# Overview of Image Watermarking And Digital Image Watermarking With Their Applications, Requirements, Techniques And Attacks

**Mr. Narendra Kumar Rayakwar[1], Dr. Nirupma Tiwari[2]**
[1]Dept of computer science
[2]Associate Professor, Dept of computer science
[1, 2] SRCEM, RGPV University Bhopal India

***Abstract***- *Digital communication plays a vital role in the world of Internet as well as in the communication technology. The secrecy of the communication is an essential part of passing the data or information. The digital watermarking is a field of hiding information which hides the crucial information in the original data for protection illegal duplication and distribution of multimedia data. Watermarking is an important application in the image processing. Watermarking is the process of inserting the watermarked message in a host document in some multimedia format. It is basically required to protect the information from the unauthorized access. The image watermarking techniques may divide on the basis of domain like spatial domain or frequency domain or on the basis of wavelets. This paper incorporates the detail study of digital watermarking definition, concept in a detailed and the main contributions in this field such as categories of image watermarking process. It starts with overview, applications, process of watermarking, requirements, techniques or classification, and various attacks of watermarking.*

***Keywords***- Image Watermarking, Digital watermarking, Image Embedding, Digital Watermarking Techniques, Watermarking Attacks

## I. INTRODUCTION

Currently, the availability of image processing technology is highly diverse, thus image content becomes easily manipulated by irresponsible parties. Replacement of content is very harmful to the owner especially when it comes to legal cases. Therefore, research on detection and localization of tampered images is an important issue. One approach that is widely used is the technique of digital watermarking. This is a technique of inserting secret information or image’s information into an original image prior to sending. The original image is the image where the confidential information is inserted, while the secret information is a watermark. The watermark component selection is done by considering the purpose of the watermarking technique. In general, the watermark used for image authentication and recovery uses two watermarks, which are bit authentication and bit recovery. For image recovery, bit recovery is selected from the image feature, usually from the original image compression form. When the watermark used is generated from the original image, it is known as the self-embedding watermarking scheme [1].

Watermarking is a branch of information hiding which is used to hide proprietary information in digital media like photographs, digital music, or digital video. The ease with which digital content can be exchanged over the Internet has created copyright infringement issues. Copyrighted material can be easily exchanged over peer-to-peer networks, and this has caused major concerns to those content providers who produce these digital contents. This paper provides a survey of techniques to watermark data files like text, images, audio and video [2].

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence [3].

Watermarks are embedded into images by changing some bits in image representation. The original data (payload) is first encrypted and watermarked in encoder (sender) and then sent to a decoder (receiver) through the internet to be decrypted and extracted. The most important properties of any digital watermarking techniques are robustness, security, imperceptibility, complexity, and verification. Robustness is defined as if the watermark can be detected after media (normal) operations such as filtering, lossy compression, colour correction, or geometric modifications. Security means the embedded watermark cannot be removed beyond reliable detection by targeted attacks. Imperceptibility means the watermark is not seen by the human visual system. Complexity is described as the effort and time required for watermark embedding and retrieval. Lastly, verification is a procedure whereby there is private key or public function (Dittmann, Mukherjee & Steinebach, 2000). Each of these properties must be taken into consideration when applying a certain digital watermarking technique. Furthermore, the watermark must be either robust or fragile, depending on the application. By "robust", we mean the capability of the watermark to resist manipulations of the media, such as lossy compression (where compressing data and then decompressing it retrieves data that may well be different from the original, but is close enough to be useful in some way), scaling, and cropping, among others. [4]

**Image Watermarking**

Image Watermarking is the technique of embedding of owner copyright identification with the host image. When and how watermarking is used first is the topic of discussion but it can used at Bologna, Italy in 1282 .at first it is used in paper mills as paper mark of company. Then it is common in practice up to 20th century. After that watermark also used in the postage stamp and currency notes of any country. Image watermarking is an efficient method for hiding the information in the image. It is the secure method for the reliable communication [4].

**Process of Image Watermarking**

The process of watermarking is divided into two parts [5]:

- Embedding of watermark into host image.
- Extraction of watermark from image

a. **Watermarking Embedding:** The process of image watermarking is done at the source end. In this process watermark is embedding in the host image by using any watermarking algorithm or process.
b. **Watermarking Extraction:** This is the process of Extracting watermark from the watermarked image by reverse the embedding algorithm.

**Applications of the Image watermarking**

Image watermarking can be used for varieties of applications; some of the applications are given below [5]:

a. **Tamper detection:** Image watermark are used for the tamper detection, it identifies the degrade or destroy watermark in the image and that content is not trusted.

b. **Telecast monitoring:** This type of monitoring is used to especially in the advertisements to make sure that the content broadcasted as the contract between the advertisement company and the customer.

c. **Software clipping:** In this the consumers are able to see the software before they buy it , some of the features of the program such as saving it, or printing it are disabled until they purchase a registration key to use it for this the watermarking is used .
d. **Copyright protection:** Image watermarking is basically used for the copyright protection. The copyright data or information can be inserted as the watermark into the image and can be extracted to show the ownership of the company if needed.

e. **Validation of the Authentication and integrity**: To detect whether the image is modified or not watermark can be used. Integrity of image can be verified by using fragile watermark which has low robustness.

f. **Medical applications:** Image watermarking can be also used in the medical images .it can be used for keeping the patient’s data confidential so that an unauthorized user cannot access it.

**Watermarking Properties**

Watermarking need some desirable properties based on the application of the watermarking system some of the properties are presented here [6]:

a. **Effectiveness:** This is the most important property of watermark that the watermark should be effective means it should surely be detective. If this will not happened the goal of the watermarking is not fulfilled.

b. **Host signal Quality:** This is also important property of watermarking. Everybody knows that in watermarking, watermark is embedded in host signal (image, video, audio etc.). This may put an effect on the host signal. So the watermarking system should be like as, it will minimum changes the host signal and it should be unnoticeable when watermark is invisible.

c. **Watermark Size:** Watermark is often use to owner identification or security confirmation of host signal and it always use when data is transmitted. So it is important that the size of watermark should be minimum because it will increases the size of data to be transmitted.

d. **Robustness:** Robustness is crucial property for all watermarking systems. There are so many causes by which watermark is degraded, altered during transmission, attacked by hackers in paid media applications. So watermark should robust, So that it withstand against all the attacks and threats [7].

**Digital Watermarking**

Digital Watermarking started back in 1979, but it was not until 1990 that it gained popularity. Its full-fledged application began around 1998. No one is credited with founding or inventing the digital watermark, still it is in its growth stages today, and with cases like Napster, it is showing more and more reasons to have digital watermarking. Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography. But unlike steganography, watermarks typically hide very little information and rely on the part on redundancy of the mark to survive attacks such as cropping. Digital watermarks contain information that may be considered attributes of the covering image such as copyright data, and the cover is the object of communication - not the watermark. It is a digital signal or pattern inserted into a digital document such as text, graphics or multimedia, and carries information unique to the copyright owner, the creator of the document or the authorized consumer. Watermarking leaves the original file/ image intact and recognizable [8].

**Digital Watermarking Technology**

As an emerging technology, digital watermarking involves the ideas and theories of different subject coverage, such as signal processing, cryptography, probability theory and stochastic theory, network technology, algorithm design, and other techniques. Digital watermarking hides the copyright information into the digital data through certain algorithm. The secret information to be embedded can be some text, author‘s serial number, company logo, images with some special importance. This secret information is embedded to the digital data (images, audio, and video) to ensure the security, data authentication, identification of owner and copyright protection. The watermark can be hidden in the digital data either visibly or invisibly. For a strong watermark embedding, a good watermarking technique is needed to be applied. Watermark can be embedded either in spatial or frequency domain. Both the domains are different and have their own pros and cons and are used in different scenario [6].

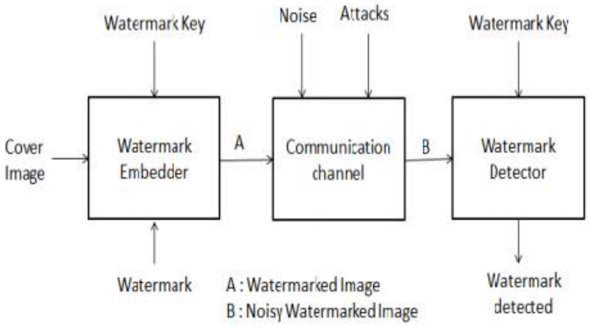

Figure 1: Digital watermarking System

**Application of Digital Image Watermarking**

a. **Copyright Protection:** The copyright information can be embedded as a watermark into the new production. Once there is a dispute on the ownership, the watermark can be extracted to provide the evidence of who is the owner of this product.

b. **Authentication:** The watermark is embedded to detect if the image has been modified or not, this process can be used for authentication.

c. **Broadcast Monitoring:** This type of monitoring is used especially in the advertisements to make sure that the content broadcasted as the contract between the advertisement company and the customer.

d. **Owner Identification:** To achieve owner identification, there was a traditional form for intellectual ownership verification which was a visual mark. However, nowadays, this is easily overcome by the use of some software’s that modify images. For example, the images with the copyright registration symbol c which have this mark is removed by specialized software. To solve this problem, invisible watermarks are used in order to overcome the problem.

e. **Fingerprinting:** The main purpose of fingerprinting is to protect customers. If someone got a legal copy of a product, but redistributed illegally, fingerprinting can prevent this. This can be achieved by tracing the whole transaction by embedding unique robust watermark for each recipient. Thus, the owner can identify who redistributed this product by extracting the watermark from the illegal copy.

f. **Copy Control:** The watermark contains owner data and specifies the corresponding amount of copies allowed. This presupposes hardware and software for updating the watermark whenever it has been used. It also provides copy tracking for unauthorized distribution since the owner of data is embedded in the watermark.

g. **Tamper proofing:** Digital watermarks which are fragile in nature, can be used for tamper proofing. Digital content can be embedded with fragile watermarks that get destroyed whenever any sort of modification is made to the content. Such watermarks can be used to authenticate the content.

### Requirements of Digital Image Watermarking

Digital image watermarking concerns to solve some issues properly, thus, this paper highlights the main requirements of watermarked image as following [9]:

a. **Robustness:** The robustness is the ability of detecting the watermark after some signal processing modification such as spatial filtering, scanning and printing, lossy compression, translation, scaling, and rotation, and other operations like digital to analog (D/A), analog to digital (A/D) conversions, cutting, image enhancement. In addition, not all watermarking algorithms have the same level of robustness, some techniques are robust against some manipulation operations, however, and they fail against other stronger attacks. Moreover, it’s not always desirable for watermark to be robust, in some cases; it’s desired for the watermark to be fragile. Therefore, the robustness can be classified as following:

b. **Imperceptibility:** Imperceptibility (also known as Invisibility and Fidelity) is the most significant requirement in watermarking system, and it refers to the perceptual similarity between the original image before watermarking process and the watermarked image. In other words, the watermarked image should look similar to the original image, and the watermark must be invisible in spite of occurrence of small degradation in image contrast or brightness. However, the challenge is that imperceptibility could be achieved, but the robustness and the capacity will be reduced, and vice versa, imperceptibility may be sacrificed by increasing the robustness and the capacity. Moreover, the watermark not always desired to be invisible, sometimes, it is preferred to have visible watermark into the image.

c. **Capacity:** Capacity (also known as Payload) refers to the number of bits embedded into the image. The capacity of an image could be different according to the application that watermark is designed for. Moreover, studying the capacity of the image can show us the limit of watermark information that would be embedded and at the same time satisfying the imperceptibility and robustness.

d. **Security:** Security is the ability to resist against intentional attacks. These attacks intended to change the purpose of embedding the watermark. Attacks types can be divided into three main categories: unauthorized removal, unauthorized embedding, and unauthorized detection. According to the specific usage of watermarking, the specific feature should be available in the watermark to resist the attacks. Therefore, for unauthorized removal, the watermark should be robust and not to be removed, and for unauthorized embedding (also known as forgery), the watermark should be fragile or semi fragile to detect any modification. Lastly, for unauthorized detection, it should be imperceptible watermark.

e. **Low Complexity:** The cost is the reason behind studying the complexity, so it should be at a reasonable cost. It describes the economics of using watermark embedders and detectors, because it can be very complicated and depends on business model that is used. The main two issues of complexity are the speed of embedding and detection, and the number of embedders and detectors.

### Digital Watermarking Techniques

Digital watermarking is the general technique of embedding some information in the original file, such that an altered file is obtained. This information serves as one of different uses, such as, identifying piracy, sensing tampering, or reassuring integrity. The approaches to watermarking are diverse and can be broadly classified based on their visibility, robustness, or fragility. Their uses are also versatile, as they can be applied to text, images, audio, or video. Digital watermarking comprise of various watermarking techniques for the protection of the data. Watermarking techniques are divided into two categories [10]:

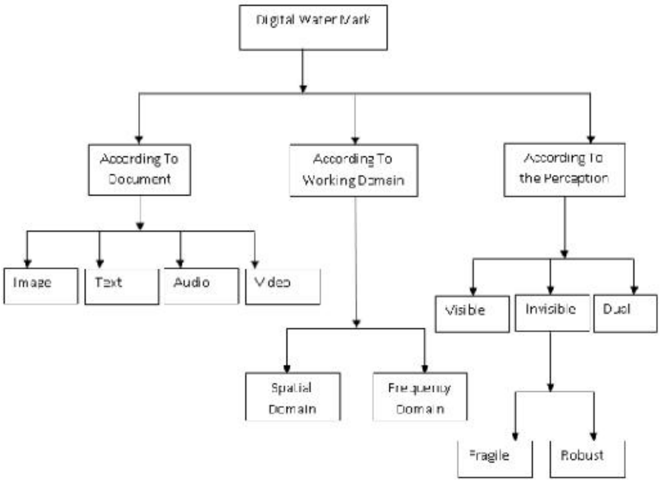

Figure 2: Classification of Digital Watermarking techniques

## A. According to Document

There are arranged into four categories [7]

- **Image watermarking:** This is used to conceal the particular information into the image and to identify and extract that particular information for the author’s ownership.
- **Video watermarking:** This inserts watermark into the video stream to organize video applications. It is the expansion of image watermarking. This method forces actual time quality extraction and robustness for compression.
- **Audio watermarking:** This inserts watermark to the audio signals such as MP3 or internet music to embed and it is used to identify the copyright.
- **Text watermarking:** This includes watermark to the PDF, DOC and other text file to avoid the changes made to the text. The watermark is appended in the font shape and the space between characters and line spaces.

## B. According to Working Domain

There are arranged into 2 categories [7]

1. Spatial domain watermarking
2. Frequency Domain watermarking

### 1. Spatial domain watermarking

In this type of watermarking the information is added by varying the pixel values of the carrier signal .least significant bit is one of technique of the spatial domain watermarking. Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. On the other side, in frequency domain techniques the image is first transformed to the frequency domain by the use of any transformation methods such as Fourier transform, discrete cosine transform (DCT) or discrete wavelet transform (DWT). Now the information is added to the values of its transform coefficients. After applying the inverse transform, the marked coefficients form the embedded image.

#### a. Least significant bit

The watermark is added in the pixel of the image. The pixel of the images is accessed and the information which is to send is inserted in the pixel. This provides security to the data that is to be transmitted. In this technique watermark is embedded in the LSB of pixels. Two types of LSB techniques are proposed. In the first method the LSB of the image was replaced with a pseudo-noise (PN) sequence while in the second a PN sequence was added to the LSB. This method is easy to use but not very robust against attacks.

#### b. Patchwork Technique

In patchwork, n pairs of image points, (a, b), were randomly chosen. The image data in a were lightened while that in b were darkened .High level of robustness against many types of attacks are provided in this technique. But here in this technique, very small amount of information can be hidden.

#### c. Predictive Coding Scheme

In this method, a pseudorandom noise (PN) pattern says W(x, y) is added to cover image. It increases the robustness of watermark by increasing the gain factor. But due to high increment in gain factor, image quality may decrease.

### 2. Frequency Domain watermarking

In this type of watermarking the information is embedded into the frequency coefficient of the carrier signal. It is more robust, and its capacity of hiding the information is more. Fourier transforms (FT), discrete cosine transform (DCT), discrete wavelet transform (DWT) etc are some of the technique of frequency Domain watermarking.

#### a. Discrete cosine transform (DCT)

In discrete cosine transform an image is broken into the different frequency bands that are high, medium and low frequency bands. It transforms a signal from the spatial domain to the frequency domain. The watermark is embedded into these band according to the choice made. DCT is applied in many fields like data compression, pattern recognition and every field of image processing. DCT is a real transform with better computational efficiency and also gives a better performance in the bit rate reduction.

**b. Discrete wavelet transform (DWT)**

In discrete wavelet transform images is divided into sub bands of different resolution. On the arrival of the image the decomposition of an image can be done at different level using series of low pass and high pass filter. Due to its spatial localization and multi resolution technique DWT is used in the digital watermarking. it give better visual image quality , localization and is highly robust technique.

**c. Discrete Fourier transform (DFT)**

It transforms a continuous function into its frequency components. Discrete Fourier transform is scaling, rotation and translation invariant whereas the spatial domain DCT and DWT are not RST invariant. So DFT can be used to recover from various geometric attacks such as cropping.

**C. According to Human Perception**

a. **Visible watermarking:** Visible watermarking was the first and most fundamental way of watermarking. Visible watermarks are one, which are embedded in visual content in such a way that they are visible when the content is viewed. In this method the concealed object is taken and the watermark is added on it. This makes the watermark visible on the concealed object.

b. **Invisible Watermarking:** In invisible watermarking, secret data is added as digital data to audio, picture or video but it cannot be identified. An invisible watermark is a concealed image, which cannot be seen, but which can be detected algorithmically. The watermark, generally a personal Identification Number, is digitally embedded within the image. While these watermarks can be defeated, they propose confirmation of your ownership if they always turn up in a publication without your authorization. Invisible watermark is used as verification of ownership and to detect misappropriated images. An invisible watermark is used as a backup for the visible watermark.

c. **Dual watermarking:** This technique is a pattern of visible and invisible watermark. It contains both visible and invisible watermark inside the conceal.

d. **Robust Watermarking:** Robust watermarking is a technique in which modification to the watermarked content will not affect the watermark. The term robust watermark describes those watermarks that can be detected within an object after significant levels of tampering of all kinds. The detection process of watermark can give just the probability of availability of watermark if the tampering level is too high. However, when an object is tampered with, it is automatically modified from the original, and in that sense its quality is degraded. This degradation can either be detected or not by the human sensors. Therefore, we can define some limits for the maximum required robustness of the embedded watermark. In robust watermarking applications, the extraction algorithm should be able to accurately produce the watermark, even if the modifications were strong.

e. **Fragile Watermarking:** Fragile watermarking is a technique in which watermark gets damaged when watermarked content is modified or manipulated with. A watermark that potentially displays selective robustness, generally called fragile watermark, is required for tamper-proofing purposes. In short, fragile watermarking involves embedding information into a file which is damaged if the file is modified. This method is inappropriate for footage the copyright holder of the file since it can be so easily removed, but is useful in situations where it is important to prove that the file has not been damaged with, such as using a file as proof in a court of law, since any damaging would have removed the watermark. Fragile watermarking techniques tend to be easier to implement than robust methods. In fragile watermarking, the extraction algorithm should fail if any change is made to the signal [11].

**Watermarking Attacks**

The transmission media can cause some loss in the signal implying in a damaged content. These attacks may be intentional or accidental [6]. Intentional attacks use all available resources to destroy or modify the watermark making it impossible to extract it, the methods usually used are: signal processing techniques, cryptanalysis, steganalysis. On the other hand, accidental attacks are inevitable, because every image processing or transmission noise may introduce distortions. Besides these types, there are other types of attacks called estimation based on attacks. In estimation based attacks, estimates of either the watermark data or the original object can be obtained using stochastic methods [12].

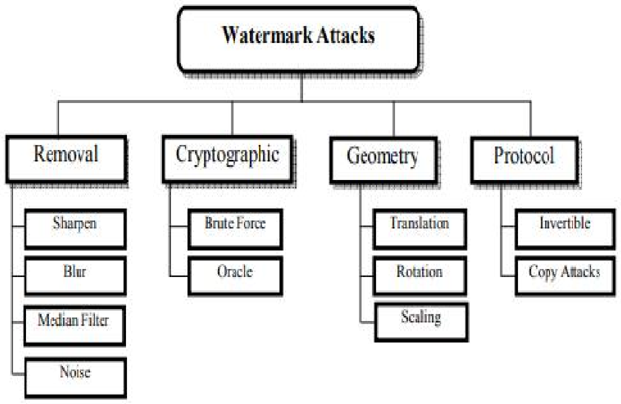

Figure 3: Classification of watermark attacks

1. **Removal and Interference Attacks:** Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal. Moreover, interference attacks are those which an additional noise to the watermarked object. Lossy compression, quantization, collusion, denoising, remodulation, averaging and noise storm are some examples of this category of attacks. The collusion attack occurs when a number of authorized recipients of the multimedia object come together to generate an unwatermarked object by averaging all the different watermarked objects.

2. **Geometric Attacks:** Geometric attacks are specific to images and videos. Geometric attacks do not actually remove the watermark, but manipulate the watermarked object in such a way that the detector cannot find the watermark data. This type of attack includes affine transforms such as rotation, translation, and scaling. Warping, line/column removal and cropping are also included in this family of attacks. Another example of geometric attack is the mosaic attack. In this mosaic attack, the watermark image is divided into several parts and rearranged using proper HTML code, constructing watermark image in which the watermark detector will fail to provide desired results. Local pixel jittering is an efficient spatial domain geometric attack.

3. **Cryptographic Attacks:** The above two types of attacks, removal and geometric, do not breach the security of the watermarking algorithm. On the other hand, cryptographic attacks deal with the cracking of the security. For example, finding the secrete watermarking key using exhaustive brute force method is a cryptographic attack. Another example of this type of attack is the oracle attack [7]. In the oracle attack, a non-watermarked object is created when a public watermark detector device is available. These attacks are similar to the attacks used in cryptography.

4. **Protocol Attacks:** The protocol attacks exploit the loopholes in the watermarking concept. One example of such attack is the IBM attack [8]. The IBM attack is also known as the deadlock attack, inversion attack, or fake-original attack. This attack embeds one or several additional watermarks such that it is unclear which the watermark of the original owner was. Watermarking of an already watermarked image is called re-watermarking. In some inversion attacks, a fake original object is created that produces the same results through the detector as that of the real original object.

## II. LITERATURE REVIEW

**Soppari, K., & Chandra, N. S. [2020]** plans to develop an effective digital watermarking framework using an optimized clustering approach. The proposed model consists of several phases like image scaling, block separation, computation of feature vectors, spotting of regions for watermarking, message transformation, watermark embedding, IDCT, and message restoration. After image scaling, the block separation is done by DCT, and further, the feature vectors correspond to the pixel values are extracted. The optimized FCM clustering is adopted to categorize the blocks into suitable and unsuitable watermarking regions. The optimized FCM with Least Favorable-based Whale Optimization Algorithm (LF-WOA) enabled initial centroid selection takes the decision regarding the regions where the watermark can be inserted. After the watermarking embedding, the message is restored by the reverse process. Finally, the experimental results will achieve a higher demand for watermarking in terms of robustness and sensitivity [13].

**P. Pal et al. [2018]** comprehend the concept, details, properties, techniques and application of digital watermarking.

In today's era, with the increasing use of internet it's become challenging to secure data. In sequence to authenticate or protect digital media from the various attacks techniques like cryptography, steganography and digital watermarking are introduced. Digital watermarking technique hides the secret information (Watermark) in multimedia data for the purpose of protection, copyright and authentication. The secret information is submerged into the cover data with the minimum or negligible distortion of cover data [14].

**Y. He and Y. Hu [2018]** In this paper, a watermarking algorithm of color image is proposed based on Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition (DWT-DCT-SVD). First convert host color image from RGB color space to YUV color space. Then a layer of discrete wavelet transform is applied to the luminance component Y, and divided the low frequency and into blocks by using discrete cosine transform, and conducted SVD with every block. Finally embed watermark to the cover image. The experimental results show that the algorithm is good invisibility and strong robust, and can effectively resist common watermark attacks [15]

**W. Zhang et al. [2018]** aimed to summarize the research program of applying digital watermarking technology for printing, and find a kind of printing anti-counterfeiting technology which is difficult to copy, easy to identify, bottom cost and pollution-free. We summarized the research program of three stages that included generating and embedding watermarks, printing and scanning, extracting and detecting watermarks, was defined that divided from the process of digital watermarking technology. The results shown that, further studies could focus on the research on effects of the printing and scanning attacks on watermarks, so the relationship of invisibility and robustness to resist printing-scanning attacks could be balanced. Due to digital watermarking technology that was applied to digital images, it was necessary to research the fragile ability that prevents the secondary printing to establish the relationship between watermarking algorithm, printing process and parameters [16].

**Y. Guo et al. [2018]** In this paper, a new data embedding domain, rounding/truncation error domain, is discovered for JPEG image data embedding. This RTE domain is obtained by calculating the rounding/truncation error during the decompression of JPEG image. With the new domain discovered, a new data embedding method DRDE, which can be generally applied to data hiding and authentication, is designed to demonstrate the usage of RTE domain. DRDE embeds data by modifying the RTE domain values according to the guidelines that the amendments should be reduced after the rounding/truncation step at the JPEG standard decoder side, which can thus improve the imperceptibility of the proposed method [17].

**E. Mathur and M. Mathuria [2017**] This research is done to find the best digital watermarking technique to highly secure digital image form the illegal copies. The research work also done to analyze the possibilities of dual watermarking. Various standard research articles were studied and it is found that dual watermarking is possible with some situation. This research work motivates and offers different combinations on digital watermarking techniques in near future for efficient output of watermarking.[18]

**M. Boreiry and M. Keyvanpour [2017]** The main goal of this manuscript is to investigate the video watermarking methods with declaring the strengths and weaknesses of each method. Of course, each case besides the weakness is suitable for certain applications in watermarking. And also, besides the mentioned methods, combining the basic approaches in this field will lead to increase the efficiency of proposed algorithm. By considering the expected application and investigating event vulnerability, appropriate solution can be represented due to prepare minimum security requirements. [19]

**R. S. P. Rao and P. R. Kumar [2016]** Proposed Genetic Algorithm based Digital Image watermarking scheme is improved by embedding the watermark in Third Level Discrete Wavelet Transform (DWT) of original image, after applying Singular Value Decomposition (SVD) to watermark image. The Genetic Algorithm optimization technique (GA) is used for best scaling factor (SF) to modify the SVD coefficients of watermark image. The PSNR and NCC used as fitness function in GA and it evaluate the Robustness and Imperceptibility of watermarking scheme. Experimental results are provided to illustrate that the proposed scheme is able to withstand a variety of image processing attacks very well and comparison is made with previous work [20].

## III. CONCLUSION

Digital watermarking of multimedia content has become a very active research area over the last several years. Watermarking is a very important field for copyrights of various electronic documents and media. With images widely available on the Internet, it may sometimes be desirable to use watermarks. Digital watermarking is the processing of combined information into a digital signal. A watermark is a secondary image, which is overlaid on the host image, and provides a means of protecting the image. It acts as a digital signature, giving the image a sense of ownership or authenticity. Digital watermarking technique is very impressive for image authentication or protection for attacks. In this paper we presented digital watermarking overview, application, Requirements, attacks and techniques. We tried to classify and analyze many recent watermarking techniques.

## REFERENCES

[1] Rakhmawati, L., Wirawan, W., & Suwadi, S. (2019), “A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability”, EURASIP Journal on Image and Video Processing, 2019(1), doi: 10.1186/s13640-019-0462-3.

[2] https://www.researchgate.net/publication/242571578_A_Study_on_Digital_Watermarking_Techniques

[3] https://www.cl.cam.ac.uk/teaching/0910/R08/work/essay-ma485-watermarking.pdf.

[4] Lalit Kumar Saini , Vishal Shrivastava,” A Survey of Digital Watermarking Techniques and its Applications”, International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, May-Jun 2014.

[5] Dr.B.Hari Krishna and Dr.T.Sarvanan, “A survey on Digital Image Watermarking”, International Refereed Journal of Engineering and Science (IRJES) ISSN (Online) 2319-183X, (Print) 2319-1821 Volume 1, Issue 4 (December 2014), PP.49-53.

[6] Prabhishek Singh, R S Chadha ,“A Survey of Digital Watermarking Techniques, Applications and Attacks”, International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9, March 2013.

[7] Mei Jiansheng, Li Sukang, “A Digital Watermarking Algorithm Based On DCT and DWT”, Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA’09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107.

[8] Pal M. et al. [2016], “A Survey on Digital Watermarking and its Application”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016.

[9] Mohammad Abdullatif et al. [2013], “Properties of Digital Image Watermarking”, 2013 IEEE 9th International Colloquium on Signal Processing and its Applications, 8 - 10 Mac. 2013, Kuala Lumpur, Malaysia.

[10] Deepti Shukla et al. [2016], “Survey on Digital Watermarking Techniques”, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.9, No.1 (2016), pp.239-244.

[11] M.Hariharalakshmi et al. [2017], “Survey of Digital Watermarking techniques for Data security”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 3, March 2017.

[12] Kirti and Vikram Nandal [2014], “A Review on Digital Watermarking and Its Techniques”, International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 3, Issue. 6, June 2014, pg.686 – 690.

[13] Soppari, K., & Chandra, N. S. (2020), “Development of improved whale optimization-based FCM clustering for image watermarking”, Computer Science Review, 37, 100287, doi:10.1016/j.cosrev.2020.100287.

[14] P. Pal, H. V. Singh and S. K. Verma, "Study on Watermarking Techniques in Digital Images," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, 2018, pp. 372-376, doi: 10.1109/ICOEI.2018.8553743.

[15] Y. He and Y. Hu, "A Proposed Digital Image Watermarking Based on DWT-DCT-SVD," 2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Xi'an, 2018, pp. 1214-1218, doi: 10.1109/IMCEC.2018.8469626.

[16] W. Zhang, J. Meng and C. Ma, "Research progress of applying digital watermarking technology for printing," 2018 Chinese Control And Decision Conference (CCDC), Shenyang, 2018, pp. 4479-4482, doi: 10.1109/CCDC.2018.8407905.

[17] Y. Guo, X. Cao, R. Wang and C. Jin, "A New Data Embedding Method with a New Data Embedding Domain for JPEG Images," 2018 IEEE Fourth International Conference on Multimedia Big Data (BigMM), Xi'an, 2018, pp. 1-5, doi: 10.1109/BigMM.2018.8499451.

[18] E. Mathur and M. Mathuria, "Unbreakable digital watermarking using combination of LSB and DCT," 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, 2017, pp. 351-354, doi: 10.1109/ICECA.2017.8212832.

[19] M. Boreiry and M. Keyvanpour, "Classification of watermarking methods based on watermarking approaches," 2017 Artificial Intelligence and Robotics (IRANOPEN), Qazvin, 2017, pp. 73-76, doi: 10.1109/RIOS.2017.7956446.

[20] R. S. P. Rao and P. R. Kumar, "An efficient genetic algorithm based gray scale digital image watermarking for improving the robustness and imperceptibility," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016, pp. 4568-4571, doi: 10.1109/ICEEOT.2016.7755580.