the protected image. SVD plays significant role in increasing accuracy and to decrease memory constraint to reward digital image watermarking techniques. The greater singular values contain significant information related to image and they are also resistant to attacks. If watermarks are embedded using SVD then singular values don't get much affected which stabilize the robustness of infixed watermarks. As algebraic properties are used in singular value decomposition so when watermarks are embedded in image by slightly modifying singular values, it doesn't influence the image so perceptivity remain intact. Every singular value obtained using SVD is a representation of luminance of an image layer. Singular vectors illustrates the geometry of image layer.

VI. Categories of Watermarking

On the basis of operational principles watermarks can be broadly categorized in six categories: Host signal based, Perceptivity based, Robustness based, Watermark type based and Data extraction based [26] as shown in figure (5).

A. Host signal based watermarking techniques

Host or cover signal based watermark could be classified in following categories:

- *Text watermarking:* In this technique, watermarks are embedded in font shape and also in space between characters and lines.
- *Image watermarking:* In this watermarking technique, payloads are embedded to image. Information attached to image is detected or extracted to check for ownership.
- *Video watermarking:* This technique is an extension to image watermarking scheme. In this classification real time extraction methods and robustness is involved to perform compression.
- *Audio watermarking:* This watermarking technique is a hot research issue due to large availability of MP3 files in various fields.

B. Perceptivity based watermarking techniques

According to perceptivity watermarking techniques are divided in visible and invisible categories.

- *Visible Watermark:* It is same as embossing a watermark on any official document or notice paper. In most of the channels on TV, logo is attached at corner of the picture these are the example of visible watermark.
- *Invisible Watermark*: These watermarks are not visible and very complex. They are generally used for identifying copyright data like name of author, license etc.

C. Robustness based watermarking techniques

Watermarks requires robustness to defend the ownership from several kind of malicious attacks. Watermarks are classified into following categories based on the robustness.

- *Robust:* In these kind of watermarking techniques, embedded watermarks remain unaffected from geometrical and non-geometrical attacks.
- *Semi-fragile*: In these techniques, watermarks can tolerate manipulations up to some level, such as in case of addition of quantized noise to watermarked image.
- *Fragile:* In these techniques, small tempering to watermarked images could result in complete distortion of watermark. These kind of watermark techniques are highly useful for protecting and verifying the authentic content.

D. Watermark type based watermarking techniques

Watermarking techniques can be classified in following two categories.

- *Noise type:* Noise type watermark category consists of chaotic sequences, Gaussian and pseudo noises.
- *Image type:* In this kind of watermarking technique binary images, stamps, label and logo are used.

E. Data Extraction based watermarking techniques:

To identify embedded watermark information, following types of techniques are used.

- *Non-blind:* This kind of technique needs an original media. This method can extract information using possible distorted image and the original media.
- *Semi-blind:* In this technique original media is not required for extraction of data for watermark detection.
- *Blind:* In this category neither original media nor embedded watermarks are required for data extraction. This kind of techniques are also referred as public watermarking techniques.

VII. Watermarking Attacks

These attacks are performed over watermarked digital media which creates distortions in content. Watermarking attacks [27] are broadly classified in four categories: signal processing attacks, geometric attacks, cryptographic attacks and protocol attacks. Combination of above attacks can also be used by attacker.

- *Signal Processing Attacks:* These attacks are also known as non-geometrical attacks. These attacks include addition of Gaussian, salt or pepper noise, histogram equalization, collusion, gamma correction etc.
- *Geometric Attacks:* These attack does not remove any information from watermark but they try to distort digital media content. Geometric attacks involve several operations such as scaling, cropping, translation, rotation, shearing, random bending, shifting, stretching etc. To deal with such kind of attacks feature based, template based or invariant domain based schemes are used. Mosaic attack is also one of the most common form of geometric attack. In mosaic attack image is depleted into pieces. Template removal attacks are used to remove the synchronized template.

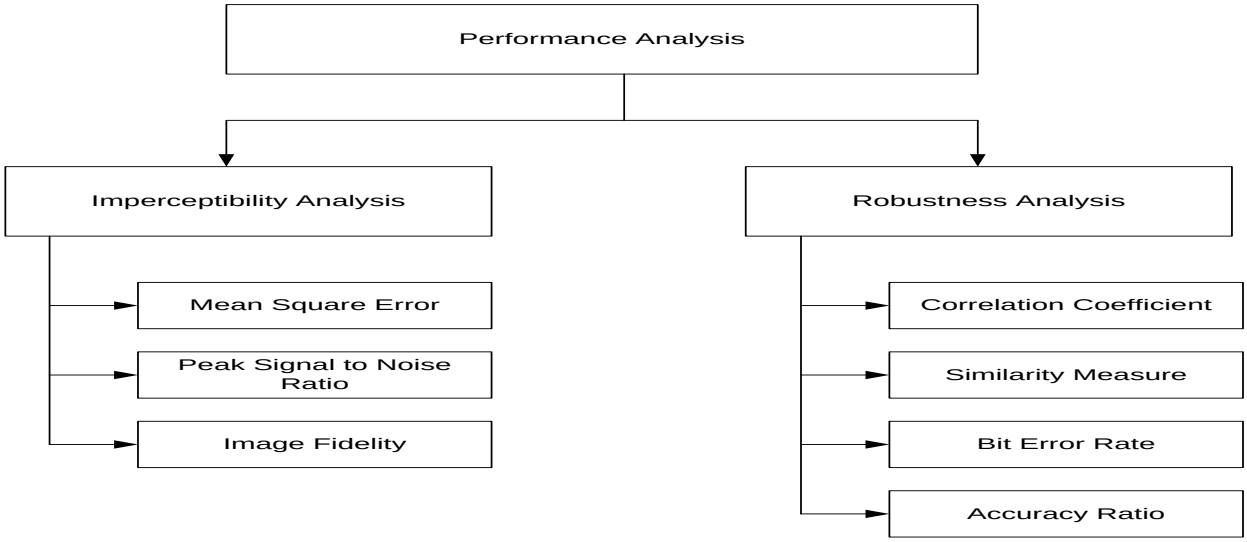

Fig.6. Performance analysis metrics for watermarking techniques.

- *Cryptographic Attacks:* These attacks focus on cracking the security codes and methods involved in watermarking techniques. Brute force search is an example of cryptographic [28] category of attack in which embedded secret information is detected using exhaustive search. In oracle attack, using watermarked image a non-watermark image is achieved with the help of watermark detector devices. These attacks possess high computational cost so they are used less frequently. Other attacks like statistical averaging and collusion are used for fetching crucial information. In this instances of different data set is provided, every time a different key or watermark is signed and averaged to calculate the malicious attacked data. In collusion technique small segment of each data set is taken to figure out a novel attacked data set using segments of differing datasets.
- *Protocol attacks:* This type of attacks include invertible and copy attacks. The main principle of invertible attacks [29] is that no watermark should be extracted from a non-watermarked image. In

this attack, an attacker can extract his own watermark from digital media and claim himself as owner of the original digital media. Other type of protocol attack is copy attack. The purpose behind such attacks is not to alter or delete watermarks but to judge watermark from watermarked digital media. These watermarks are copied to some other target data. Using this attack, attacker can claim that he has both original and watermarked image.

VIII. Performance Analysis

Performance analysis [30] plays crucial role in analyzing watermarked image and extracted watermark. Different statistical measures are used to analyze performance as shown in figure (6). The watermark robustness solely depends on the watermark embedding strength, which results in image visual degradation. These visual degradation are helpful in performance evaluation.

A. Imperceptibility Analysis

Imperceptibility [31] of watermarked image is qualitatively observed by analyzing visual artifacts. Various literatures has suggested many metrics. Following metrics are used for quantitative measure. Notation used are enlisted below:

$\mathrm{Im}(i, j)$: Original Image

$\mathrm{Im}'(i, j)$: Watermarked Image

S : Size of image

- *Mean Square Error (MSE):* Original image and watermarked image metrics can be used for computing Mean Square Error [32] as shown in (20)

$$MSE = \frac{1}{S}\sum_{i,j}(\mathrm{Im}(i, j) - \mathrm{Im}'(i, j))^2 \qquad (20)$$

- *Peak Signal to Noise Ratio (PSNR):* PSNR value is calculated between original image and watermarked image as shown in (21)

$$PSNR = 10\log_{10}\frac{(255\times 255)}{MSE} \qquad (21)$$

Perceptual quality is satisfactory if value of PSNR is more than 30dB.

- *Image Fidelity (IF):* Image Fidelity [32] is measurement of transparency or imperceptibility of watermarked image. IF can be computed using (22).

$$IF = 1 - \frac{\sum_{i,j}(\mathrm{Im}(i, j) - \mathrm{Im}'(i, j))^2}{\sum_{i,j}(\mathrm{Im}(i, j))^2} \qquad (22)$$

Value of IF should be high.

B. Robustness Analysis

If watermarks are available in the form of logo which are visually meaningful then using visual artifacts in extracted watermark are qualitatively observed to check robustness of watermarked image. To compute quantitative measures following metrics are applied when watermark is in the form of logo or binary sequence. These metrics shows the extent to which extracted watermarks are reliable and readable. Notation used are mentioned below.

$Wt(i, j)$: Original Watermark

$Wt'(i, j)$: Extracted Watermark

- *Correlation Coefficient (CRC):* This metric is calculated to find compatibility present between original and extracted watermark. Value of CRC should lie between 0 and 1. CRC can be estimated using (23)

$$CRC = \frac{\sum_i\sum_j Wt(i, j)Wt'(i, j)}{\sqrt{\sum_i\sum_j Wt(i, j)^2 \times \sum_i\sum_j Wt'(i, j)^2}} \qquad (23)$$

- *Similarity Measure (SIM):* Similarity measure is computed for assessment of extraction fidelity. It shows the similarity between extracted and embedded watermark. SIM is also known as Similarity Coefficient (SC). SC can be measured using (24)

$$SIM(Wt, Wt') = \frac{\sum_i\sum_j Wt(i, j)Wt'(i, j)}{\sum_i\sum_j Wt'(i, j)^2} \qquad (24)$$

- *Bit Error Rate (BER):* BER [32] is used for representing probability of wrongly detected binary patterns. This performance metric suited to random binary sequence watermark. This metric shows the ratio of faulty decoded bits and length of binary sequence. It can be measured using (25)

$$BER = \frac{DB}{TB} \qquad (25)$$

Where, DB shows number of incorrectly decoded bits and TB shows total number of bits.

- *Accuracy Ratio (AR):* This performance metric is useful in calculating resemblance between original watermark and extracted watermark. It is computed as the ratio between number of correct bits between original and extracted watermark and

total number of bits in original watermark. It can be estimated using (26).

$$AR = \frac{CB}{TB} \quad (26)$$

Where, CB shows number of correct bits and TB shows total number of bits of original watermark. If AR value is nearer to 1 it means high resemblance between original watermark and extracted watermark.

IX. Conclusion

Due to increase in exchange of digital information there is high requirement of data security. Multimedia documents like audio, video, images get effected due to transmission of data through different medium. Users are expecting more effective solutions which can ensure copyright protection and authenticity of documents should be maintained. Nowadays, there is high demand of image manipulation tools and techniques which caused development of more effective and sophisticated tools and these tools are available to various peoples. Unfortunately, such situations has increased the production of more specialized counterfeit. Image watermarking, a very recent arena of research can be used as complementary countermove methods. This approach is mainly concerned to content authentication than to rigorous digital integrity. In current scenario, it is complicated to state that which method is more worthy to assure integrity service to multimedia documents. In this paper digital watermarking overview, characteristics, techniques, attacks, applications are discussed. As per survey done for watermarking techniques, several techniques are discoursed as spatial domain and frequency domain based techniques. In case of frequency domain (DCT, DFT, DWT) information can be diffused to entire image so these techniques are more robust than spatial domain watermarking techniques. DWT based techniques are more effective due to multiresolution characteristic and splendid time frequency analysis. Image features are highly invariant to deformations so these can be utilized for detecting insertion positions. The main purpose of watermarking techniques is to restrict both geometrical and signal processing attacks. Since, no such watermarking technique is detected which can resist all the attacks performed over digital media. There is lot of scope for robust watermarking technique. In future using different robust features and suitable embedding techniques, robustness of watermarking techniques can be enhanced. Techniques which are truly transparent, secure and robust should be developed. Several optimizations methods can be applied to identify regions of watermark imbedding.

References

[1] C. S. Lu, “Multimedia Security: Steganography and Digital Watermarking for Protection of Intellectual Property”, Idea Group Publishing, 2005. DOI: https://doi.org/10.4018/978-1-59140-192-6

[2] F. Hartung, and M. Kutter, “Multimedia Watermarking Techniques”, Proc. IEEE, Special Issue on Identification and Protection of Multimedia Information, vol. 87, pp. 1079–1107, July 1999. DOI: https://doi.org/10.1109/5.771066

[3] K. Veeraswamy, B. Chandra Mohan and S.Srinivas, “HVS Based Robust Digital Watermarking Scheme using Contourlet”, International Journal of Computer Science and Network Security, vol.8, no.2, February 2008. DOI: DOI: https://doi.org/10.1117/12.853476

[4] G. C. Kesseler,"An Overview of Steganography", James Mandison University Infosec Transport, 2011. DOI: https://doi.org/10.1016/b978-0-12-385510-7.00002-3

[5] H. Inoue, A. Miyazaki and T. Katsura, “An Image Watermarking Method Based on the Wavelet Transform”, IEEE Conf. on Image Processing, vol. 1, pp. 296-300, 1999.DOI: https://doi.org/10.1109/icip.1999.821617

[6] Xi Zhao, Anthony T. S. Ho, “An Introduction to Robust Transform Based Image Watermarking Techniques”, Intelligent Multimedia Analysis for Security Applications , pp. 337-364, 2010. DOI: https://doi.org/10.1007/978-3-642-11756-5_15

[7] R. C. Gonzalez, R. E. Woods, B. R. Masters, “Digital Image Processing,” Third Edition, 2008. DOI: https://doi.org/10.1117/1.3115362

[8] J. C. Murphy, D. Dubbel, and R. Benson, “Technology Approaches to Currency Security,” in Optical Security and Counterfeit Deterrence Techniques II, vol. 33, no. 14, pp. 21–28, 1998. DOI: https://doi.org/10.1117/12.304695

[9] M. L. Miller, I. J. Cox and J. A. Bloom, “Watermarking in the Real World: An application to DVD,” in Multimedia and Security—Workshop at ACM Multimedia’98 (GMD Report), vol. 41, pp. 71–76, 1998.DOI: https://doi.org/10.1109/acssc.1999.831999

[10] P. Tao and A. M. Eskicioglu, “A Robust Multiple Watermarking Scheme in the DWT Domain,” Optics East 2004 Symposium, Internet Multimedia Management Systems V Conference, Philadelphia, PA, pp. 133-144, October 25-28, 2004. DOI: https://doi.org/10.1117/12.569641

[11] R. B. Wolfgang and E. J. Delp, “A watermark for Digital Images,” in Proc. IEEE Int. Conf. Images Processing,” Lausanne, Switzerland, pp. 219–222, September 1996. DOI: https://doi.org/10.1109/icip.1996.560423

[12] Tang Wenliang,”A Feature-Based Digital Image Watermarking Algorithm Resisting to Geometrical Attacks,” Second International Symposium on Electronic Commerce and Security, IEEE, 2009. DOI: https://doi.org/10.1109/isecs.2009.94

[13] N. Deshpande, A. Rajarkar, R.R. Muthalkar, “Robust Dual Watermarking Scheme for Video Derived from Strategy Fusion,” International Journal of Image, Graphics and Signal Processing, vol. 6, no. 5, pp. 19-27, 2013. DOI: https://doi.org/10.5815/ijigsp.2014.05.03

[14] C. Lu and H. Yuan M. Liao, “Multipurpose Watermarking for Image Authentication and Protection,” IEEE Transactions on Image Processing, vol. 10, no.10, pp. 1579–1592, October 2001. DOI: https://doi.org/10.1109/83.951542

[15] M. Miller, I. J. Cox, J. P. Linnartz and T. Kalker, “A review of watermarking principles and practices,” In Digital Signal Processing in Multimedia Systems, pp. 461-485, 1999.

[16] J. G. Proakis, “Digital Communications,” McGraw-Hill, New York, NY, USA, 3rd edition, 1995.

[17] C. Rey, “Blind Detection of Malicious Alterations on Still Images using Robust Watermarks,” in Secure Images and

Image Authentication Colloquium, IEE Electronics & Communications, London, UK, 2000. DOI: https://doi.org/10.1049/ic:20000218
[18] A. K. Singh, N. Sharma, M. Dave and A. Mohan "A novel technique for digital image watermarking in spatial domain," in Parallel Distributed and Grid Computing (PDGC), 2nd IEEE International Conference, pp. 497-501, 2012. DOI: https://doi.org/10.1109/pdgc.2012.6449871
[19] Neeta Deshpande, Snehal Kamalapur and Jacobs Daisy, "Implementation of LSB steganography and Its Evaluation for Various Bits," 1st International Conference on Digital Information Management, pp. 173-178, 6 Dec. 2006. DOI: https://doi.org/10.1109/icdim.2007.369349
[20] Tosihiro Akiyama, Fumiaki Motoyoshi, Osamu Uchida and Shohachiro Nakanishi, "Hybrid Digital Watermarking for Color Images Based on Wavelet Transform," IADIS International Conference Applied Computing 2006, San Sebastian, Spain, February 2006.
[21] S. D. Lin., S. C. Shie and J.Y. Guo "Improving the Robustness of DCT-Based Image Watermarking Against JPEG Compression," Computer Standards & Interfaces, vol. 32, pp. 54-60, 2010. DOI: https://doi.org/10.1016/j.csi.2009.06.004
[22] A. M. Kothari, V. Dwivedi, "Video Watermarking Combination of Discrete Wavelet & Cosine Transform to Achieve Extra Robustness," International Journal of Image, Graphics and Signal Processing, vol. 5, no. 3, pp. 36-41, 2013. DOI: https://doi.org/10.5815/ijigsp.2013.03.05
[23] P. Tao and A. M. Eskicioglu, "A Robust Multiple Watermarking Scheme in the DWT Domain," Optics East 2004 Symposium, Internet Multimedia Management Systems Conference, Philadelphia, pp. 133-144, October 25-28, 2004. DOI: https://doi.org/10.1117/12.569641
[24] Baisa L. Gunjal and R.R. Manthalkar "An Overview Of Transform Domain Robust Digital Image Watermarking Algorithms," Journal of Emerging Trends in Computing and Information Sciences, 2011.
[25] H.-H. Tsai, Y. J. Jhuang and Y. S. Lai "An SVD-based Image Watermarking in Wavelet Domain using SVR and PSO", Applied Soft Computing, vol. 12, pp. 2442-2453, 2012. DOI: https://doi.org/10.1016/j.asoc.2012.02.021
[26] L. Robert and T. Shanmugapriya," A Study on Digital Watermarking Techniques", International Journal of Recent Trends in Engineering, vol. 1, no. 2, May 2009.
[27] N. Chandrakar and J. Baggaa,"Performance Comparison of Digital Image Watermarking Techniques: A Survey," International Journal of computer Application Technology and Research, vol. 2, no. 2, pp. 126-130, 2013. DOI: https://doi.org/10.7753/ijcatr0202.1008
[28] D. Mistry, "Comparison of Digital Watermarking Methods," International Journal on Computer Science and Engineering, vol. 02, no. 09, pp. 2905-2909, 2010.
[29] J. Fridrich, M. Goljan, and R. Du, "Invertible Authentication," in Proc. SPIE Conf. Security and Watermarking of Multimedia Contents III San Jose, Calif, USA, vol. 43, no. 14, pp. 197–208, , January 2001. DOI: https://doi.org/10.1117/12.435400
[30] Shereem Ghanem and Fatma A.E. Abou-Chadi, "Contourlet Versus Wavelet Transform: A Performance Study for a Robust Image Watermarking," 2009. DOI: https://doi.org/10.1109/icadiwt.2009.5273921
[31] Sin-Joo Lee and Sung-Hwan Jung, "A Survey of Watermarking Techniques Applied toMultimedia," ISIE 2001. DOI: https://doi.org/10.1109/isie.2001.931796
[32] V. S. Jabade and S. R. Gengaje, "Literature Review of Wavelet Based Digital Image Watermarking Techniques," International Journal of Computer Appliations, vol. 31, no. 1, 2011, pp 28-36.

Authors' Profiles

Anuja Dixit is a Research scholar pursuing M.Tech in Cyber Secutity from Madhav Institute of Technology & Science, Gwalior, India. She has received B.Tech degree in Computer Science & Engineering from University Institute of Engineering & Technology, Kanpur, Uttar Pradesh, India.

Rahul Dixit is a Research Scholar pursuing Ph.D. from National Institute of Technology, Rourkela, India. He has received M.Tech. degree from Indian Institute of Technology, Dhanbad, India. His area of specialization is Multimedia Security.

How to cite this paper: Anuja Dixit, Rahul Dixit,"A Review on Digital Image Watermarking Techniques", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.9, No.4, pp.56-66, 2017.DOI: 10.5815/ijigsp.2017.04.07

