International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Extensive Analysis of Digital Image Watermarking Techniques

Sachin Gaur[1] , Varun Barthwal[2]

Submitted: 18/08/2023 **Revised**: 06/10/2023 **Accepted**: 20/10/2023

Abstract: With recent advancements in information technology, digital media authenticity has become a major problem, and much study has been done to preserve digital media ownership. In all these investigations, digital image watermarking has become a crucial method. In digital image watermarking, digital content or a watermark is planted in a host image and can be removed to safeguard the host image's ownership. The two primary categories of digital image watermarking approaches are frequency domain and spatial domain. Spatial watermarking involves modifying an image's pixel values with techniques such as least significant bit (LSB) and intermediate significant bit (ISB), whereas frequency domain watermarking involves modifying an image's frequency components with techniques such as discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD). An overview of digital image watermarking, including its different types, characteristics, applications, and techniques, is given in this study. The quality of watermarking techniques is also examined using assessment metrics like PSNR and NCC, as well as various assaults that can be used against watermarked images. This wider perspective review on digital image watermarking is for those researchers who wish to get started and conduct research in this area.

***Keywords**: DWT; DCT; SVD; LSB; ISB; PSNR; NCC; BER*

1. Introduction

We are animate in a digital world where the internet has become an inevitable and indispensable part of our daily lives. Globally, every second, an immense volume of digital data comprising thousands of bytes is exchanged. With the rapid creation and consumption of digital data arises the problem of data authenticity, copyright protection, and content security during transmission [1]. To combat these issues, watermarking can be applied to any digital document. The practice of watermarking has been around for centuries, dating back to the time when paper was first invented. Watermarking was used as a tool to identify the Author of the paper and also to discourage counterfeiters. The process of adding a design pattern on the paper takes place when the paper is wet, which is why it is called a 'watermark' [2]. With the rise of digital media, the need for watermarking has moved from physical paper to digital documents, and this concept of digital watermarking was first introduced in the late 1980s and early 1990s as a way to protect electronic media from unauthorized use and distribution. Digital Watermarking is the process of adding a visible or invisible identifier to a digital media like an image, audio, video, or document to protect it from unauthorized use and distribution [3]. The scope of this paper is limited to digital image watermarking only. The watermark that is embedded must be both robust and imperceptible, making it challenging for attackers to detect and capable of withstanding their attempts at attack. There are several techniques to embed a watermark in the host image, but primarily these algorithms are categorized into two major domains: spatial domain techniques and frequency domain techniques.

The spatial domain views an image as a combination of pixels, and these techniques directly work on manipulating the intensity values of the pixels of the original image [4]. Spatial domain techniques are less complex and time-efficient but lack robustness. In transform-domain techniques, the watermark is not directly added to the cover image. First, the cover image is transformed using a transformation function like DFT, DCT, DWT, etc. [5-8]. And then watermarks are inserted into the coefficient of the transformed image. Although the frequency domain techniques are complex and computationally expensive, they yield high performance factors, i.e., good imperceptibility and robustness [9, 49]. Imperceptibility refers to the degree to which the watermark is detectable or noticeable to the human eye, whereas robustness pertains to the watermark's ability to endure various kinds of attacks.

In the past few years, digital picture watermarking techniques have made significant progress, especially in terms of security and robustness. Various techniques now integrate encryption and other security features to strengthen watermark protection [10]. Secure image watermarking techniques have found a diverse range of applications in several industries, such as entertainment, news media, medical, banking, and e-commerce. Having a comprehension of the capabilities and constraints of digital image watermarking methods enables individuals, businesses, and content creators to enhance the safeguarding of their intellectual property. The purpose of

[1] *B.T.Kumaon Institute of Technology Dwarahat,India*
ORCID ID : 0000-0002-7638-3875
[2] *H.N.B Garhwal University Pauri Garhwal, India*
ORCID ID : 0000-0002-5289-9471
Corresponding Author Email: ersgaur1234@gmail.com

this essay is to present a detailed and all-encompassing summary of digital image watermarking, which covers its varieties, features, methods, vulnerabilities, measures for evaluation, and practical implementations; determine the limits of the currently used methods; Examine the current methods that fully satisfy a few of the demands of image watermarking strategies; and elucidate the difficulties that the next generation of researchers will need to overcome.

This paper is structured into several sections, with a literature review appearing in Section II. Digital image Watermarking Background and Structure in Section III Basic requirements and performance evaluation of the digital image watermarking system are described in Section IV. Digital watermarking categories in Section V Classification of watermarking attacks in Section VI. Application of Digital Image Watermarking in Section VII A summary of the numerous kinds of watermarking techniques is provided in Section VIII. Conclusions in Section IX are given.

2. Literature Review

This section will review earlier research on digital image watermarking, including spatial domain-based, frequency-domain-based, and hybrid domains, as well as using optimization methods and cryptography algorithms, which will have served as inspiration for our review study. Larijani et al. [11] provided a scheme for grayscale watermarking using the spatial domain as the space of insertion to take advantage of low complexity and simplicity in the calculation. This method has great fidelity when compared to other methods and is robust in terms of various image processing attacks. Kester et al. [12] introduced a spatial domain watermarking approach on the basis of image features built on formal concept analysis. In this approach, we choose to employ formal concept analysis since altering pixel values might alter the lattice that is created from the image. This approach is very effective for analysing and verifying digital image data. Danti et al. [13] proposed a colour cover image with a colour secret image; a 2-3-3 LSB insertion technique employs secret data with eight bits. The final three bits are placed in the B channel, followed by two bits in the R channel and three bits in the G channel. These bits are inserted into the LSB in a 2-3-3 sequence. Comparing this method to the hash-based 3-3-2 methodology, the MSE and PSNR values are better. Abraham et al. [14] presented a method for colour picture watermarking in the spatial domain that doesn't appreciably reduce image quality or alter the perception of colour. The watermark is included in every image block to provide the highest image quality and highest level of attack resilience, making authentication and/or recovery feasible. Muyco et al. [15] proposed a digital watermarking method using the least significant bit hash algorithm for embedding and extracting. LSB hash code was used to encrypt the original file and to remove the embedded hash code, which led to the creation of an output file that resembled the original one. In this instance, the data extraction tool's embedded watermark is undetectable. Kitanovski et al. [16] offer a blind watermarking access for image authentication; in this scheme, a watermark is produced using the image hash like a key in the low transform component with quantization index modulation to enhance the robustness in opposition to common image processing attacks in addition being fragile to tempering. Chi-Man Pun [17] invented a method using a Gaussian low-pass filter and resistance to JPEG contraction. With this technique, a 512x512-pixel image has 4096 bits of information embedded in it.he twelve indicative DCT coefficients that encrypt the watermark can be selected via adaptive quantization. Patra et al. [18] introduced a Chinese Remainder Theorem (CRT)-based watermarking approach in the DCT orbit that surpasses a CRT method using the spatial domain techniques according to resilience and confidentiality when it comes to resilience against brightness, JPEG compression, and sharpening effects. A semi-blind, robust DCT watermarking method for digital data authorization, integrity confirmation, tamper identification, and safeguarding was proposed by Laouamer et al. [19] using DCT and linear interpolation methods. The visibility and robustness of a watermark can be balanced. Rotation, JPEG compression, noise, and median filtering were among the attacks the system was shown to be extremely resistant against. The scheme can now accurately remove the watermark; this was the primary benefit of the study. Roy et al. [20] introduced a colour watermarking method based on DCT that allows for the insertion of various watermarks for ownership of copyright and affirmation. The system shown enhanced sturdiness and invisibleness and created a greater PSNR value by eliminating blocking artefacts, which are the core problem with block-based DCT techniques (a lack of some data). Vishwakarma et al. [21] develop a grayscale image watermarking approach according to differential evolution and kernel extreme learning machine (DE-KELM) in the DCT, in which the low -transform parameters are chosen in a zig-zag pattern like that the watermarked image appearance is not diminished. Liu et al. [22] introduced an enhanced DCT encipher approach for watermarking, in which the host image is first encrypted using fractal encoding and then encrypted again using DCT. The suggested system became more reliable and efficient thanks to this dual encryption technique. Blossom *et al.* [23] suggested a DCT-based watermarking scheme that offers increased resilience against image processing attacks, including but not limited to JPEG contraction, noise, rotation, and rephrasing. In this particular method, the watermark is inserted within the mid-transform band of the DCT blocks, which holds the low-transform components while discarding the high-frequency sub-band components. The achievement analysis indicates that the watermark is highly resilient. Shih *et al.* [24] presented a combinational

watermarking technique. The host image was divided into two parts; for embedding, the spatial domain technique LSB was applied to one part, and the frequency domain technique DCT was applied to the other part. This was done to increase the capacity and robustness without compromising the imperceptibility of the image. Here authors proposed that using this technique, additional watermark information could be inserted into the cover image. Mistry *et al.* [25] compared spatial domain techniques (like LSB) of digital image watermarking with frequency domain techniques (like DCT and DWT). The author concluded that the transform domain method achieves superior quality of the watermarked image by initially converting the source image into the frequency domain utilizing numerous transformations, such as the Fourier Transform, the discrete cosine transform (DCT), or the discrete wavelet transform (DWT). Zhang [26] presented an overview of digital watermarking and its characteristics. The author also provided a theoretical overview of different digital watermarking algorithms like DCT, LSB, Spread Spectrum, the Text Minitrim algorithm, and the Texture Mapping algorithm. Ching-Yung *et al.* [27] provided a watermarking algorithm in which a watermark is embedded into the 1-D signal of the host image after applying a Fourier transform to the input image. According to the experimental results, the watermark generated through the proposed algorithm is robust against RST distortions such as rotation, scaling, and Translation. Vleeschouwer *et al.* [28] presented a comprehensive overview of perceptual watermarking, emphasizing the importance of creating a watermarking system that is imperceptible to human perception and can maintain robustness despite image and video processing operations. The authors discussed several techniques used to achieve invisibility and also suggested future research directions in the field, emphasizing the need for more advanced watermarking techniques that can address the challenges of copyright protection in the digital age. Celik *et al.* [29] presented a Hierarchical watermarking scheme that offered a significant advantage over other watermarking schemes because it allows for the detection of cropping while still authenticating untampered cropped regions. The authors proposed a new technique based on the public key watermark proposed by Wong *et al.* [30], which eliminated the vulnerabilities against vector quantization counterfeiting attacks. A wavelet-based threshold classification watermarking method for digital pictures was created by Chen et al. [31]. This programme analyses the complexity of a picture to assess its sturdiness and invisibleness. The procedure separates the cover image into a number of blocks, some of which are picked to include the watermark. With the use of the inferred preferred sub-bands, the coefficient of DWT is then categorized due to sub-bands with lower frequencies. The results of several tests revealed that the system was incredibly durable and immune to a number of common dangers. Haribabu et al. [32] suggested a DWT-based effective digital image watermarking method in HIS colour space for copyright protection. In this scheme, the grayscale watermark image is embedded in a 1-level DWT LL sub-band that is segmented into 8X8 blocks and achieves more robustness as compared to the existing scheme. Jia et al. [33] proposed a DWT-based noval colour image watermarking scheme with QR decomposition. In this scheme, 1-level DWT is applied to each component of the colour host image and then segmented into blocks, and then each block is decomposed by QR decomposition for embedding a watermark. This scheme shows that it is more sturdy against familiar image processing onslaugt. Nikita Kashyap *et al.* [34] proposed an image watermarking scheme based on 3-level DWT. The process of embedding a multi-bit watermark involves utilising the alpha blending technique to insert it into the low frequency sub-band of the cover image. 3-level DWT is applied on the host image as well as on the watermark, and embedding is done on the LL3 band. To evaluate the competent of the recommended approach, statistical parameters such as peak signal-to-noise ratio (PSNR) and mean square error (MSE) are employed and used to compare its performance with 1-level and 2-level DWT-based image watermarking techniques. According to the empirical outcomes, the watermark achieve through the suggested algorithm is imperceptible, and the quality of the watermarked image and the recovered image is enhanced. Choudhary *et al.* [35] proposed a watermarking scheme that uses 2-level DWT. First, the host image and the watermark are decomposed into 4 sub-bands, namely LL1, LH1, HL1, and HH1, using 1-level DWT, and furthermore, the LL1 sub-band of both images is decomposed into 4 sub-bands, namely LL2, LH2, HL2, and HH2, by again applying 1-level DWT to the LL1 sub-band. And then the watermark is embedded into the LL2 sub-band of the host image for high robustness and increased imperceptibility. Finally, the performance parameters, i.e., PSNR and NCC, are compared with respect to 1-level DWT, which shows increased performance in 2-level DWT as compared to 1-level DWT. Chang *et al.* [36] proposed an SVD-based digital image watermarking scheme in which both the D and U components were explored for embedding, which provided stronger robustness against different attacks and better image quality. Katti *et al.* [37] presented a definition as well as an algorithm for evaluating the capacity of a watermarking system. According to the authors, capacity is the number of bits transmitted under constraints like the probability of detection, the probability of false alarms, and the MSE between the original image and the watermarked image. Yusof *et al.* [38] proposed a paper containing a detailed overview of the wavelet transform technique. The authors also provided an overall view of digital image watermarking, including its types, techniques, and future trends. A new watermarking evaluation method was introduced by Yang *et al.* [39],

which relied on the masking properties of the human visual system. The suggested technique, referred to as Masking-based Peak Signal to Noise Ratio (MPSNR), was found to outperform other methods in assessing imperceptibility. The outcomes indicated that a stronger masking effect led to a lower level of deterioration in the watermarked image quality. Chunlin *et al.* [40] conducted an analysis of various digital image watermarking attacks. The efficacy of a digital watermarking technology relies significantly on its ability to withstand attacks that aim to eliminate or damage the watermark from the host data. And the researchers provided an in-depth explanation of various attacks that can be employed to compromise a watermarked image. The paper also includes a series of experimental findings demonstrating the impact of these attacks on watermarks generated using different watermarking methods. Poljicak *et al.* [41] proposed a DFT-based watermarking technique that was fast, simple, and robust against different attacks. The authors were mainly focused on the quality evaluation of the watermarking system using the evaluation metric PSNR (Peak Signal to Noise Ratio). The paper proposed that the distortion of the image after embedding depends on many features. Hernandez *et al.* [42] recommended a DFT-based watermarking scheme for medical imaging management. The suggested technique was robust against geometric attacks and signal processing operations. Aslantas *et al.* [43] proposed a DWT-SVD-based image watermarking technique using the PSO optimizer. In their approach, the discrete wavelet transform (DWT) is used to decompose the cover image, and then singular value decomposition (SVD) is used with the high-frequency sub-bands. PSO is used to search for the optimal values of the watermark embedding parameters. The performance of the proposed scheme is evaluated by the peak signal-to-noise ratio (PSNR) and the normalized correlation (NC) coefficient. Xiaoyi *et al.* [44] recomrnded a hybrid image watermarking method depending on DWT-SVD. Initially, the watermark is divided into four parts to guarantee that if it experiences significant harm, it can still be restored by matching the corresponding pixels from each of the four parts. Afterward, a two-level DWT is employed, followed by performing SVD on the HL and LH sub-bands. The goal of the suggested hybrid technique is to merge the benefits of DWT and SVD to improve the performance of watermarking. DWT offers spatial and frequency localization, whereas SVD enhances the resistance against attacks. Tao *et al.* [45] conducted an analysis of different watermarking techniques and evaluated different techniques like SVD and DWT. The major focus of paper was on the robustness of the watermarking system against geometrical distortions. Gorai *et al.* [46] propose a PSO-based approach for grey-level image enhancement. The authors optimize the parameters of a nonlinear mapping function using PSO to enhance the contrast of grey-level images. The attainment of the recommended approach is evaluated using various benchmark images. The results show that the proposed approach provides a significant improvement in contrast enhancement over existing methods. Kuppusamy *et al.* [47] recommended an optimized picture watermarking method based on PSO. The authors use PSO to optimize the embedding strength and evaluate the performance of the scheme by testing its robustness against various attacks. The results show that the proposed scheme provides good robustness against different types of attacks. Sonam Tyagi *et al.* [48] presented a comprehensive overview of digital watermarking techniques for security applications, highlighting their significance in today's digital landscape. The paper discusses a variety of techniques, including spatial domain methods and transform domain methods such as DCT, DWT, and DFT. Furthermore, the author covers the characteristics, applications, types, and potential vulnerabilities of these methods. Anuja Dixit *et al.* [49] proposed a review paper on digital image watermarking techniques wherein the authors gave a detailed description of digital image watermarking, its applications and types, characteristics, and performance factors. The authors also gave a brief overview of the various domains of digital image watermarking, the techniques used in each domain, and a few attacks that can be applied to the watermarked image. Rao *et al.* [50] proposed a DWT-DCT-SVD-based digital image watermarking scheme using PSO. In their approach, the cover image is first decomposed using DWT and DCT to obtain the high-frequency sub-bands. Then, SVD enforced to the high-frequency sub-bands to obtain the singular values. PSO utilized to find the ideal values of the watermark embedding parameters. The performance of the proposed scheme is evaluated by the PSNR, the NC coefficient, and the bit error rate (BER). Thakkar *et al.* [51] proposed a PSO and block-SVD-based watermarking technique for digital images. In their approach, the cover image is first blocks separated so as not to overlap, and then to acquire the singular values, SVD is performed to each block.. PSO is used to search for the optimal values of the watermark embedding parameters. The act of the uggested scheme is evaluated by the PSNR, the NC coefficient, and the robustness against different attacks. Poonam *et al.* [52] suggested a DWT-SVD-based robust digital watermarking method where it is possible to insert a digital watermark within host data using either the spatial or frequency domain. The presented method in this study utilises both the discrete wavelet transform (DWT) and Singular Value Decomposition (SVD) in a hybrid approach to embed a watermark within the sub-bands' singular values of the host image. The proposed technique is able to achieve good imperceptibility and robustness. Gangadhar *et al.* [53] proposed a technique for watermarking that utilises the wavelet domain and incorporates particle swarm optimization (PSO) and singular value decomposition (SVD). In the proposed scheme, PSO is employed to optimize the scaling factor in the watermark embedding

process. Finally, to evaluate the performance of the proposed technique, PSNR and NCC are calculated, which testify to good imperceptibility and robustness. Kumar *et al.* [54] propose a watermarking scheme that uses DWT and PSO for embedding and detecting high-energy coefficient watermark bits in the cover image. The authors evaluate the performance of the scheme by testing its robustness and imperceptibility against different types of attacks. The outcomes depicted that the recommended scheme provides good imperceptibility and robustness. Seif Eddine Naffouti *et al.* [55] proposed a robust watermarking scheme based on DWT-SVD. First, the host image and the watermark are decomposed into 4 sub-bands using 1-level DWT, and then SVD is applied to the high-frequency sub-band HH of both images, thus decomposing them into 3 matrices: U, S, and V. The embedding is performed on the singular diagonal matrix, i.e., S. Finally, the proposed approach is assessed based on the performance metrics of NCC and PSNR, concluding that it fulfils the requirements of imperceptibility and offers robust security against common signal processing operations and attacks. Singh *et al.* [56] proposed a robust and secure digital watermarking method depending on DWT, DCT, and SVD for securing digital content over unsecured social networks. The methods used multiple watermarks embedded in different frequency bands of the host image to enhance security and reduce storage and bandwidth requirements. The use of a back propagation neural network and error-correcting codes further enhanced the robustness of the watermark against distortion and channel noise. The selective encryption of important multimedia data also improved the protect the input and watermarks image. The suggested method attained excellence in achievement in terms of robustness, security, capacity, and perceptible quality. A nonblind watermarking method described by Jane et al. [57] uses the DWT and SVD in conjunction with LU decomposition. The authors suggested combining the widely used transform domain technique (DWT) and the decomposition method (SVD) via LU decomposition to make watermarked images substantially more resistant to some attacks. The suggested algorithm can therefore be thought of as resistant to "filtering," which stands for compression-based assaults, as well as "scaling" and "rotation," which denote geometric attacks, in contrast to existing DWT and SVD watermarking algorithms. Sridhar et al. [58] integrated DCT, DWT, and SVD to improve sturdy and imperceptibility. It was shown that this hybrid technique is unaffected by the filtering JPEG contraction algorithm, salt-and-pepper noise, rotation, cropping, scaling, and translation techniques. For the purpose of defending digital assets in a hybrid environment, another plan by Kumar et al. [59] was presented. The least significant bits and a wavelet transform (DWT and SVD), where the cover picture is separated into sub-bands (LL, HL, HH, and LH) by utilizing the transformation technique in the frequency domain, are used in the strategy to safeguard digital contents while transmitting digital resources in a hybrid context. The watermark is extracted via the previously specified embedding techniques. This hybrid technique offers superior quality and resistance to many assaults, including JPEG compression and Gaussian noise. Another study Abdulrahman et al. [60] used DWT and DCT together to improve the sturdiness of the watermarking methodology. The resilience and imperceptibility of the watermarking approach are both guaranteed by a hybrid approach that combines DWT and SVD. Savakar et al. [61] Pizzolante et al. [62] provided a creative method that works better for integrating watermark images into the image sequences captured by confocal microscopy. This approach offers a decent trade-off between resilience and computational complexity, making it somewhat resistant to the lossy compression onslaught. Zear et al. [63] offer DWT, DCT, and SVD-based multiple watermarking for healthcare applications. This technique employs three watermarks: a doctor's signature and identification code, a medical Lump image watermark, and the patient's diagnosis code data as text watermarks, with the goal of confirming the identity of the user. For improving the robustness and security, author has used a back propagation neural network (BPNN) and Arnold transform in this method. Takor et al. [64] proposed a new hybrid watermarking scheme using Lifting wavelet transform (LWT), discrete cosine transform (DCT), and singular value decomposition (SVD) with PSO. This scheme acquires improved resistance to several assaults. Zhou et al. [65] suggested a highly robust and hybrid watermarking scheme with DWT, SVD, and the all-phase discrete cosine biorthogonal transform (APDCBT). This scheme is block-based (APDCBT) for improving imperceptibility and strong resilience in defending against several image processing threats. Zhang et al. [66] offer a feature-based image watermarking approach using scale-invariant feature transform (SIFT), SVD, and all-phase biorthogonal transform (APBT). This scheme achieved good imperceptibility and high robustness against various attacks. Jamal et al. [67] proposed a new watermarking approach by using the chaotic fractional S-Box Transformation. In this scheme to create the chaotic S-box, a set of nonlinear ordinary differential equations that generate a continuous-time dynamical system that exhibits attractor-like fractal properties is utilised and this algorithm is highly robust against malicious attacks like noise, cropping, and compression. Wang et al. [68] proposed a watermarking scheme based on Haar Wavele for colour images. This scheme has better resistance to attacks such as loss compression and adding noise. Vaishnavi et al. [69] provide colour pictures with Resilient and transparent Image Watermarking using SVD. Two distinct approaches to image watermarking in the RGB colour space are suggested in this work. The input image's blue colour channel elements are implanted with the watermark in the

first technique's grey scale, while the input image's blue colour channel elements are implanted with the watermark in the second way. The watermark is then incorporated into the singular values that were obtained by using SVD on the input image's blue channel, and this method achieved better imperceptibility and was highly robust against various image processing attacks.

3. Digital Image Watermarking Background and Structure

The quick expansion of the internet, multimedia frameworks, and worldwide networks of computers has made it possible for digital material to be quickly disseminated over communication channels at the moment. Digital mage watermarking enables the construction of a platform for e-researchers by protecting digital evidence against unlawful interactions, handling of information, and data storage, possession, replication, modification, and dissemination using tangible transportation mediums.

Since the invention of paper watermarks in 1282, digital watermarking methods have been enhanced by including paper composition, character, and capacity variables. Watermarking is widely utilized to improve security [70]. Digital image watermarking has seen several advancements since its introduction in 1988 as a computerized technique that offers availability, secrecy, and integrity. A watermark (a marker of the owner's legitimacy) is inserted into the host signal using watermarking techniques, and its contents may subsequently be retrieved. A sole bit, a collection of binary information, or an array of source signal bits can all be found in the watermark data, which may or may not be apparent [71]. Digital image watermarking is a technique used to prove the authenticity or ownership of a digital image by embedding a digital watermark, which is usually an imperceptible piece of information, into the host image. It is used to verify the integrity of the image and prevent unauthorized use or distribution of the image.

A watermarking process is usually divided into two phases: watermark embedding and watermark extraction, as shown in Figs. 1 and Fig. 2. In digital watermarking, a low-energy signal is imperceptibly embedded into another digital signal [72, 73]. The low-energy signal is called a "watermark, and it shows some metadata, such as security or copy-right information, of the original signal. The original signal in which the watermark is embedded is referred to as the cover signal, since it covers the watermark. The cover signal is typically a stable image, audio clip, video sequence, or text document in digital format.

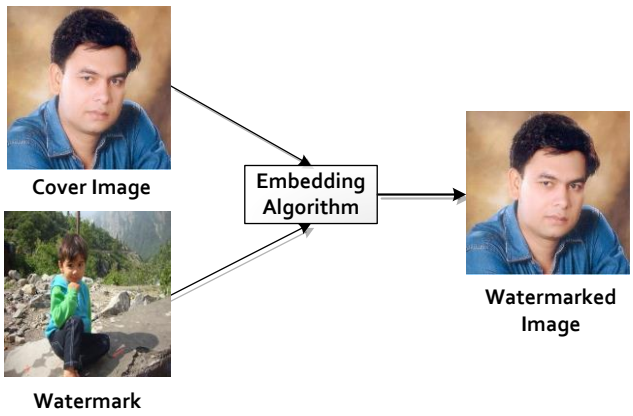

Fig.1. Watermark Embedding

Mathematically C_O , W and C_W are original, watermark and watermarked image signal then watermarked signal C_W is given by equation [1]

$$C_W = C_O + f(C_O, W) \quad (1)$$

Watermarked image (invisible watermarking) visually identical to the original signal, where $'f'$ is an arbitrary function [76]. The digital watermarking system basically consists of a watermark embedding algorithm and a watermark detection algorithm as depicted in Fig.3 In this Fig.3 there are three blocks: one is embedding block (watermark signal, watermark key), communication channel block (attacks) and watermark detector block. The watermark embedding algorithm inserts a watermark signal into the cover digital signal and the watermark detection algorithm identifies the existence of watermark signal.

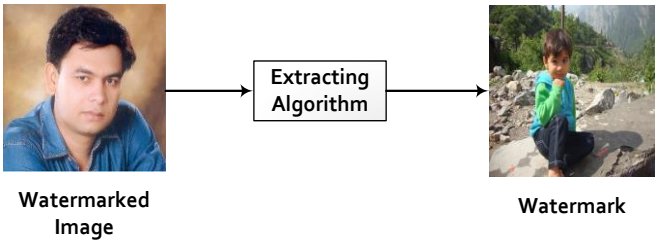

Fig.2. Watermark Extraction

The insertion and extraction of watermarks can also make use of a component known as a watermark key. Every watermark message has a specific watermark key, meaning that they can only communicate with one another. Only authorised individuals have access to the watermark key, which guarantees that only authorised individuals may remove the watermark. Digital watermarking solutions should be robust to both noise and vulnerability assaults since the communication channel might be noisy and hostile (i.e., for security attacks) [71].

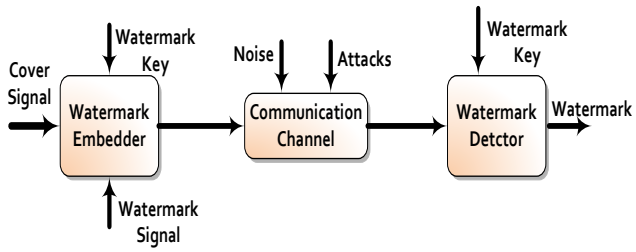

Fig.3. Digital Watermarking System

4. Basic Requirement and Performance Evaluation of Digital Image Watermarking System

The basic requirements of watermarking are robustness, imperceptibility, capacity, security, data payload, and computational cost. However, a watermarking scheme may not satisfy all of these requirements. The watermarking system is designed to fulfil the desired properties according to the type of application. In the case of temper detection, imperceptibility is not an issue, whereas for copyright protection, it is one of the most important issues. The effect of one property may affect another property. For example, if robustness is increased, it decreases imperceptibility. Hence, there is a tradeoff between these requirements, according to the application. Some of the basic requirements are described in this section [71, 74, and 75]. The criteria for methods for watermarking are shown in Fig. 4. These specifications assess the effectiveness of watermarking technologies based on their use.

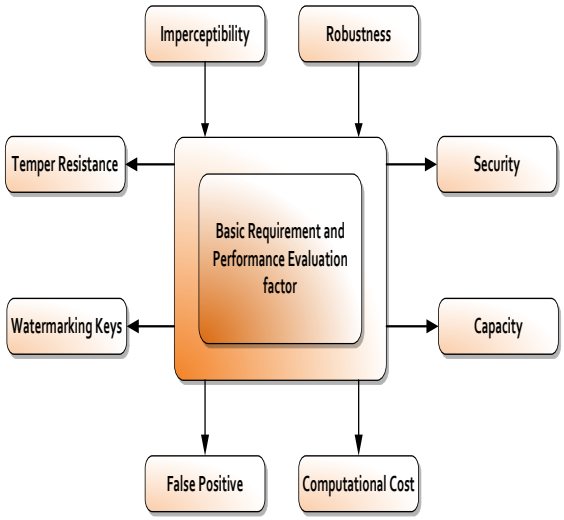

Fig.4. Basic Requirement and Performance Evaluation Factor

1.1. Imperceptibility Analysis

The imperceptibility measures perceptual transparency between the watermarked image and the original image, i.e., there is a negligible difference between the watermarked image and the cover image signal after embedding the watermark image [76]. The watermark data is embedded into the cover signal such that its presence is not visible or perceptible by the user. Theoretically, the watermark should be invisible to the human eye. Although visible watermarks are more robust, for most applications, they are advantageous, for example, for ownership or copyright contents [3]. The imperceptibility of the watermark is the most important factor for analysing the watermarking algorithm. There are many metrics that can be used to analyses imperceptibility; however, the most widely used metrics are given bellow.

1.1.1. Mean Square Error (MSE)

MSE stands for Mean Square Error, which measures the difference between the original image and the watermarked image.

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - D(i,j)] \quad (2)$$

where:

- n × m: the size of the image
- $I(i,j)$: Original image i ,j coordinate pixel value
- $D(i,j)$: Watermarked Image i,j coordinate pixel value

The MSE value ranges from 0 to infinity, where a lower MSE value indicates a smaller difference between the two images, and hence a higher quality of the processed image MSE can be calculated by using the equation (2).

1.1.2. Peak Signal –to –Noise Ratio (PSNR)

PSNR stands for Peak Signal-to-Noise Ratio, which is a commonly used metric in digital image watermarking to measure the aspect of an image after applying a watermark. The PSNR formula is as follows:

$$\text{PSNR} = \frac{10 \log_{10}[\max(\text{I(i,j)})^2]}{\text{MSE}} \quad (3)$$

where:

- max I is the maximum possible pixel value of the image (e.g., 255 for an 8-bit grayscale image).
- MSE is the mean squared error between the original image and the watermarked image.

PSNR is expressed in decibels (dB) and represents the ratio between the maximum pixel value and the noise in the image. A higher PSNR value indicates a better-quality image with less noise and distortion, which is desirable in digital image watermarking

1.2. Robustness Analysis

A digital watermark is durable if it can withstand a specific group of copyright-related modifications (attacks). The resilience criteria focus on two issues: (i) if the watermark persists after being modified in the digital data, and (ii) whether the watermark detector can detect it. The watermark's robustness accounts for the capability of the watermark to survive signal manipulations like malicious attacks and common signal processing operations. Therefore, it is essential to create a watermarking system that can withstand these procedures [68]. A watermark must be strong enough to withstand all assaults and signal processing procedures in order to be used in watermarking applications. A watermark only has to endure assaults and signal processing procedures that are likely to happen while the watermarked signal is present in the communication channel. In the case of fragile watermarking, robustness is completely irrelevant; the watermark contents are embedded in such a way that they get disturbed due to any possible attack. So, in these schemes, higher robustness is not required. The robustness of the watermark is the most important factor for analysing the watermarking algorithm. There are many metrics that can be used for robustness analyses; however, the most widely used evaluation metrics are given as:

4.2.1 Normalized Correlation Coefficient (NCC)

NCC stands for Normalized Correlation Coefficient, which is

a metric used to measure the equivalently among two images. It is commonly used in digital image watermarking to evaluate the efficiency of a watermarking algorithm. For finding the NCC values equation (4) is given:

$$\mathrm{NCC} = \frac{\sum_{i}^{n}\sum_{j}^{m}\left(W_{ij}^{O} \times W_{ij}^{E}\right)}{n \times m} \quad (4)$$

where:

W_{ij}^{O} is the pixel value at location (i, j) in the original watermark image

W_{ij}^{E} is the pixel value at location (i,j) in the extracted watermark image n and m are the dimensions of the watermark image (i.e., the number of rows and columns)

The NCC value ranges from -1 to 1, where a value of 1 indicates a perfect match between the two images, 0 indicates no correlation, and -1 indicates a perfect negative correlation. A higher NCC value indicates a better correlation between the original watermark and extracted watermark image, indicating that the watermark is more robust.

4.2.2 Bit Error Rate (BER)

BER stands for Bit Error Rate, which is a measure of the number of bit errors in a digital signal, typically expressed as a ratio of the number of errors to the total number of bits transmitted. In the context of digital image watermarking, BER can be used to calculate the achiement of a watermarking technique by measuring the accuracy of watermark detection and extraction.

The formula for BER is:

$$\mathrm{BER} = \frac{\text{Number of Bits in Error}}{\text{Total Number of Bits transfered}} \quad (5)$$

In digital image watermarking, the "number of bits in error" refers to the number of bits in the extracted watermark that do not match the original watermark, while the "total number of bits transmitted" mention the total number of bits that were embedded in the original image.A lower BER indicates a more accurate watermark extraction, while a higher BER indicates a higher rate of errors in the extracted watermark. A BER of 0 indicates perfect extraction, while a BER of 1 indicates that all the extracted bits are incorrect**.**

4.2.3 Accuracy Ratio (AR)

AR stands for accuracy ratio which is used to assess how well the extracted and hidden watermarks match. It displays the relationship between the accurate bits and the original watermark bit

$$\mathrm{AR} = \frac{\mathrm{CB}}{\mathrm{NB}} \quad (6)$$

Where:

CB is the number of correct bits NB is the total number of bits

Capacity

It is the quantity of number of bits that may be incorporated into the given cover image. In case of audio watermarking, the capacity is defined by the number of bits embedded into the signal per second and for video watermarking, it is the number of bit embedded per frame without disturbing the quality of the signal.

Secutity

The security of watermark refers to protect the watermark content against malicious attacks. Depending on the application, there could be different watermark security requirements. It is not always necessary that each robust watermarking algorithm is secure. Secure watermarking schemes protect the watermark content from intentional or unauthorized attacks like removal of watermark, fake watermark embedding, modification or detection [77].

5. Fragility

Main goal of the weak watermark is data identification. This is the resilience criterion's opposite procedure. The watermarks may be made to survive a range of permissible watermark variations caused by alterations in the media content.

6. Computational Cost

The computational cost generally implies that the embedding and extraction time of the watermark contents. Complex watermarking methods have higher computational cost whereas less complex algorithms have lower computational cost. It is to be measured by execution time of embedding and extracting watermarking algorithms.

7. False Positive Rate

The feature employed to detect watermarks in images without watermarks is called the false positive rate. This issue arises when the retrieved watermark and the inserted watermark are dissimilar [78]. A variety of plans have been used to conduct the test. For copy control and ownership, this attribute has mostly been employed. The following equation [79] describes the false positive rate (FPR), which is determined if a watermark picture W has dimension l and the recovered watermark is W^E.

$$False\ Positive\ rate(FPR) = \frac{I^H}{I} \quad (7)$$

Where I^H distorted distance of watermark W and W^E.

8. Watermark Key

The watermark key is a secret key that controls some embedding function settings. The embedding domain, embedding direction, and/or subset of image coefficients are all included in this key. Estimating and mapping the watermark key is crucial since it impacts the system's degree of protection for watermarking depends on a number of factors, including the encoded message and watermarked picture [80]. In order to assure security, a hidden key is required for the inserting and extraction procedure. Private, detection, and public keys are all included in the secret key. A court of law will recognize the detection key, the user has access to the private key, and the general public can extract the public key [81].

9. Tamper Resistance

The watermarking system's ability to detect tampering can be utilized to confirm authenticity. The picture is altered whenever the watermark data is altered. Therefore, the system assesses whether or not the watermark data has been altered by verifying integrity [82].

10. Reversibility

Reversibility ensures accurate reconstruction of the host picture and the extraction of the watermark. For medical imaging, the rebuilt picture is utilized for diagnosis while the changed image serves as the host image [83].

11. Trade-Off Between Performance Factor

Digital image watermarking is evaluated based on three primary factors: imperceptibility, robustness, and capacity. However, these factors must be balanced against one another, and any improvement in one factor may negatively impact the others. When attempting to increase imperceptibility, the watermark's capacity to carry additional information may be limited, as changes to the image become more significant with greater amounts of information. Similarly, increasing a watermark's robustness may require making it more visible, which can detract from its imperceptibility. Increasing the watermark's capacity can also reduce imperceptibility, as the necessary changes to the image become more noticeable with larger amounts of information.

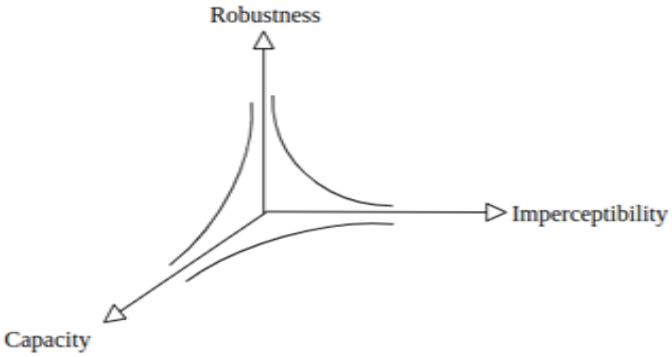

Fig.5. Trade-off between imperceptibility, robustness, and capacity.

Achieving great durability, capacity, and concealment in digital image watermarking requires a delicate trade-off between these factors. High imperceptibility may come at the expense of capacity and robustness, whereas high capacity may result in lower imperceptibility and robustness. Ultimately, the optimal balance between these factors will depend on the specific application and desired level of security. Fig. 5 shows the Trade-off between imperceptibility, robustness, capacity and Table.1 depicted the satisfies the several requirements between various approaches of digital image watermarking.

Table 2. Approaches that concurrently satisfy several requirements

Used Method	Factors	Results	Applications
Spatial Domain Method[63]	Computational Complexity and Robustness	Improve Robustness and Security	Safeguard for Microscopic Image

DWT+DCTand SVD [64]	Imperceptibility, Robustness, Capacity and Security	Improve the Visual Quality	Medical Images
PSO+Block SVD [51]	Imperceptibility, Robustness	Improve the Robustness	Authencity, Copyright Protection
Hybrid frequency Domain + PSO [65]	Robustness, Imperceptibility	Perform better than previous method	Image Authentication
DWT+SVD and APDCBT based Techniques [66]	Imperceptibility, Robustness	Outperform previously existence method	Copyright Protection
Feature Based Method using SVD and APBT [67]	Robustness, Imperceptibility	Improve the Robustness and Imperceptibility	Image Authentication and Copyright Protection

12. Types Of Digital Watermarking

The type of working domain, type of documents, human perceptibility, and type of application all affect the watermarking methods used on digital images. This section provides an overview of all available digital image watermarking methods, which are shown in Fig. 6.

Spatial domain watermarking is a type of digital watermarking technique that operates directly on the pixels of an image or video in its spatial domain. In this technique, the watermark is embedded into the host image or video by modifying the values of selected pixels or groups of pixels [84]. The simplest form of spatial domain watermarking is called "overlay watermarking," where the watermark is simply overlaid onto the host image or video. However, this type of watermarking is easily removable and does not provide sufficient protection against piracy or unauthorized distribution. Spatial domain watermarking has several advantages, such as simplicity, low complexity, improved efficiency, faster execution, low computational cost, and the ability to directly visualise the watermark [85]. However, it can be vulnerable to attacks such as image cropping, resizing, and filtering. Spatial domain watermarking techniques use several techniques, including LSB (Least Significant Bit) and ISB (Intermediate Significant Bit). In this domain, watermark bits are inserted into the image's pixel values, usually in the least significant bits. In this domain Watermark bits are inserted into the image's pixel values, usually in the least significant bits. The spatial domain method is often fast and simple and can be applied to a variety of multimedia formats, making it popular for many applications such as copyright protection and content authentication. However, they are typically less robust against attacks compared to frequency-domain techniques [4, 29].

14.1 Spatial Domain Based:

The watermark is then converted to binary form, and its length should match the number of pixels selected for modification. The least significant bit of each selected pixel is then replaced

with the corresponding bit of the binary watermark [9]. While the LSB technique is simple and provides high imperceptibility, it is vulnerable to various attacks such as image compression or cropping. As a result, more advanced watermarking techniques such as spread spectrum or frequency domain watermarking may be employed for applications requiring greater security and robustness [87]

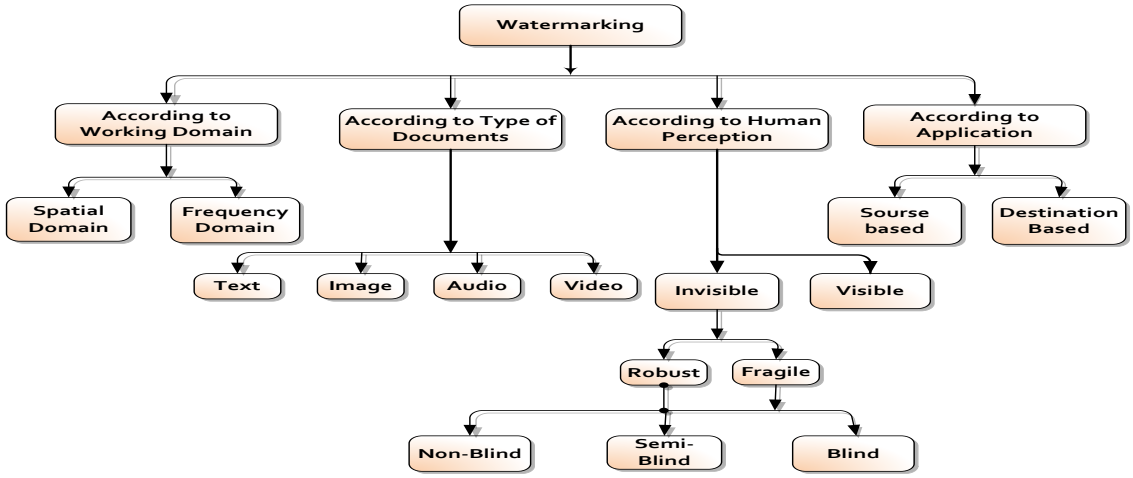

Fig.6. Types of Digital Watermarking System

1.2.1. Least Significant Bit (LSB)

LSB, or Least Significant Bit, is a usually used method in digital image watermarking that affect change the least significant bits of certain pixels in an image with the bits of a watermark. This is carried out in a manner that reduces any distortion to the original image while hiding the watermark [86]. The technique involves selecting pixels in the image that will be modified, typically in areas with low contrast or where small distortions will be difficult to detect.

1.2.2. Intermediate Significant Bits (ISB)

LSB is the most prevalent spatial domain technique, but LSB does not ensure robustness; for this reason, ISB is developed to improve the robustness as well as imperceptibility quality of the watermarking system [88]. ISB (Intermediate Significant Bits) is a digital image watermarking technique that involves replacing the middle bits of selected pixels in an image with the bits of a watermark. This method provides a trade-off between the robustness and the imperceptibility of the watermark [89]. ISB watermarking is more robust than LSB, as it is less affected by image compression or cropping. However, it may be less imperceptible than LSB, as it can introduce noticeable distortions in the image. Additionally, ISB may not be suitable for applications that require high levels of security and robustness, such as digital forensics or copyright protection.

1.3. Frequency Domain Based:

Techniques used for spatial domain watermarking are too brittle and susceptible to manipulation. Compared to frequency-domain algorithms, these methods are significantly less resistant to diverse kinds of assaults. Because of these shortcomings, researchers are concentrating on developing transform-domain watermarking methods, which more successfully conceal data in a signal's transform space than in its time domain. Frequency domain watermarking is a type of digital watermarking technique that operates in the frequency domain of an image or video. The frequency domain refers to the representation of the image or video in terms of its frequency components, obtained by performing a mathematical transformation such as the Fourier transform or wavelet transform. In frequency domain watermarking, the watermark is embedded into the host image or video by modifying the coefficients of the frequency components. The most common technique used in frequency domain watermarking is called "discrete cosine transform (DCT) watermarking", where the watermark is embedded into the DCT coefficients of the host image or video. Another technique is called "wavelet transform watermarking", where the watermark is embedded into the wavelet coefficients of the host image or video.

Frequency-domain watermarking has several advantages over spatial-domain watermarking, such as increased the ability to withstand image processing procedures including scaling, filtering, and cropping. Another benefit of frequency-domain watermarking is that it can embed the watermark more deeply. The watermark as compared to spatial-domain watermarking.

However, frequency-domain watermarking is computationally more intensive and may require more sophisticated algorithms to embed and extract the watermark. Also, the watermark may not be directly visible in the frequency domain, making it difficult to assess the quality of the watermarking process.

Frequency domain watermarking techniques include techniques like discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD). They are commonly used in applications such as telecast monitoring and copyright protection. Watermark embedding and extracting procedure shown in Fig. 7.

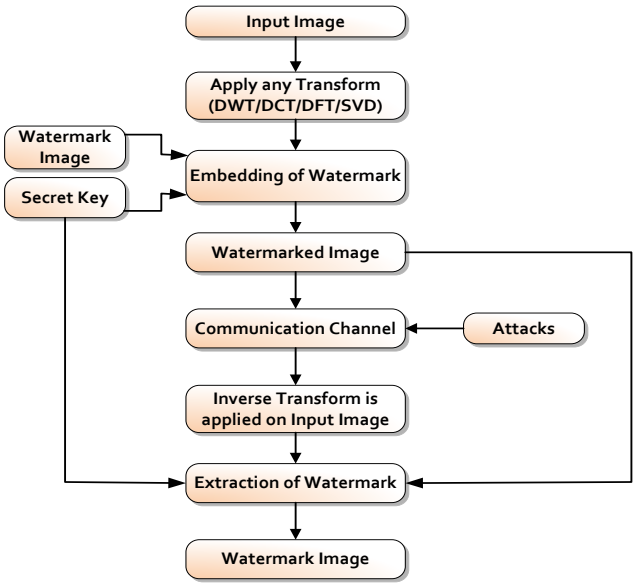

Fig.7. Watermark embedding and extraction in the Frequency domain

1.3.1. Discrete Cosine Transform (DCT)

Discrete cosine transform (DCT) is one of the most popular and fast transform methods for transforming the signal into basic frequency components and denotes an image as a sum of sinusoidal and fluctuating frequencies. It is widely used for image compression because it has high energy packing capabilities and the ability to correlate the image data and then encode the transform coefficient without losing compression efficiency [90]. The 2-D DCT is one of the famous transform methods used for digital image watermarking.

The Mathematical expression for 2-D discrete Cosine Transform of image block of size $N \times N$ is defined as:

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

Where $u,v = 0,1,2,3 \ldots\ldots N-1, f(x,y)$ is the pixel value in the spatial domain. $F(u,v)$ is the pixel value in the transform domain called transform coefficient.

2-D inverse cosine transform (IDCT) defined as:

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \alpha(u)\alpha(v)F(u,v)\left[\frac{\pi(2x+1)u}{2N}\right] cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (9)$$

Where $0 \le x,y \le N-1$ in both the equation $\alpha(u) and \alpha(v)$

$$\alpha(u)\alpha(v) = \begin{cases} \sqrt{\frac{1}{N}} & u,v = 0 \\ \sqrt{\frac{2}{N}} & u,v = 1\ upto\ N-1 \end{cases} \quad (10)$$

$$\alpha(0,0) = \frac{1}{N \times N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} f(x,y) \quad (11)$$

The first transform coefficient is the average value of the block of an image whereas maximum energy of the image lies in the low-frequency coefficients rather than middle and high frequency coefficients. Low frequency band contains most visual information, called DC component of the image and rest are AC components of the image. On methods for digital picture watermarking in the DCT field, several studies have previously been conducted. Among them, block-by block DCT image watermarking operates by first segmenting the cover image into distinct image blocks, after which the DCT transform is applied to the image.

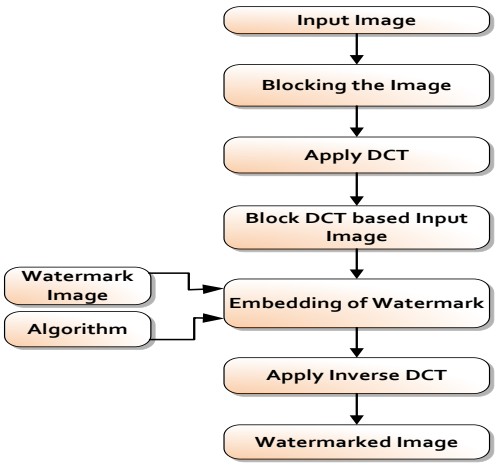

Fig.8. Watermark embedding in a block-based DCT domain.

The watermarked image is then created using the inverse discrete cosine transform (IDCT). Fig. 8 is the best representation of the above-discussed DCT techniques for embedding watermarks and the watermark removal may be done in reverse process. We may infer from literature survey experiments that when utilising embedding in the DCT domain, image watermarking is resilient to the majority of assaults. It is, nevertheless, prone to scaling and cropping.

4.3.2. Discrete Wavelet Transform (DWT)

DWT (Discrete Wavelet Transform) is a widely used technique in digital image watermarking. It involves transforming an image into its frequency domain using the wavelet transform and then embedding a watermark in the frequency sub-bands and improved robustness, security. It is a mathematical tool to decompose a signal in to wavelets instead of frequencies. The wavelets are sampled discretely in DWT. One benefit of DWT over Fourier transform (ie.DCT) is ability to resolve temporal information, this increase the study appeal of DWT by collecting a variety of information such as location, time, and frequency [91,92]. The wavelet transform is helpful for signal noise reduction, image compression, and digital signal processing. The usage of a collection of basis function (as wavelets) that provide localization in the frequency domain is the fundamental concept behind a wavelet transform.

The DWT of a indicate $x[n]$ is describe by the following equations:

$$W_\phi(j_o, k) = \frac{1}{\sqrt{M}}\sum_x f(x)\phi_{j_o,k}(x) \quad (12)$$

$$W_\psi(j, k) = \frac{1}{\sqrt{M}}\sum_k f(x)\psi_{j,k}(x) \quad (13)$$

For, $j \ge j_o$ and the Inverse DWT (IDWT) is defined as:

$$f(x) = \frac{1}{\sqrt{M}}\sum_k W_\phi(j_o, k)\phi_{j_o,k}(x) + \frac{1}{\sqrt{M}}\sum_{j=j_o}^{\infty}\sum_k W_\psi(j, k)\psi_{j,k}(x) \quad (14)$$

Where:

$f(x)$, $\phi_{j_o,k}(x)$ and $\psi_{j,k}(x)$ are functions of the discrete variable x = 0,1, 2,,M−1.

In order to create watermarked image, the system first applies the DWT, insert the watermark into the source image using an algorithm, and then uses the reverse DWT for extracting the watermark image. The entire procedure shown in the Fig. 10.

DWT is widely use in applications that requires high level of security and robustness such as forensic copyright protection, and image authentication.

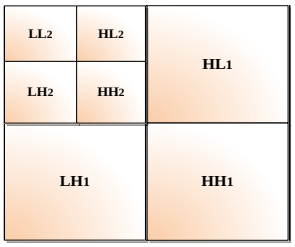

Fig.9. Two-level discrete wavelet decomposition.

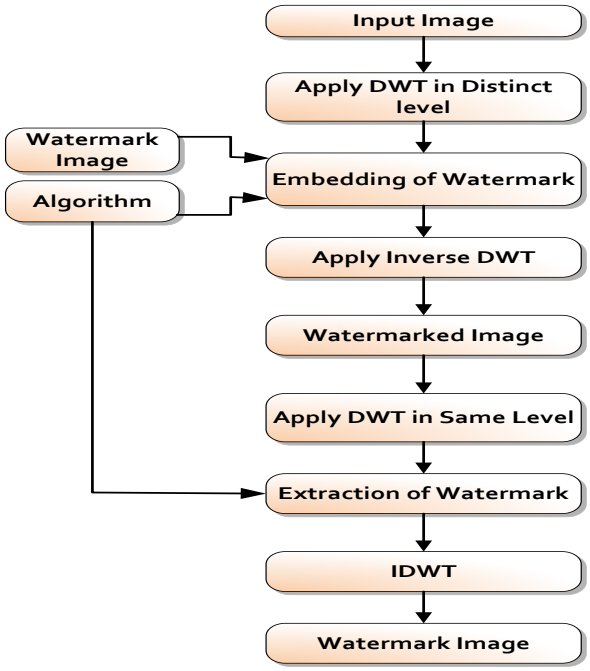

Fig.10. Block Diagram of embedding and extraction in a Discrete Wavelet Transform (DWT) domain.

Using DWT, the host image is divided into 4 sub-bands LL, LH, HL, HH according to frequency which is shown in the Fig. 9. From the study of literature survey we can say that watermarking where DWT is used having greater resistance to the edition of noise, image compression, and filtering etc.

14.2.3. Singular Value Decompositon (SVD)

Singular Value Decomposition is a linear algebra transform used to factorize or decompose real or complex matrix into its three constituents, a left singular matrix $'U'$ a diagonal matrix of its singular values $'S'$ and a right singular matrix $'V'$. The left singular matrix is an orthogonal matrix which represents the relationship between the columns of the original matrix. The diagonal matrix S contains the singular values of the original matrix, arranged in descending order along its diagonal. The columns of $'U'$ form an orthonormal basis for the columns space of the original matrix. These singular values represent the relative importance of the different patterns or features in the original matrix. The larger the singular value, the more important the corresponding pattern or feature is. The right singular matrix $'V'$ is also an orthogonal matrix which represents the relationship between the rows of the original matrix. The columns of $'V'$ form an orthonormal space for the row space of the original matrix.

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

The process of reconstructing the original matrix $'A'$ is achieved by multiplying the matrices U, V and S. This procedure is commonly referred to as the inverse SVD.

$$A \leftarrow USV^T \quad (5)$$

Singular Value Decomposition (SVD) can be interpreted as a matrix transformation procedure [51]. Overall, the resultant matrices of SVD tells us about the relationships and patterns within the original matrix, allowing us to analyze and modify data in various ways. SVD is a powerful mathematical tool in the fields like image processing, data analysis, machine learning. In image processing, SVD decomposition is used for various purposes like image compression by selecting only the significant singular values and disregarding the rest, image enhancement by modifying the singular values of the image or watermarking.

Singular value decomposition is a widely used technique used in digital image watermarking which decomposes an image into its constituent parts, including its singular values. In digital image watermarking, by modifying the singular values in a way that is unseeable by human eye, a watermark can be inserted into the image, which can be later extracted from the watermarked image. This technique is very efficient in ensuring authenticity and integrity of digital images. Hence SVD is used in fields like copyright protection and digital forensics. One of the appealing mathematical aspects of SVD is that minor modifications in singular values have no effect on how the input image appears to the eye. This property drives the watermark embedding process to increase transparency and resilience. [93].

13. Types of Document:

A watermarking method called document-based image watermarking embeds the watermark directly into the text of the document rather than onto the image itself. With this method, the watermark will always be visible, regardless of how the image is cropped, scaled, or removed from the page.

1.4. Text:

In this technique, a hidden message or information, usually in form of text is embedded into a digital document or an image. A text image in watermarking is a watermark that is made up of text or letters rather than visual components like logos, pictures, or patterns. A popular method for incorporating information into digital photographs that is not immediately visible but may be removed or validated as needed is text watermarking. Text watermarks are frequently employed for a number of functions, such as data authentication, ownership identification, and copyright protection.

1.5. Image:

In this technique, hidden message in form of image is embedded into host image. An image watermark is a sort of watermark used in watermarking that is included into a digital image to denote ownership, copyright information, or to prevent unauthorised use of the image. The image that is used as a watermark is typically a logo, design, or pattern that is layered on top of the primary picture and blended in such that it blends in without being overtly noticeable.

1.6. Audio:

In this technique, hidden message is embedded into audio signal in such a way that it is imperceptible to human ears. Music, speech, or any other audio content can be enhanced with additional data or information using a process called audio watermarking. The original audio is not greatly harmed by the encoded data, which is undetectable to the human ear. Audio watermarking is primarily used to protect copyright, authenticate material, and trace intellectual property.

1.7. Video:

In this technique, hidden message is embedded into video signal in such a way that it is imperceptible to human eyes. Using a method called video watermarking, extra information or data may be added to video footage for a number of reasons, including copyright protection, content authentication, ownership identification, and intellectual property tracking. Video watermarking, like picture and audio watermarking, strives to make the encoded information undetectable to viewers while staying secure from possible threats and typical video processing procedures.

14. Perception Based:

Perceptual-based image watermarking is a method for incorporating digital watermarks into images while taking into consideration the properties of the human visual system (HVS). In order to retain the watermark's resistance to different image processing techniques and assaults, it must be rendered invisible or undetectable to the human eye.

1.8. Invisible:

Invisible watermarking is a type of digital watermarking where the embedded watermark is imperceptible to the human eye or ear while still being detectable by an appropriate decoder or detector. It is used for various purposes, such as copyright protection, content authentication, and data hiding. Invisible watermarking techniques often exploit the limitations of human perception to make the watermark imperceptible, such as adding the watermark in the high-frequency regions of the signal or using a perceptual model to adjust the embedding strength based on the sensitivity of the human visual system. It can further be classified into two categories:

1.8.1. Robust:

In this technique, the digital watermarking system is specifically designed in such a way that it is resistant against various kinds of attacks and modifications that digital documents can undergo. In this approach, the watermark is integrated in a manner that it becomes not easy to change or delete, even if the document undergoes processes such as compression, cropping, or scaling. The primary application of robust watermarking is in scenarios where the content needs protection against unauthorized usage or distribution, like in digital rights management (DRM) systems or copyright protection for digital media. The efficacy of the watermarking technique can be assessed by its ability to remain detectable even after different types of attacks, such as lossy compression, geometric distortions, and image cropping. It is divided into three categories.

1.8.1.1. Non-blind:

In this technique, the embedding of the watermark ensures that it is impossible to extract the watermark without the original content. This approach is also referred to as "open watermarking" since the original content is required during the watermarking process. Non-blind watermarking techniques are widely used in applications where high levels of security and authentication are required, such as digital forensics, copyright protection, and anti-counterfeiting measures. Spread spectrum, quantization index modulation (QIM), and patchwork watermarking are a few examples of non-blind watermarking techniques.

16.1.1.2. Semi-blind:

In this technique, a watermark is inserted according to the principle that it is impossible to extract the watermark

without the original content; only some partial recovery of the watermark can happen without requiring the original content. Semi-blind watermarking techniques aim to strike a balance between the blind and non-blind watermarking approaches by providing some recovery of the watermark even when the original content is not entirely available. This technique is typically employed in applications that require a moderate level of security and authentication, such as medical imaging and document authentication. Some examples of semi-blind watermarking techniques include the quantization index modulation-based method, adaptive embedding, and the zero-watermarking technique.

1.8.1.2. Blind:

This approach allows for the extraction of the watermark even when the original material is not there. In other words, the watermark on the media may be removed without having to access the original material. It is also known as "closed watermarking" because it does not require access to the original content during the embedding process. Blind watermarking techniques are often used for applications that require high levels of security and authentication, such as in military and government communications, as well as in copyright protection for digital media. Examples of blind watermarking techniques include spread spectrum, quantization index modulation (QIM), and integer wavelet transform-based methods.

1.8.2. Fragile:

In this technique, watermarking system are created in such a way that they can identify any unauthorized modification or tampering of a digital media, such as images, audio, video, or documents. This technique involves embedding a watermark that is highly sensitive to any alterations made to the media, allowing even the slightest changes to be detected. Fragile watermarking is employed in situations where the authenticity and integrity of the content are critical, such as in medical imaging, forensic analysis, and legal documents. Examples of fragile watermarking techniques include checksum-based methods, cryptographic hashing, and digital signature-based techniques. Unlike robust watermarking, which is designed to withstand various types of attacks and modifications, fragile watermarking is intended to detect any alteration to the media.

1.9. Visible:

In this technique, watermark is added as overlay over the digital media, such as images, audio, video, or documents, to indicate ownership, copyright, or other information. The visible watermark is designed to be easily recognizable and distinguishable from the underlying content, and it is typically added to discourage unauthorized use or distribution of the media by making it clear that it is protected by a copyright or other intellectual property rights. The visible watermarking technique is widely used in industries such as photography, music, and film, as well as in the publishing and advertising sectors.

15. According to Application Domain:

According to application point of view, the watermarking scheme can have divided into two categories one is source based and other is destination based watermarking. In the source based watermarking all the copies of the cover image are watermarked with a unique watermark and used for ownership identification or authentication. The unique watermark identifies the owner of the content. In the destination based watermarking, the watermarks are embedded uniquely to every copy.

1.10. Source Based:

The method of embedding a watermark into an image during its generation or rendering is referred to as source-based image watermarking, also known as model-based watermarking. The watermark is inserted based on the features of the visual generating process or the source of the image, as opposed to directly altering the image. This method is very helpful when the original image is unavailable and it is difficult to change the pixel values directly.

1.11. Destination Based:

Embedding a watermark into an image after it has undergone specific transformations or processing, such as compression or encryption, is known as destination-based image watermarking, also known as receiver-based watermarking or post-compression watermarking. Destination-based watermarking adds the watermark after the picture has reached its intended receiver or destination, in contrast to conventional watermarking techniques that embed the watermark into the original image.

16. Classification of Watermarking Attacks

An assault, as used in the context of watermarking, is any operation that might make it more difficult to identify the watermark or communicate the information it conveys. Attacked data is the phrase used for the processed watermarked data. Robustness is a crucial component of all watermarking strategies. These assaults can remove or desynchronize watermark data while leaving the image's appearance intact. The outlook quality and robustness of attacked data can be measured by finding the peak signal to noise ratio (PSNR) and normalized correlation coefficient (NCC) [85]. The attacks are broadly classified into four categories as removal attacks, geometric attacks, cryptography attacks and protocol attacks which is illustrated in the Fig. 11.

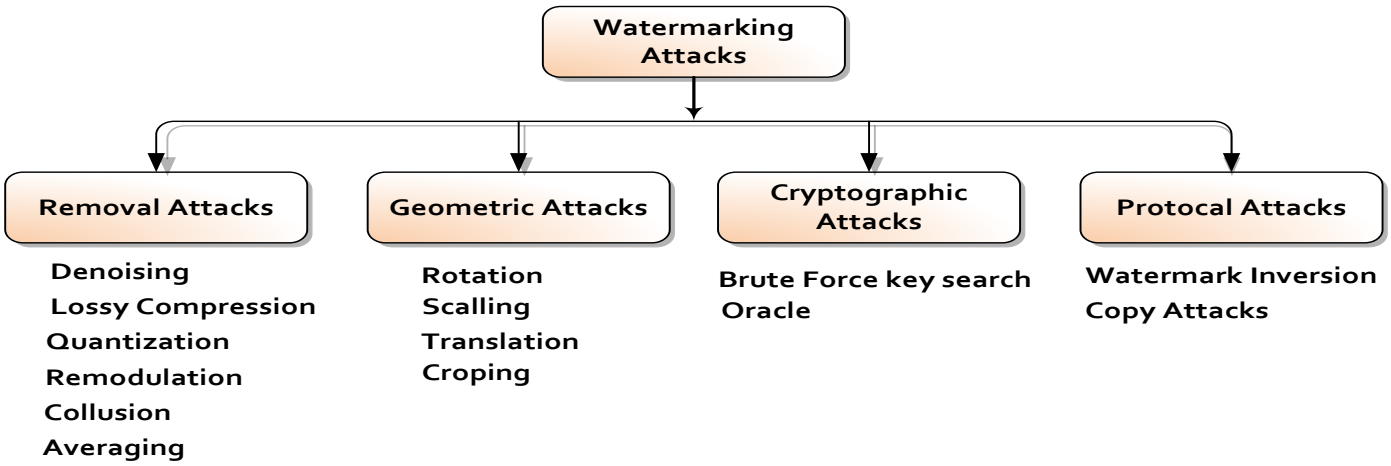

Fig.11. Classification of Watermarking Attacks.

1.12. Removal Attacks:

Removal attacks are those attacks that attempt to analyze the watermarked data, estimate the watermark or the host data, separate the watermarked data into host data and watermark, and discard only the watermark i.e. complete removal of the

watermark from cover data. The category of these attacks is remodulation, quantization, denoising, lossy compression and collusion attacks. The concept behind denoising is that a watermark may be viewed as statistical noise. As a result, it may be inferred from the copy of watermarked data that is readily available. Lossy compression has the same effect as denoising. Remodulation assault makes a watermark prediction by subtracting the median filtered version of the watermarked

image from the original watermarked image. Collusion attacks are applicable when many copies of given data set, each signed copy with different watermark, can be obtained by an attacker.

1.13. Geometric Attacks:

Geometric attacks distorted the watermarked data through spatial and temporal alteration. The assaults often cause the watermark detector to go out of sync with the inserted data. After perfect synchronization the detector can recover the embedded watermark data information. The categories of these attacks are rotation, scaling, change the aspect ratio, translation, shearing and cropping etc.

1.14. Cryotography Attacks:

In order to erase the inserted watermark data or to insert deceptive watermarks, cryptographic assaults try to break the safety mechanisms used in watermarking systems. The brute-force search for implanted secret information is one such method. The so-called Oracle assault, which may be used to produce an unwatermarked signal while a watermark-detecting device is accessible, is another attack in this category. Practically, these assaults can only be used in limited circumstances due to their high processing complexity.

1.15. Protocol Attacks:

The idea of invertible watermarks serves as the foundation for the protocol attack [94]. Inversion is a technique where the attacker asserts ownership of the watermarked material by removing his own watermark from it. This can raise questions about who actually owns the data. It is demonstrated that non-invertible watermarks are required for copyright protection purposes. It should not be feasible to remove a watermark from a document that has not been watermarked, according to the condition of non-inevitability of the watermarking technique. Another protocol attack is the copy attack. Instead of erasing the watermark or making it harder to identify it, the goal in this case is to estimate a watermark from watermarked data and copy it to other information, referred to as destination data [73]. The estimated watermark is adapted to the unique local features of the target data in order preserve imperceptibility. The copy attack is appropriate when a genuine watermark in the target data can be produced without mathematical understanding of the watermarking method or knowledge of the watermarking key. Once more, signal-dependent watermarks may be protected against the copy attack.

17. Application of Digital Image Watermarking

Digital Image watermarking is a specialized field of study owing to the possibility of using it in media applications like privacy protection, media forensics, data encryption and device management, copyright protection, and medical reports. Digital Watermarking methods can be used in a variety of applications [75, 95]. This section describes some of its major groups and applications. Some of the digital watermarking applications are depicted in Fig. 12.

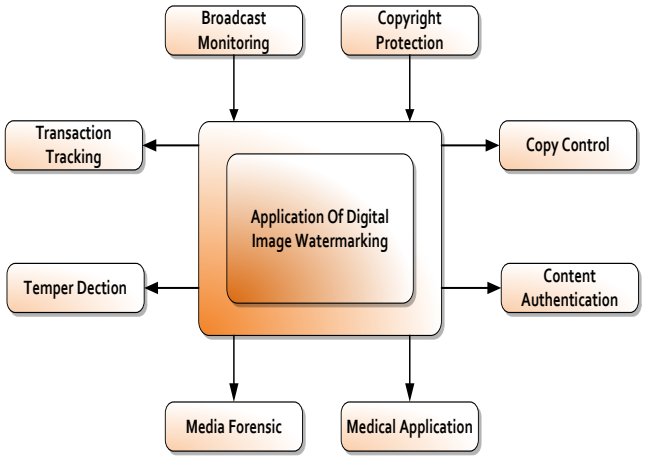

Fig.12. Application of Digital Image Watermarking.

1.16. Copyright Protection:

The watermarking algorithms are used to identify or prove the ownership of copyright materials. The proprietor of the electronic media employs a watermark to preserve intellectual property rights so they may subsequently demonstrate that a third party violated copyrights. The incorporated watermark serves as proof that the digital media belongs to the owner. Digital watermarking has several uses, including copyright protection. It makes it possible to identify the owner of the copyright and safeguards that person's rights to material dissemination. To safeguard the owner's rights, an image has strong watermarks placed on it. Despite standard image manipulation, geometric deformations, image contraction, and many additional forms of image alteration, it must be feasible to recognize the watermark. Thus, purposeful deletion of the strong watermark would significantly degrade the image's visual quality. If the watermark can be found, the owner must be positively identified. A preferable alternative to obvious copyright marks is watermarking. One possible target is a file header containing a copyright assertion. On the other hand, tough watermarks are difficult to get rid of without significantly lowering the image's quality. It is therefore appropriate to identify ownership and safeguard their copyright. Table. 2 shows the characteristics and its associated uses.

Table 2. Characteristics and their corresponding applications.

Characteristics	Applications
Data Payload	Integrity of medical images.
Imperceptibility	Copyright protection.
Robustness	Content authentication, and integrity verification
Computation cost	Protection of microscopy images.
Security	Copyright protection, data authentication, fingerprinting and tracking to digital contents
False Positive	Copy control and ownership.

1.17. Broadcast Monitoring:

Broadcast monitoring is used to verify the programmers broadcast on TV or radio. It especially helps the advertising companies to see if their advertisements appeared for the right duration or not. In this case, digital watermarks are imperceptible codes inserted into the broadcast video and audio that can be detached through the use of specialized hardware or software. By including watermarks in commercials, it is possible to use an automated system to check that the commercials are broadcast at the appropriate times. The system receives the broadcast and looks for these watermarks to determine the location and timing of the broadcast of the advertising. For audio and video clips, the same procedure may be applied.

1.18. Content Authentication:

Authentication is a means of confirming that the information or data that has been obtained must be the same as what has been transmitted. It shouldn't be altered in any way. For that reason, the sender included a digital watermark in the host data that would be retrieved and confirmed at the recipient's side. Content integrity is one of the major requirements of the owner or distributer of the content in the application, like the authentication of critical documents (e.g., photo ID), news photographs, medical records, etc. In image watermarking, authenticity pertains to the guarantee of the image's integrity [75, 96]. When a picture hasn't been altered, it's considered to be real. It helps with lawsuits by assuring reliable images for use as court testimony. and certification of digital artworks, medical records, and paintings from cultural heritage. For this objective, semi-fragile watermarks are appropriate since they can withstand acceptable alterations and flag up large manipulations.

1.19. Transaction Tracking:

Digital watermarks can be used to monitor how digital information is being utilized. Digital content copies can each be individually watermarked with metadata identifying the resource's authorized users. By identifying the people who copied the content unlawfully, such watermarks may be utilized to detect illicit content duplication. An IP (intellectual property) owner or content distributor can use transactional watermarks, sometimes referred to as hand prints, to add a distinctive, unique watermark to each permissible copy of a document in order to identify the source of an illegal replica. If a document with a transaction watermark is mistreated or distributed

illegally, the owner can track down the culprit. The delivery of movie dailies is a well-known practical use of fingerprinting. The output of each day's photography over the course of a movie's production is frequently given to a number of people engaged in its development. These daily reports are extremely secret, yet the media occasionally gets them. Because it is unique in each copy, the watermark serves as a tracker to identify the leak's source [75].

1.20. Tamper Detection and Localization:

To prevent tampering with the image, delicate digital watermarks are employed to indicate where changes have been made. Digital multimedia material often includes watermarks; however, these watermarks are brittle and can be erased by changes to the digital information. This software programme's objective is to find changes and modifications in a document. It has a strong connection to authentication. An image is considered fake if it has been tampered with. By identifying the areas of the picture that have been tampered with, tamper localization enables further investigation of manipulation. Media forensics can use this information to help. For instance, it is possible to determine the extent of the tampering and the motivations behind it. Depending on the applications, Robust, fragile, or semi-fragile watermarks can all be used for fraud exposure and localization.

1.21. Copy Control:

Most of the applications of watermarking appear to be unlawful. For instance, copyright violations have occurred rather than attempts to stop them from happening.

The watermarks that are described are either disseminated unlawfully or used after questionable alteration. However, the duplicate, alteration, and dissemination processes—which are the major sources of unlawful activity—can be controlled with the use of intelligent gear. The purpose of the copy control applications is to prevent people from making illegal copies of copyrighted content. In this application, to prevent the illegal copying of the copyrighted content, by embedding a watermark in the songs, images of movies, etc.

1.22. Medical Application:

Medical media and documents are also digitally verified, with the information of the patient and the visiting doctors. These watermarks can be both visible and invisible. This watermarking helps doctors and medical applications verify that the reports are not edited by illegal means [97].

1.23. Media Forensic:

Investigating digital data is part of media forensics, which aims to produce factually sound material for court testimony. Digital technologies are typically used to find deleted and concealed data [98]. Due to a variety of circumstances, media forensics has grown in importance as a study field. For instance, the rise in online crimes, the demise of revenue from piracy and fraud, and the requirement for justice.

18. Summary of Watermarking Techniques of Working Doamin

We may infer from the aforementioned studies that some watermarking methods are easy to appliance. While some prescriptions just slightly reduce the image quality, others significantly deceive it. Some are difficult to accomplish, while others are quite resilient against ordinary image processing; nonetheless, they are susceptible to geometrical attacks. Others, on the other hand, are extremely resistant to geometrical assaults yet extremely vulnerable to various noises. While some of them guarantee higher PSNR, NCC values as well as others have lower PSNR. Some applications are sturdy, while others are fragile, depending on the targeted applications. With the aid of the accompanying Table 3, this part therefore provides an overview of the outcomes of the state-of-the-art watermarking technics described above among persistent tendencies in watermarking methods. Table 3 includes a list of the methods in use, types of images, sizes of images, parameters, advantages, and associated applications.

We draw the conclusion from Table 3 that DCT offers the most robustness and imperceptibility, whereas LSB shows the lowest robustness and imperceptibility. In terms of durability and imperceptibility, the ranking might be expressed as

DCT > SVD > DWT > DFT > LSB

Table 3. Summary of the literature study watermarking methods.

Method Used	Type of Image	Size (Input Image and watermark Image)	Achievement of this Method	Limitation	Application
LSB Modification [14]	Color	512 × 512, 64 × 64	More robust resist different image processing attacks, and high imperceptibility	The worst case for there to be no division between the host image and the watermark image is when just the B component is utilized to embed colour.	Copyright protection
LSB with hash approach [15]	-	-	Effectively remove watermark information	less resistant to certain assaults	Histogram analysis
ISB [81]	Grayscale Image	256 × 256, 90 × 90	Enhanced resilience - Minimal watermark image distortion	Less resistant to geometrical assaults such as scaling, rotation, filtering, and cropping.	Image identification
DCT with hash key [16]	-	512 × 512, 64 × 64	Secure and resistant to basic image processing procedures	sensitive to interference; fragile	Image identification
DCT [17]	Grayscale Image	512 x 512, 64 × 64	resistant to JPEG compression and the Gaussian low pass filter	less resistant to certain assaults	Image identification
DCT with Chinese remainder theorem [18]	Grayscale Image	512 × 512, 64 × 64	Reduced computational complexity compared to SVD; increases security withstand JPEG compression assaults	weaker against manipulation attacks	Image verification
DCT [19]	Color	256 × 256, 256 × 256	resistant to attacks including rotation, noise, JPEG compression, and median filtering	More Complex	copyright protection, detection of tampering, image verification,
DCT with Arnold Transform [68]	Grayscale and Color image	512 × 512, 64 × 64	rotation, cropping, Gaussian noise, filtering, and combination assaults resistant,	less resistant to crop operation	Copyright protection
DFT [41]	Bitmap	512 × 512,	resilient to amplitude modulation,	less resistant to cropping	Image authentication

DFT with Chaotic system [69]	Grayscale image	256 × 256, 50 × 50	resistant to noise, cropping, and JPEG compression	Less resistant to rotational operation; difficult to compute	Content authentication
DWT [31]	Grayscale	256 × 256, 32 × 32	robust against JEPG compression, rotation, and median filtering	less resistant to cropping	Image identification
DWT [32]	Color and Grayscale image	512 × 512, 256 × 256	robust to noise types including Gaussian, salt-and-pepper, and speckle	less resilient to transformational operations	Copyright protection
DWT [33]	Color image	512 × 512, 32 × 32	resilient to filtering, cropping, and compression	less resistant to cropping and salt-and-pepper noise	Copyright protection
DWT with Haar wavelet [70]	Color	256 × 256, 64 × 64	resistant to Gaussian noise and lossy compression	Complex	content authentication
SVD [36]	Grayscale	512 × 512, 32 × 32	robust to JPEG compression, Gaussian noise, sharpening, and cropping	less resistant to scaling and rotation	Image verification
SVD [71]	Color and Grayscale image	256 × 256, 256 × 256	resistant to motion blur, median filtering, salt-and-pepper noise, gaussian noise, and JPEG compression	Not robust against rotation, cropping, and scaling	Content authentication

19. Conclusion

At present, digital information is easily manipulated due to the advanced development of digital multimedia. This issue makes a major area of study is digital picture watermarking. Digital image watermarking has been used as a crucial tool for digital security of the image, tamper detection, copyright protection, image identification, and verification in a variety of ways. In this paper, we examine the most popular modern watermarking methods. This study has shown that DWT is a superior and reliable image watermarking approach because of its multi-resolution capabilities. The key elements for building a successful watermarking system are robustness, imperceptibility, and capacity. However, completing all of these demands at once is practically impossible. It is necessary to maintain a healthy trade-off between these three needs. Therefore, to satisfy the aforementioned three crucial objectives, future work might be expanded by merging numerous methodologies from other disciplines. Furthermore, researchers should concentrate on creating novel, sophisticated methodologies in order to enhance resilience as well as security.

References

[1] N. Tarhouni, M. Charfeddine, and C. Ben, "Novel and Robust Image Watermarking for Copyright Protection and Integrity Control," Circuits, Syst. Signal Process.,vol. 39,pp.5059–5103,2020. https://doi.org/10.1007/s00034-020-01401-1

[2] L. Verma, "A Review on Digital Image Watermarking Using Transformation and Optimization Techniques," in 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2020, pp. 1008–1012. doi: 10.1109/ICACCCN51052.2020.9362885.

[3] C. I. Podilchuk and E. J. Delp, "Digital Watermarking: Algorthim and Applications," IEEE Signal Process. Mag., vol. 18, no. 4, pp. 33–46, 2001.

[4] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," Signal Processing, vol. 66, no. 3, pp. 385–403, 1998. https://doi.org/10.1016/S0165-1684(98)00017-6

[5] W. N. Cheung, "DIGITAL IMAGE WATERMARKING IN SPATIAL AND

TRANSFORM DOMAINS," in IEEE Conference, 2000, vol. 3, pp. 374–378. doi: 10.1109/TENCON.2000.892292.

[6] C. Pun, "A Novel DFT-based Digital Watermarking System for Images," ICSP2006 Proc., vol. 2, no. 8, pp. 3–6, 2006. doi: 10.1109/ICOSP.2006.345581.

[7] T. K. Tewari, "An Improved and Robust DCT based Digital Image Watermarking Scheme," Int. J. Comput. Appl., vol. 3, no. May 2014, pp. 28–32, 2010. 10.5120/699-980

[8] G. Tianming and W. Yanjie, "DWT-based Digital Image Watermarking Algorithm," 2011, vol. 3 no. 2, pp. 163–166. doi: 10.1109/ICEMI.2011.6037879.

[9] M. Begum and M. S. Uddin, "Digital Image Watermarking Techniques: A Review," Inf. Rev., MDPI, vol. 11, no. 110, pp. 2–38, 2020.; https://doi.org/10.3390/info11020110

[10] N. A. Loan, S. Member, N. N. Hurrah, and S. Member, "Secure and Robust Digital Image Watermarking using Coefficient Differencing and Chaotic Encryption," IEEE ACCESS, vol. 6, pp.19876-19897 no. c, 2018. doi: 10.1109/ACCESS.2018.2808172.

[11] H. H. Larijani and G. R. Rad, "A New Spatial Domain Algorithm for Gray Scale Images Watermarking," in Proceedings of the International Conference on Computer and Communication Engineering, 2008, pp. 157–161. doi: 10.1109/ICCCE.2008.4580587.

[12] Q. Kester, L. Nana, A. C. Pascu, S. Gire, M. Jojo, and N. N. Quaynor, "A Spatial Domain Watermarking Approach for Digital Images based on Image Features built on Formal Concepts Analysis," Int. J. Comput. Appl., vol. 119, no. 7, pp. 5–10, 2015.

[13] G. R. Manjula, Ajit Danti "A NOVEL HASH BASED LEAST SIGNIFICANT BIT (2-3-3) IMAGE STEGANOGRAPHY IN SPATIAL DOMAIN," vol. 4, no. 1, pp. 11–20, 2015.

[14] J. Abraham and V. Paul, "An imperceptible spatial domain color image watermarking scheme," vol. 31, issue-1 pp. 125–133, 2019.

[15] S. D. Muyco and A. A. Hernandez, "Least Significant Bit Hash Algorithm for Digital Image Watermarking Least Significant Bit Hash Algorithm for Digital Image Watermarking Authentication," no. April, 2019. https://doi.org/10.1145/3330482.3330523

[16] V. Kitanovski, D. Taskovski and S. Bogdanova, "Watermark Generation using Image-dependent Key for Image Authentication," EUROCON 2005 - The International Conference on "Computer as a Tool", Belgrade, Serbia, 2005, pp. 947-950, doi: 10.1109/EURCON.2005.1630103.

[17] C. -M. Pun, "High Capacity and Robust Digital Image Watermarking," 2009 Fifth International Joint Conference on INC, IMS and IDC, Seoul, Korea (South), 2009, pp. 1457-1461, doi: 10.1109/NCM.2009.85.

[18] J. C. Patra, J. E. Phua and D. Rajan, "DCT domain watermarking scheme using Chinese Remainder Theorem for image authentication," 2010 IEEE International Conference on Multimedia and Expo, Singapore, 2010, pp. 111-116, doi: 10.1109/ICME.2010.5583326.

[19] L. Laouamer and O. Tayan, "A Semi-Blind Robust DCT Watermarking Approach for Sensitive Text Images," Arab J Sci Eng, vol. 40, pp. 1097–1109, 2015.

[20] S. Roy and A. K. Pal, A Blind DCT based Color Watermarking Algorithm for Embedding Multiple Watermarks "Department of Computer Science and Engineering, Department of Computer Science and Engineering," AEUE - Int. J. Electron. Commun., 2016

[21] V. P. Vishwakarma and V. Sisaudia, "Gray-scale image watermarking based on DE-KELM in DCT domain domain," in Procedia Computer Science, 2018, vol. 132, no. Iccids, pp. 1012–1020. https://doi.org/10.1016/j.procs.2018.05.017

[22] S. Liu, Z. Pan, and H. Song, "Digital image watermarking method based on DCT and fractal encoding," IET Image Process. Spec., pp. 815–821, 2017. DOI:10.1049/IET-IPR.2016.0862

[23] B. Kaur, A. Kaur, and J. Singh, "STEGANOGRAPHIC APPROACH FOR HIDING IMAGE IN DCT DOMAIN," Int. J. Adv. Eng. Technol., vol. 1, issue. 3, pp. 72-78, 2011.

[24] F. Y. Shih and S. Y. T. Wu, "Combinational image watermarking in the spatial and frequency domains," Pattern Recognit., vol. 36, issue. 4 pp. 969–975, 2003. https://doi.org/10.1016/S0031-3203(02)00122-X

[25] J. R. Aparna and S. Ayyappan, "Comparison of digital watermarking techniques," International Conference for Convergence for Technology-2014, Pune, India, 2014, pp. 1-6, doi: 10.1109/I2CT.2014.7092189.

[26] Y. Zhang, "Digital Watermarking Technology: A Review," 2009 ETP International Conference on Future Computer and Communication, Wuhan, China, 2009, pp. 250-252, doi: 10.1109/FCC.2009.76.

[27] C. . -Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller and Y. M. Lui, "Rotation, scale, and translation

resilient watermarking for images," in IEEE Transactions on Image Processing, vol. 10, no. 5, pp. 767-782, May 2001, doi: 10.1109/83.918569

[28] C. De Vleeschouwer, J. -F. Delaigle and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," in Proceedings of the IEEE, vol. 90, no. 1, pp. 64-77, Jan. 2002, doi: 10.1109/5.982406.

[29] M. Utku Celik, G. Sharma, E. Saber and A. Murat Tekalp, "Hierarchical watermarking for secure image authentication with localization," in IEEE Transactions on Image Processing, vol. 11, no. 6, pp. 585-595, June 2002, doi: 10.1109/TIP.2002.1014990.

[30] Ping Wah Wong, "A public key watermark for image verification and authentication," Proceedings 1998 International Conference on Image Processing. ICIP98 (Cat. No.98CB36269), Chicago, IL, USA, 1998, pp. 455-459 vol.1, doi: 10.1109/ICIP.1998.723526.

[31] Z. Chen, Y. Chen, W. Hu, and D. Qian, "Wavelet Domain Digital Watermarking Algorithm Based on Threshold Classification," vol. 1, pp. 129–136, 2015. https://doi.org/10.1007/978-3-319-20469-7_15

[32] M. Haribabu, C. H. Bindu, and K. Veera, "A Secure & Invisible Image Watermarking Scheme Based on Wavelet Transform in HSI color space," Procedia - Procedia Comput. Sci., vol. 93, no. September, pp. 462–468, 2016. https://doi.org/10.1016/j.procs.2016.07.234

[33] S. Jia, Q. Zhou, and H. Zhou, "A Novel Color Image Watermarking Scheme Based on DWT and QR Decomposition," J. Appl. Sci. Eng., vol. 20, no. 2, pp. 193–200, 2017.

[34] N. Kashyap, "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)," I.J.Modern Educ. Comput. Sci., no. April, pp. 50–56, 2012.

[35] R. Choudhary and G. Parmar, "A robust image watermarking technique using 2-level discrete wavelet transform (DWT)," 2016 2nd International Conference on Communication Control and Intelligent Systems (CCIS), Mathura, India, 2016, pp. 120-124, doi: 10.1109/CCIntelS.2016. 7878213..

[36] C.-C. Chang, P. Tsai, and C.-C. Lin, "SVD-based digital image watermarking scheme," Pattern Recognit. Lett., vol. 26,Issue no. 10, pp. 1577–1586, 2005. https://doi.org/10.1016/j.patrec.2005.01.004

[37] S. J. Katti, Vyagreswara Rao Namuduri and K. R. Namuduri, "A practical approach for evaluating the capacity of watermarking channel," Proceedings of 2005 International Conference on Intelligent Sensing and Information Processing, 2005., Chennai, India, 2005, pp. 193-198, doi: 10.1109/ICISIP.2005.1529447.

[38] Y. Yusof and O. O. Khalifa, "Wavelet Transform," in IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, 2007, no. May, pp. 14–17.

[39] H. Yang, Y. Liang, X. Wang, and S. Ji, "A DWT-BASED EVALUATION METHOD OF IMPERCEPTIBILITY OF," in Proceedings of the 2007 International Conference on Wavelet Analysis and Pattern Recognition, Beijing, China, 2007, pp. 2–4.

[40] C. Song, S. Sudirman, M. Merabti and D. Llewellyn-Jones, "Analysis of Digital Image Watermark Attacks," 2010 7th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 2010, pp. 1-5, doi: 10.1109/CCNC.2010.5421631.

[41] Poljicak, L. Mandic, and D. Agic, "Discrete Fourier transform – based watermarking method with an optimal Discrete Fourier transform – based watermarking method with an optimal implementation radius," Jour nal Electron. I maging, no. july, 2011 DOI:10.1117/1.3609010.

[42] M. C. F. Garcia-ugalde and M. N. H. Perez-meana, "Robust watermarking method in DFT domain for effective management of medical imaging," 2013. https://doi.org/10.1007/s11760-013-0555-x

[43] V. Aslantas, A. Latif Dogan and S. Ozturk, "DWT-SVD based image watermarking using Particle Swarm Optimizer," 2008 IEEE International Conference on Multimedia and Expo, Hannover, Germany, 2008, pp. 241-244, doi: 10.1109/ICME.2008. 4607416..

[44] Xiaoyi Zhou, Jixin Ma and Wencai Du, "SoW: A hybrid DWT-SVD based secured image watermarking," PROCEEDINGS OF 2013 International Conference on Sensor Network Security Technology and Privacy Communication System, Harbin, China, 2013, pp. 197-200, doi: 10.1109/SNS-PCS.2013. 6553864..

[45] H. Tao, J. M. Zain, and A. N. Abdalla, "Robust Image Watermarking Theories and Techniques: A Review," vol. 12, issue no.1 January, pp. 122–138, 2014.

[46] Gorai and A. Ghosh, "Gray-level Image Enhancement By Particle Swarm Optimization," 2009 World Congress on Nature & Biologically Inspired Computing (NaBIC), Coimbatore, India, 2009, pp. 72-77, doi: 10.1109/NABIC.2009.5393603

[47] K. T. K.Kuppusamy, "Optimized Image Watermarking Scheme Based On PSO," Int. coference Model. Optim. Comput., vol. 38, pp. 493–503, 2012.

[48] S. Tyagi, H. V. Singh, R. Agarwal and S. K. Gangwar, "Digital watermarking techniques for security applications," 2016 International Conference on Emerging Trends in Electrical Electronics & Sustainable Energy Systems (ICETEESES), Sultanpur, India, 2016, pp. 379-382, doi: 10.1109/ICETEESES.2016. 7581413..

[49] Dixit, "A Review on Digital Image Watermarking Techniques," I.J. Image, Graph. Signal Process., vol. 4, no. April, pp. 56–66, 2017. DOI: 10.5815/ijigsp.2017.04.07

[50] V. S. Rao, R. S. Shekhawat and V. K. Srivastava, "A DWT-DCT-SVD based digital image watermarking scheme using particle swarm optimization," 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, Bhopal, India, 2012, pp. 1-4, doi: 10.1109/SCEECS.2012.6184795.

[51] F. Thakkar and V. K. Srivastava, "A particle swarm optimization and block-SVD-based watermarking for digital," Turkish J. Electr. Eng. Comput. Sci., vol. 25, no. 8, pp. 3273–3288, 2017.

[52] S. M. Arora, "A DWT-SVD based Robust Digital Watermarking for Digital A DWT-SVD based Robust Digital Watermarking for Digital Images," Procedia Comput. Sci., ScienceDirect vol. 132, pp. 1441–1448, 2018. https://doi.org/10.1016/j.procs.2018.05.076

[53] Y. Gangadhar, V. S. G. Akula, and P. C. Reddy, "Biomedical Signal Processing and Control An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation," Biomed. Signal Process. Control, vol. 43, pp. 31–40, 2018.

[54] V. Kumar, R. Lautan, M. Faisal, and K. M. Pandey, "Dwt and Particle Swarm Optimization Based Digital Image Watermarking," Int. J. Eng. Res. Technol., vol. 2, no. 9, pp. 2144–2149, 2013.

A. S. Seif Eddine Naffouti · Anis Kricha, "A sophisticated and provably grayscale image watermarking system," Vis. Comput., pp. 1–40, 2022. https://doi.org/10.1007/s00371-022-02587-y

[55] Mohan, "Multiple Watermarking Technique for Securing Online Social Network Contents using Back Propagation Neural Network," Future Generation Computer SystemsVolume 86, September 2018, Pages 926-939

[56] Onur JANE, Ersin ELBAS¸I "A new approach of nonblind watermarking methods based on DWT and SVD via LU decomposition" Turkish Journal of Electrical Engineering & Computer Sciences pp.1354-1366, 2014.

[57] P. Sridhar, "A Robust Digital Image Watermarking in Hybrid Frequency Domain," Int. J. Eng. Technol., vol. 7, pp. 243–248, 2018.

A. Kumar, "A Review on Implementation of Digital Image Watermarking Techniques Using LSB and DWT," Inf. Commun. Technol. Sustain. Dev. Adv. Intell. Syst. Comput., pp. 595–602, 2020. https://doi.org/10.1007/978-981-13-7166-0_5

[58] K. Abdulrahman and S. Ozturk, "A novel hybrid DCT and DWT based robust watermarking algorithm for color images," Multimed. Tools Appl 78, 17027–17049 2019. https://doi.org/10.1007/s11042-018-7085-z

[59] D. G. Savakar and A. Ghuli, "Robust Invisible Digital Image Watermarking Using Hybrid Scheme," Arab J Sci Eng 44, 3995–4008 (2019). https://doi.org/10.1007/s13369-019-03751-8.

[60] R. Pizzolante, A. Castiglione, B. Carpentieri, A. De Santis, and A. Castiglione, "Protection of Microscopy Images Through Digital Watermarking Techniques," in 2014 International Conference on Intelligent Networking and Collaborative Systems Protection, 2014, pp. 65–72. doi: 10.1109/INCoS.2014.116.

[61] Zear, A., Singh, A.K. & Kumar, P. A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimed Tools Appl 77, 4863–4882 (2018). https://doi.org/10.1007/s11042-016-3862-8

[62] T. T. Takore, "A New Robust and Imperceptible Image Watermarking Scheme Based on Hybrid Transform and PSO," I.J. Intell. Syst. Appl., vol. 11, no. November, pp. 50–63, 2018. DOI: 10.5815/ijisa.2018.11.06

[63] X. Zhou, H. Zhang, and C. Wang, "A Robust ImageWatermarking Technique Based on DWT, APDCBT, and SVD," Symmetry (Basel)., vol. 10, issue 77, pp. 2–14, 2018. https://doi.org/10.3390/sym10030077

[64] Y. Zhang, C. Wang, X. Wang, and M. Wang, "Feature-Based Image Watermarking Algorithm Using SVD and APBT for Copyright Protection," Futur. Internet, vol. 9, no. 13, pp. 2–15, 2017. https://doi.org/10.3390/fi9020013

[65] Jamal, S.S., Khan, M.U. & Shah, T. A Watermarking Technique with Chaotic Fractional S-Box Transformation. Wireless Pers Commun 90, 2033–2049 (2016). https://doi.org/10.1007/s11277-016-3436-0

[66] J. Wang and Z. Du, "A Method of Processing Color Image Watermarking Based on the Haar Wavelet," J. Vis. Commun. Image Represent., p. 102627, 2019.

[67] D. Vaishnavi and T. S. Subashini, “Robust and Invisible Image Watermarking in RGB Color space using SVD,” Procedia - Procedia Comput. Sci., vol. 46, no. Icict 2014, pp. 1770–1777, 2015.

[68] Mohanarathinam, A., Kamalraj, S., Prasanna Venkatesan, G.K.D. et al. Digital watermarking techniques for image security: a review. J Ambient Intell Human Comput 11, 3221–3229 (2020). https://doi.org/10.1007/s12652-019-01500-1

[69] J. Cox, M. L. Miller, and I. Way, “A review of watermarking and the importance of perceptual modeling,” proceedings.spiedigitallibrary.org, vol. 3016, pp. 92–99, 2014. DOI:10.1117/12.274502

[70] F. Cayre, C. Fontaine and T. Furon, "Watermarking security: theory and practice," in IEEE Transactions on Signal Processing, vol. 53, no. 10, pp. 3976-3987, Oct. 2005, doi: 10.1109/TSP.2005.855418.

[71] P. Luis, P. Comesa, and J. Ram, “Watermarking Security: A Survey,” Trans. DHMS I, LNCS, pp. 41–72, 2006. https://doi.org/10.1007/11926214

[72] J. Cox and J. M. G. Linnartz, “A review of watermarking principles and practices,” Digit. Signal Process. Multimed. Syst., vol. chapter 28, no. July 2000, pp. 461–485, 2015.

[73] J. Cox, M.L. Miller and J.A. Bloom., “Digital Watermarking and steganography”, 2nd ed. Morgan Kaufmann Publishers, San Francisco, USA, Volume 02, Issue 10 (October 2013) 2008.

[74] I. Podilchuk and Wenjun Zeng, "Image-adaptive watermarking using visual models," in IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 525-539, May 1998, doi: 10.1109/49.668975.

[75] Li and F. Yang, “One-dimensional neighborhood forming strategy for fragile watermarking,” J. Electron. Imaging, vol. 12, no. 2, pp. 284–291, 2003.

[76] H. Ling, R. C. Phan, and S. Heng, Robust blind image watermarking scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition “International Journal of Electronics and Communications., vol. 67, no. 10, pp. 894–897, 2013

[77] Goos, G.; Hartmanis, J.; Van Leeuwen, J. Cloud Computing and Security In Proceedings of the 4th International Conference, ICCCS, Haikou, China, 8–10 June 2018; pp. 691–697.

[78] P’erez-Freire, L.; Na, P.C.; Ramon, J.; Troncoso-Pastoriza, J.R.; Gonzalez, F.P. Watermarking Security: A Survey. In Transactions on Data Hiding and Multimedia Security; Lecture Notes in Computer Science: Berlin/Heidelberg, Germany, pp. 41–72. 2006

[79] Bruce, A.M. A Review of Digital Watermarking. Available online: https://pdfs.semanticscholar.org/d6eb/c1a3e1676df1b5a32033417215e8da096ac4.pdf (accessed on 16 February 2020

[80] Kumar, S. Basant, K. Ghanshyam, and S. Anand, Medical Image Watermarking. 2017.

A. F. Qasim, F. Meziane, and R. Aspin, “Digital watermarking : Applicability for developing trust in medical imaging workflows state of the art review,” Comput. Sci. Rev., vol. 27, pp. 45–60, 2018.

[81] Olanrewaju, R.F. Development of Intelligent Digital Watermarking via Safe Region. Ph.D. Thesis, Kulliyyah of Engineering, International Islamic University Malaysia, Selangor, Malaysia, 2011.

[82] N. Wu and M. Hwang, “Data Hiding: Current Status and Key Issues,” Int. J. Netw. Secur., vol. 4, no. 1, pp. 1–9, 2007.

[83] Habes, A. Information Hiding in BMP Image Implementation, Analysis and Evaluation. Inf. Transm. Comput. Netw., 6, 1–10. 2006 https://www.researchgate.net/publication/298223442_Information_hiding_algorithm_using_BMP_image

[84] Way, H. Fung, and C. Utfpr, “A Review Study on Image Digital Watermarking,” in The Tenth International Conference on Networks, , no. 1, pp. 24–28, 2011

A. M. Z. and A. A. Manaf, “A Novel Digital Watermarking Tec hnique Based on ISB (Intermediate Significant Bit),” World Acad. Sci. Eng. Technol. Int. J. Comput. Inf. Eng. Vol3, vol. 3, no. 2, pp. 444–451, 2009.

[85] G. N. Mohammed and A. Yasin, “Robust Image Watermarking Based on Dual Intermediate Significant Bit (DISB),” 6th International Conference on CSIT, 2014, pp. 18–22. 2014

[86] N. AHMED, T. NATARAJAN, AND K. R. RAO,Discrete, Cosine Transfonn, IEEE TRANSACTIONS ON COMPUTERS,., vol. 7, no. January, pp. 90–93, 1974.

[87] Discrete Wavelet Transform. Available online: https://en.wikipedia.org/wiki/Discrete_wavelet_transform (accessed on 23 October 2019).

[88] Kehtarnavaz, N. Digital Signal Processing System Design, 2nd ed.; Elsevier: Cambridge, MA, USA, 2008.

[89] P. Bao and X. Ma, “Transactions Letters, Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition,” IEEE Trans. Circuits Syst. Video Technol., vol. 15, no. 1, pp. 96–102, 2005.

[90] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, “Attacks on digital watermarks: Classification, estimation-based attacks, and benchmarks,” IEEE Commun. Mag., vol. 39, no. 8, pp. 118–125, 2001.

[91] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, “Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications,” IEEE J. Sel. Areas Commun., vol. 16, no. 4, pp. 573–586, 1998.

[92] Menezes, A.J., et al., Handbook of Applied Cryptography. 1996: CRC Press. 780 pages

[93] Deepthi Anand", U.C. Niranjan,“WATERMARKING MEDICAL IMAGES WITH PATIENT INFORMATION” Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Vol. 20, issue-No 2,1998

[94] R. Liu, W. Trappe, J. Wang, M. Wu, and H. Zhao, EURASIP Book Series on Signal Processing and Communications Multimedia Fingerprinting Forensics for Traitor Tracing

[95] Perez-Siguas, R. ., Matta-Solis, H. ., Millones-Gomez, S. ., Matta-Perez, H. ., Cruzata-Martinez, A. ., & Meneses-Claudio, B. . (2023). Comparison of Social Skills of Nursing Students from Two Universities of Lima. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 14–19. https://doi.org/10.17762/ijritcc.v11i2.6105

[96] Juan Garcia, Guðmundsdóttir Anna, Johansson Anna, Maria Jansen, Anna Wagner. Machine Learning for Decision Science in Healthcare and Medical Systems. Kuwait Journal of Machine Learning, 2(4). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/210