ISSN: 0067-2904

Digital Watermarking, Methodology, Techniques, and Attacks: A Review

Hind Moutaz Al-Dabbas[1]*, Raghad Abdulaali Azeez[2], Akbas Ezaldeen Ali[3]
[1]*Department of Computer Science, College of Education for Pure Sciences/Ibn Al-Haitham, University of Baghdad, Baghdad, Iraq*
[2] *Computer Unit, College of Education for Human Science-Ibn-Rushed, University of Baghdad, Baghdad, Iraq*
[3]*Department of Computer Science, University of Technology, Baghdad, Iraq*

Received: 19/5/2022 Accepted: 14/10/2022 Published: 30/8/2023

Abstract

The use of multimedia technology is growing every day, and it is difficult and time-consuming to provide allowed data while preventing secret information from being used without authorization. The material that has been watermarked can only be accessed by authorized users. Digital watermarking is a popular method for protecting digital data. The embedding of secret data into actual information is the subject of digital watermarking. This paper examines watermarking techniques, methodologies, and attacks, as well as the development of watermarking digital images stored in both the spatial and frequency domains.

Keywords: Watermarking, LSB, DCT, DWT, SVD

العلامات المائية الرقمية، المنهجية، التقنيات والهجمات: مراجعة

هند معتز الدباس[1]*، رغد عبد العالي عزيز[2] ، اقباس عز الدين علي[3]

[1]*قسم علوم الحاسبات، كلية التربية للعلوم الصرفة/ ابن الهيثم، جامعة بغداد، بغداد، العراق

[2]كلية التربية ابن رشد للعلوم الانسانية، جامعة بغداد، بغداد، العراق

[3] قسم علوم الحاسوب، الجامعة التكنولوجية، بغداد، العراق

الخلاصة:

يتزايد استعمال تقنية الوسائط المتعددة كل يوم، ويعد توفير البيانات المسموح بها وحماية المعلومات السرية من الاستعمال غير المصرح به وهي عملية معقدة وتستغرق وقتًا طويلاً. يمكن للمستخدمين المصرح لهم فقط الوصول إلى المواد التي تم وضع علامة مائية عليها. العلامات المائية الرقمية هي طريقة شائعة الاستعمال لحماية البيانات الرقمية. يعتبر تضمين البيانات السرية في المعلومات الفعلية موضوع العلامة المائية الرقمية. في هذا البحث تم دراسة تقنيات ومنهجيات وهجمات العلامات المائية ، فضلاً عن إنشاء أنظمة في وضع العلامات المائية للصور الرقمية المخزنة في كل من المجال المكاني والتردد.

1. Introduction

The rise of multimedia technology has paved the path for more worldwide communication. One of the most critical aspects of data communication is information security [1]. As a result, numerous illicit actions, including as counterfeiting, de-authentication, and utilizing and copying works without authorization, are becoming more difficult to regulate [2]. Therefore,

*Email: hind.moutaz@ihcoedu.uobaghdad.edu.iq

scientists have started to develop various methods and policies to safeguard the information transmitted through the Internet to protect copyright content, enhance security, and avoid attacks and suspicion from malicious third parties [3].

Tominaga and Komatsu in 1988 were the first to create the phrase "computerized watermarking" [2]. Although digital watermarking was first introduced in 1993, it is considered to be a useful and secure method for protecting data [4]. Digital watermarking is a technology that protects digital media by adding security, data validation, and publishing protection [5]. After 1995, interest in digital watermarking grew, and a few organizations began adopting watermarking technology in various forms [4]. This technique entails concealing sensitive information within a protected medium, which might be a text, audio, image, or video.

The watermark should be undetectable to attackers but easy to detect and extract using the appropriate method. The Copy Protection Technical Working Group (CPTWG) in 1999 discussed the possibility of developing a method that would allow video content owners to protect their Digital Video Discs (DVDs). [5]. Watermarking has been embraced by the International Organization for Standardization (ISO) to plan Moving Picture Experts Group (MPEG) principles [6] [7]. Despite the fact that watermarks may be integrated with any computerized content, this exploration focuses on watermarking images [8] [9]. Digital watermarking consists of the embedding of the information that constitutes the authentication or copyright. This information is known as a watermark, through a sequences of objects (host signal or original content) in a way that the watermark can be observed or withdrawn later when vital without destroying the host signal [5] [6].

Digital watermarking is the process of incorporating a watermark into a piece of data a multimedia file known as original content or host signal so that it may be seen or removed later without degrading the host signal. A digital watermarking system consists of an embedder and a detector in its most basic form. The watermark and the host signal are the embedder's inputs. The watermarked work is the embedder's output. The detector is in charge of detecting and decoding the presence of a watermark in digital content [10]. In this example, a simple watermarking scheme is shown in Figure 1.

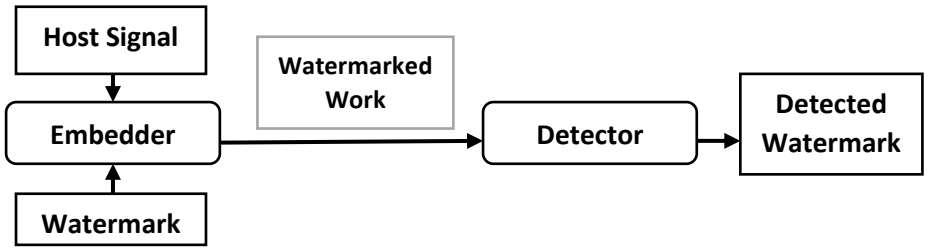

Figure 1: A simple scheme of digital watermarking [10].

The use of multimedia technology has grown exponentially since the invention of computers. This complicates the duties of preventing unauthorized access to information (confidentiality), ensuring the accuracy of data and safeguarding against illegal modifications (integrity), and ensuring that authorized individuals have access to information (availability).

These are three most important security features for the system, all of which are extremely challenging to implement. However, striking a balance between these three competing demands is challenging. The ability to withstand attack is one of the most important properties of any watermarking technique. In the context of watermarking, an attack is anything that impedes or

hinders the detection of the watermark. At that moment, the managed watermarked data is referred to as attacked data [11].

The image watermarking requirements may be handled as characteristics, properties, or attributes of image watermarking. This requirement is broad and causes numerous layout issues depending on image watermarking applications and purpose. These requirements need to be taken into consideration while the designing watermarking system. There are five basic requirements as follows [12, 13, 14].

- **Fidelity**

Watermark fidelity can be thought of as a portion of perceptual imperceptibility or transparency. It refers to how unwatermarked and watermarked photographs are alike. This approach to watermarking takes advantage of human eyesight limitations. Watermarking should not cause apparent distortions because this lowers the image's economic value.

- **Robustness**

The ability to detect a watermark after various typical manipulation operations of the signal processing is required for robustness in the digital image watermarking systems. Spatial filtering, mapping of color, printing and scanning, lossy compression, translation, scaling, and rotation are some of these procedures. Other procedures like analog to digital (A/D) and digital to analog (D/A) transformations, image enhancement, trimming, and so on are included. Numerous broad approaches to high robustness exist, including redundant embedding, spread spectrum, and embedding watermarks, among others. As a result, a strong digital image watermarking system must be resistant to a variety of attacks, ensuring that watermark data cannot be removed or excluded by unauthorized distributors.

- **Data Payload**

Watermarking capacity is another term for data payload. It refers to the maximum quantity of data that may be buried without compromising the quality of the image. The amount of hidden data can be used to assess it. This attribute specifies the amount of data that would be embedded by means of a watermark in order for it to be identified during extraction.

- **Security**

If security is a primary concern, a secret key must be utilized for the embedding and detection process. Watermark systems use three sorts of keys: public key, detection key, and private key. With the anti-reverse engineering research algorithm, the watermark should not be removed by hackers.

- **Computational Complexity**

The computational complexity of a watermarking algorithm reflects how long it takes to encode and decode data. More computational complexity is required to assure the security and authenticity of the watermark. Real-time applications, on the other hand, demand both speed and efficiency.

2. Digital Watermarking Techniques

Digital watermarking is a technique for hiding specific information within a protected asset, which could be an image, video, audio, or even text. Attackers should be unable to discover the watermark, but the exact methodology should be able to detect and extract it. Digital image watermarking techniques can be classified based on their working domain, the type of document

or media, human perceptibility, data extraction, and application. Figure 2 shows the classifications of digital watermarking [15].

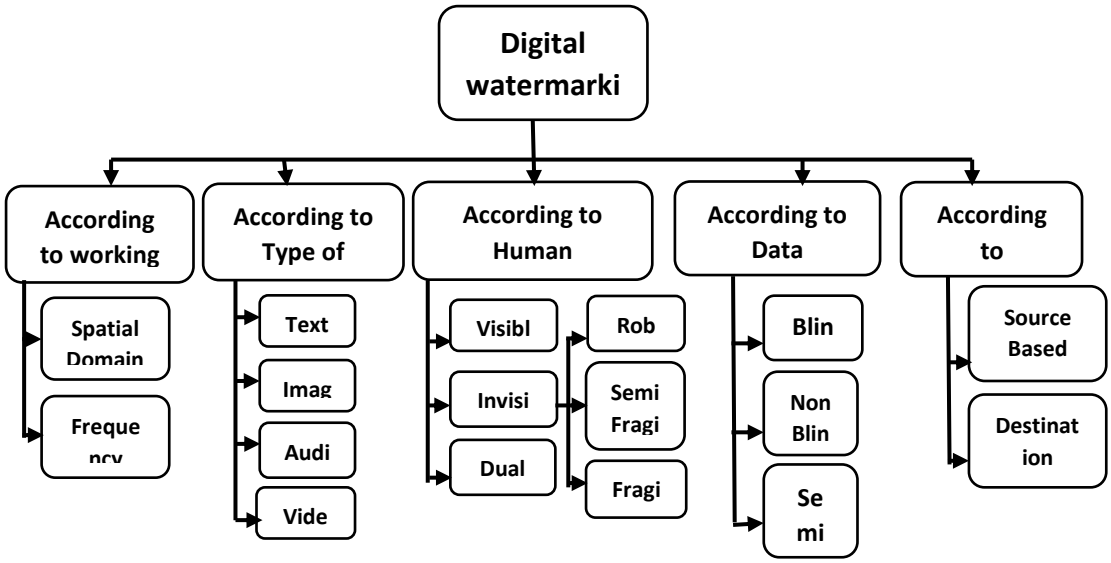

Figure 2: Digital Watermarking Techniques [15].

2.1 According to Working Domain: The watermark is inserted in a spatial domain watermarking system by directly changing the value of the pixel in an image. During watermark embedding, no transformations are applied to the host signal. The spatial domain watermarking strategy is simple and less resistant to typical signal processing operations because the watermark does not spread throughout the image and some common signal processing operations can easily remove the embedded watermark without changing the quality of the watermarked image [16] [17]. On the other hand, frequency domain watermarking schemes embed the watermark after the image has been transformed to the transform domain by modifying the transform coefficients, or convert the image to the frequency domain and then modify the transform coefficients [17].

2.2 According to the type of document or by media: The following categories apply to host or cover signal-based watermarks: [18]

- **Text watermarking***:* this technique embeds the watermarks in the font shape as well as the space between characters.
- **Image watermarking:** In this technique, payloads are placed in images using this watermarking approach. To check for ownership, information connected to the image is detected or retrieved.
- **Audio watermarking:** Due to the widespread availability of MP3 files in numerous domains, this watermarking approach is a hot research topic.
- **Video watermarking:** This technique is an extension of the image watermarking scheme. Compression is performed using real-time extraction approaches and resilience in this classification.

2.3 According to Human Perceptibility: There are two types of this watermarking technique, which are: visible and invisible categories. The watermark is translucent in the cover image in the visible watermarking, but it is implanted into the cover image in invisible watermarking, preserving the visual quality and imperceptibility. Thus, this watermark necessitates robustness to defend the ownership from different types of malicious attacks [19].

- **Robust:** In this kind of watermarking techniques, geometrical and non-geometrical attacks have no effect on embedded watermarks. Copy control, copyright protection, fingerprinting, and broadcast monitoring are all employed in this watermark.
- **Semi-fragile**: In these techniques, watermarks can withstand various changes, such as the insertion of quantization noise into a watermarked image.
- **Fragile:** mostly used to verify the integrity and content authentication of multimedia data that includes signature information are the fragile watermarks. This watermark verifies whether or not the image has been tampered with. A fragile technique is usually more straightforward to execute than a sturdy one.

In dual watermarking, the watermark is a hybrid between visible and invisible watermarking.

2.4 According to Data Extraction: the following types of techniques are used to recognize embedded watermark information [18] and [20].

- **Blind:** In this category, neither original material nor embedded watermarks are required. Public watermarking techniques are another name for this type of approach.
- **Non-blind:** This type of technique desires an original medium. This approach can extract data from a distorted image as well as the original material.
- **Semi-blind:** In this technique, the original material is not required for data extraction as watermark detection.

2.5 According to Application: Source-based watermarking and destination-based watermarking are two types of watermarking techniques. When a unique watermark recognizing the owner is presented to all copies of a single image being circulated, source-based watermarks are desired for ownership identification or authentication. It could be used to verify identity and assess whether a picture or other piece of electronic data has been tampered with. In destination-based watermarking, each disseminated copy is assigned a unique watermark that identifies the buyer. In the case of illicit reselling, the destination-based watermark might be utilized to track down the purchaser [20].

Watermarking techniques have been widely publicized in the last two decades. This paper will examine various current watermarking approaches for creating and embedding copyright information in digital image assets, focusing on digital watermarking approaches based on the working domain, which includes both spatial and frequency domains. Furthermore, attacks on digital image watermarking are taken into consideration.

3. Methodology

This study will explain working domain watermarking which is one of the watermarking techniques that includes spatial domain. It includes a Least Significant Bit (LSB) based scheme, a frequency domain and Discrete Cosine Transform (DCT), Discrete Wavelet Transformation (DWT), and Singular Value Decomposition (SVD), as well as an explanation of the attacks on watermarking and its classifications. Figure 3 shows the classifications of the working domain watermarks.

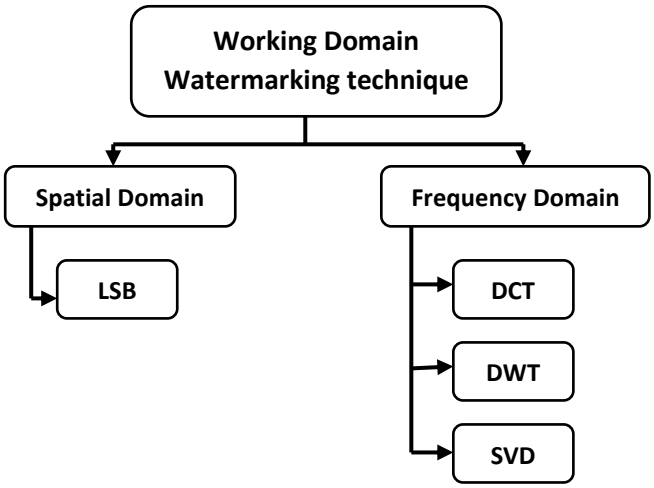

Figure 3: Working domain watermarking technique

3.1 Working Domain watermarking technique

This type of watermarking approach includes spatial and frequency domains.

3.1.1 Spatial domain

Spatial domain watermarking techniques that conduct direct transformations on image pixels are known as Least Significant Bit watermarks (LSB).

3.1.1.1 Least Significant Bit (LSB) based scheme

The Least Significant Bit (LSB) technique is a simple way to embed information into a cover image. In this method, the watermarking is performed by generating a third image that comes from overwriting the least significant bits of the original image with the least significant bits of the watermark image [21]. Although LSB coding is a straightforward technique, the watermark's resilience is limited [3]. The LSB approach has the advantage of being simple, requiring fewer computations, and causing minimal modifications in the host image after watermarking. However, the problem with this technique is that altering bits can readily remove the watermark. Watermarks can potentially be removed by noise generated during image transmission. [22, 23].

3.1.2 Frequency domain

Watermarking in the frequency domain is becoming increasingly common because these schemes have a variety of advantages, such as: (i) it is possible to achieve statistical independence between pixels as well as high-energy compression. (ii) The watermark is scattered irregularly over the entire spatial image, making it more challenging for adversaries to decipher and interpret the mark. (iii) Watermark can be hidden into a significant area, thus providing them more robust against several attacks (iv) Cropping danger to the spatial realm has little effect on transformation domain [24].

3.1.2.1 Discrete Cosine Transform (DCT)

The (DCT) function determines the two-dimensional Discrete Cosine Transform (DCT) image. The DCT has the property that, for a typical image, the majority of the image's visually significant information is concentrated in a few DCT coefficients [25]. The DCT is a linear transform that converts an n-dimensional vector into n coefficients. It is particularly resistant to Joint Photographic Experts Group (JPEG) compression, as DCT is used in JPEG compression. [3]. DCT is employed in a variety of fields, including data compression, pattern

recognition, and image processing. The image is segmented into non-overlapping blocks of a certain fixed dimension via a DCT-based technique. DCT is applied to each of the image's blocks. To extract blocks of greater value, such as Hue Saturation Value (HSV), block selection criteria are used. Coefficients are chosen to correlate with the blocks chosen. The coefficient matrix's leftmost corner contains low-frequency components that are quite essential [21].

The rightmost corner of the matrix contains high frequency components. The DCT method is used to divide an image into pseudo-frequency bands. Watermarks are typically incorporated into middle frequency subbands. When watermarks are inserted between high-frequency components, the attack resistance is reduced, but the watermarks are effectively hidden. Watermarks are placed into image coefficients by gradually changing them. [15]. In the DCT domain, many studies on digital picture watermarking technologies have previously been conducted. Block-based DCT image watermarking is one of them. It works by breaking the original image into distinct blocks of image and then applying the DCT transform to each of them. The approach then uses an algorithm to inject the watermark into the block and DCT-based host image. The watermarked image is then created using the Inverse Discrete Cosine Transform (IDCT). The DCT approaches for watermark embedding presented above are best characterized by Figure 4 [18].

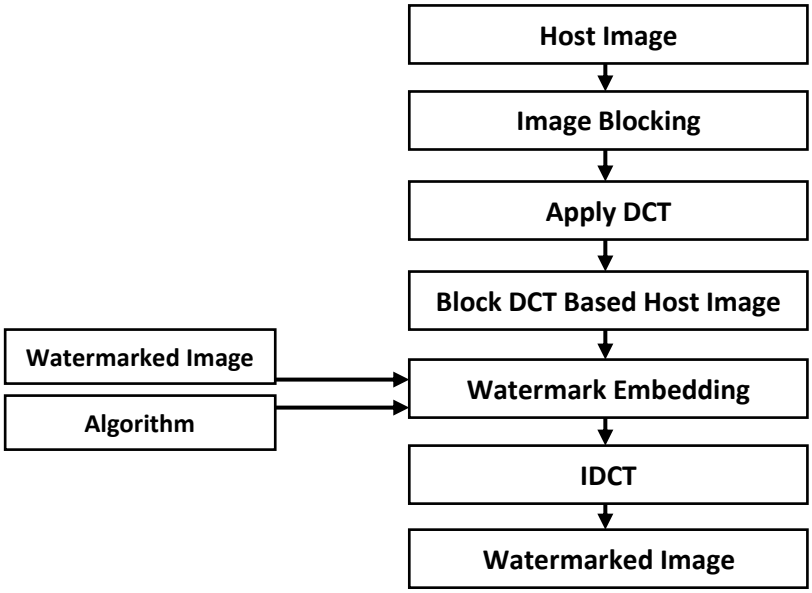

Figure 4: The embedding of watermark in a block-based DCT domain [18]

3.1.2.2 Discrete Wavelet Transformation (DWT)

A Discrete Wavelet Transform (DWT) in mathematics, a wavelet is a transform that decomposes a signal into wavelets instead of frequencies. DWT wavelets are sampled discretely. By capturing numerous information characteristics, such as position in frequency and time, DWT becomes a more appealing research subject. The signal is decomposed using a set of wavelets, which are mathematical functions. Digital signal processing, image compression, and signal noise reduction can all benefit from the wavelet transform. A wavelet transform's fundamental idea is to employ a set of basic functions named wavelets to provide frequency domain localization. When utilizing a wavelet transform, high frequency resolution may be acquired at low frequencies and high time resolution can be obtained at high frequencies [15]. The technique of DWT image watermarking divides the original image into three levels.

The watermark is implanted at three different levels using the sub bands: Low-High3 (LH3), High-High3 (HH3), and High-Low3 (HL3). Sub bands cover a large span of the image's frequency spectrum. As a result, the watermarking system's robustness is improved. [15]. A three level DWT is presented in Figure 5.

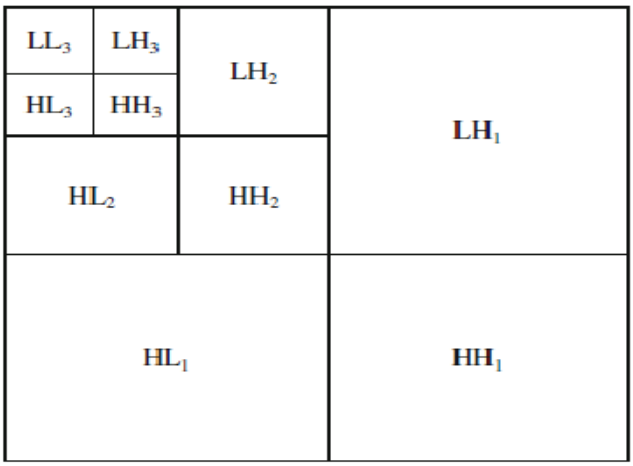

Figure 5: Three-level discrete wavelet decomposition [15]

3.1.2.3 Singular value decomposition (SVD)

Singular value decomposition is performed for dimensionality reduction. It has its roots in linear algebra. SVD may convert correlated values into a set of uncorrelated variables, revealing the numerous relationships between the original data [19]. SVD multiplies a complex or real matrix. The method generalizes the eigen-decomposition of a symmetric matrix with nonnegative eigenvalues to any m*n matrix by extending the polar decomposition. In statistics and digital signal processing, the SVD transformation is commonly utilized. Equation (1) can be used to compute the SVD of a matrix M [19].

$$M = U \Sigma V \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where M is a matrix of m*n derived from the field K, which is real numbers or complex numbers. U is either an orthogonal matrix (if K = R) or m*m unitary matrix over K, Σ is a non-negative real number on the diagonal of a diagonal m*n matrix, and V* is the conjugate transpose of V, which is a n*n unitary matrix over K. In the field of watermarking, SVD was gaining popularity [19].

3.2 Watermarking Attacks

An assault is any processing in a system of watermarking that may result in the destructive detection of the watermark or disruption of the communication delivered by the watermark. The attacked data is then identified from the processed watermark data [16], [17]. As a result of these attacks, the watermarked image has been deformed (which may be intentional or unintentional). Despite the fact that achieving robustness against attacks is still a work in progress, a few solutions can withstand global attacks. To achieve synchronization, most effective solutions rely on embedding data in a space that is geometrically invulnerable, using layouts, using self-synchronizing watermarks, or using highlight spots. When valuable information is attacked by intruders, its originality is compromised. For example, the image size may be changed and noise may be added. [16], [17], and [18].

3.2.1 Classification of watermarking attacks

Removal, geometry, protocol, and cryptographic attacks are the four basic categories of watermark attacks. These are further separated into sub-classes. (Figure 6) shows the classification of watermarking attacks.

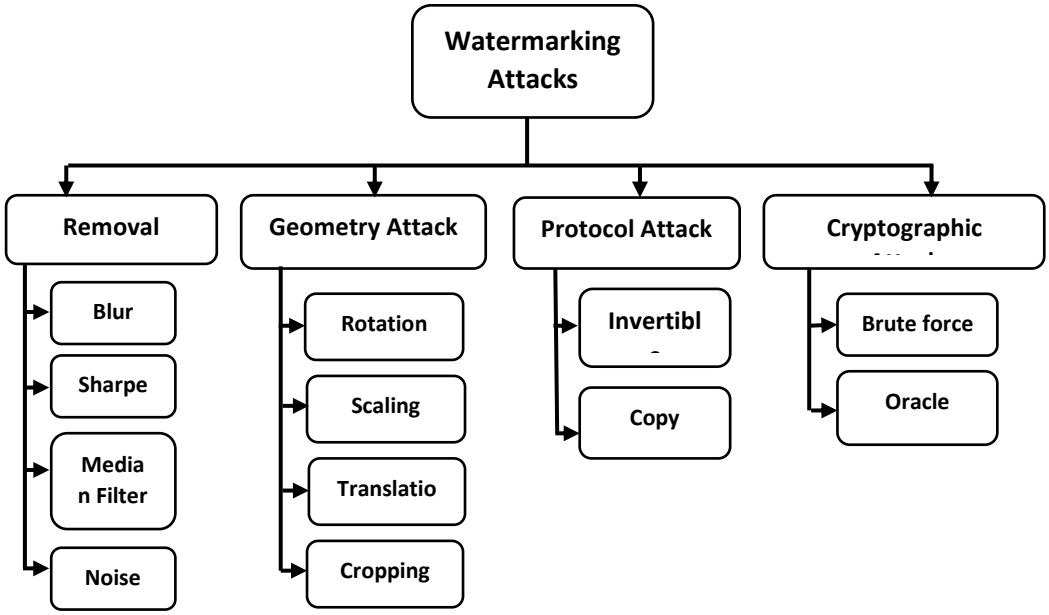

Figure 6: Types of digital watermarking attacks [23]

3.2.1.1 Removal Attack

The removal assault seeks to completely remove the watermark data without compromising the watermarking algorithm's security. Advanced watermark removal attacks try to augment techniques such as quantization and de-noising in order to obstruct the implanted watermark as much as possible while maintaining the quality of the attacked document. Median Filter, Sharpen, Blur, and Noise attacks are the four types of removal attacks. Gaussian noise, salt and pepper noise, speckle noise, and Poisson noise are all types of noise [20].

3.2.1.2 Geometry Attack

The geometry attack primarily affects the watermark locator's synchronization with the encoded data, rather than the watermark itself. Each geometric assault has a set of constraints that govern how the operation is carried out on the target. Rotation, Scaling, Translation, and Cropping are the four different types of geometry attacks [21], [22].

3.2.1.3 Protocol Attack

In this attack, the attacker put his/her watermark on the host data. Modern digital systems are vulnerable to such attacks. To cite a few examples, there is the duplication of a legitimate watermark. Invertible and copy attacks are the two forms of protocol assaults [23].

3.2.1.4 Cryptographic Attack

Cryptographic attacks try to compromise watermarking's security. They come in two varieties: Oracle and Brute-Force. Vaude-nay presented the Oracle attack for the first time at Euro Crypt '02. The attack pretends to be an Oracle that, when a cipher text is encountered, decrypts it and sends a valid or invalid response to the sender. It is assumed that the attackers have access to the padding oracle and can retrieve the padded messages that are encrypted in cipher block chaining (CBC) mode. As a result, the attacker can use approximately 128b oracle calls to recover the plaintext for the cipher content, where b is the number of bytes in a block.

In a brute force attack, the impostor tries all possible keys for decrypting the message. An exhaustive key search is another name for it. The size of the secret key influences how long it takes to decipher a cipher. A dictionary attack is another type of assault in which the impostor attempts to guess the password by using popular idioms or existing terms [24].

4. Literature review

Here is a survey of the working domain in digital watermarking techniques, which are LSB in the spatial domain and DCT, DWT, and SVD in the frequency domain, as well as digital watermarking attacks.

4.1 LSB

Van Schyndel et al. [25] proposed the potential of recording a digital watermark on a normal 512*512 intensity image with an 8-bit gray scale. The linearity property allows certain image processing, such as averaging, to take place on the image without distorting the watermark beyond recovery. This is achieved based on bit plane modification of the LSB with the use of linear addition of the watermark to the image data. The proposed work's limitation is that the watermark is undetectable only in circumstances where low-level gaussian noise is expected.

Rhoads [26] proposed a method for including or removing little irregular parts from each pixel. Every pixel's LSB was used to analyze a paired set of bits for expansion or subtraction. On the off chance that the LSB was equivalent to the comparing cover bit. The arbitrary amount was either added or deleted. Perceptual pertinence is not used in this technique.

Byun et al. [27] proposed a fragile watermarking algorithm for the authentication of images that uses a grey image of size 256×256 as an original image. They use singular value decomposition of the image to see the integrity of images. The singular values are changed to the binary bits which are inserted into the LSBs of the original image to detect any modification of watermarked images, which makes the quality of watermarked images very high. This work's limitation is that the watermark is equal to the authentication data if there is no change to the watermarked image.

Yang, et al. [28] proposed encrypting the watermark image before embedding it into the least significant bits of cover images to preserve the authenticity of the evidence by using the PKI (Public-Key Infrastructure), public-key cryptography, and watermark techniques.
Bamatraf et al. [29] proposed a new LSB scheme with embedding watermarked 512x512 grayscale images in the third and fourth LSBs, so it will be more secure against the attacks impacting the two least significant bits and show that the quality of the watermarked image is higher.

Almutiri [30] proposed the LSB techniques in the spatial domain, by selecting a subset of pixels and replacing the least significant bits of the selected pixels with the watermark bits, as well as a set of different proposed LSB algorithms, comparing them and pointing out the common strengths and main gaps that should be focused on. Even though they are sensitive to signal processing operations and generally show reduced robustness to different attacks.

Roy et al. [31] proposed an adaptive LSB replacement technique to include copyright information, i.e., the watermark bits, to increase imperceptibility. Robustness and data hiding capacity are improved by changing the higher bit-planes rather than just the LSB, which reduces conflicts between imperceptibility and data hiding capacity while also offering some robustness. Database images are used as a set of host or cover images after modifying each

image to a 256 × 256 grayscale image and, as the watermark image, a binary image of size 16 × 16.

It was noticed that the LSB technique in spatial domain watermarking was easy to destroy by changing bits, and the limitation is that the LSB is less robust against geometric attacks, like scaling, rotation, filtering, and cropping. The researchers proposed several methods for LSB and are attempting to combine other methods to make watermarking techniques more resistant to attacks over time.

As observed in Yang et al. [28] they used PKI (Public-Key Infrastructure) to check the integrity of digital images by correcting public-key without side information and protecting the watermarks without tampering or forging, and in Bamatraf et al. [29], they used the third and fourth LSB to make the quality of the watermarked image higher. In Roy et al. [31], adaptive LSB was used to improving imperceptibility.

4.2 DCT

Koch and Zhao [32] proposed calculations the place of watermarking where the image was first converted to DCT and the watermark was discovered in the repetition coefficients. In contrast to the locales where the kinds of intensities changed slowly, changes in the image data caused by moderate levels of wideband noise or controlled loss of information are hardly visibly noticeable. Therefore, the core frequencies displayed strong resistance to JPEG pressure and minimal perceptual bending.

Borg and Pitas [33] proposed certain blocks in the gray level image based on a Gaussian network classifier, consisting of embedding linear constraint amongst the chosen coefficients of DCT, and after that, defining regions of circular detection in the DCT domain. A rule is provided for producing the DCT parameters of different watermark. This leads to the generation of watermarks that are able to resist at certain JPEG compression ratios.

Shieh et al. [34] proposed a robust algorithm for DCT-based GA-watermarking that is robust against watermarking attacks. Also, examine the effectiveness of the scheme by checking the fitness function in GA to train the frequency set for embedding the watermark and also improve the watermarked image quality with the aid of GA. The calculations in obtaining the perfectly modified coefficients for the watermark insertion boost the photo nature and energy of the image watermarked at the same time.

Megalingam et al. [35] proposed a robust method for digital watermarking in the spatial domain. That deals with an image in the spatial domain which is watermarked at different intensity subsections. Furthermore, they analyzed the performance of the method and implemented a frequency domain DCT/IDCT based digital watermark. The Peak Signal-to-Noise Ratio (PSNR) obtained ensures the robustness and quality of the watermarked image.
Abraham and Paul [36] proposed a watermarking approach that offers a greater visual quality following watermark addition by allowing for undetectable watermark inclusion in grayscale images. The image's eligible pixel blocks are then modified with DCT to use the mid-frequency coefficients for watermark integration. This reveals watermarked image copies with strong signal to noise ratios and robustness.

Nandini, and Divya [37] proposed the Digital Cosine Transform (DCT), Fast Fourier Transform (FFT) and Discrete Wavelet Transform (DWT). An image is deconstructed into a set of components with limited bands that can be adjusted to reconstruct the original image

without error using the wavelet transform. This method is used to preserve the quality of a digital image while simultaneously increasing the security level of the image. The primary strengths of the method include low time complexity and high embedding capacity.

Ko et al. [38] proposed a watermarking method based on block-based discrete cosine transform (DCT) coefficient change that is both robust and transparent. To adapt this difference to a preset range, the difference in the DCT coefficients of two blocks is calculated and changed based on the watermark bit. This led to robustness against various attacks and was tested experimentally. It was found to be quite robust against both single and combination attacks. The proposed method used images which are: Lena, Airplane, and Pepper images. Each cover image is 512 × 512 and the size of the watermark is 64 × 64, they evaluated the quality of the watermarked image by using the peak signal-to-noise ratio (PSNR), normalized cross-correlation (NC), and bit error rate (BER) as benchmarks.

Hamidi et al. [39] proposed a watermarking method that is robust and hybrid based on discrete cosine transform (DCT), discrete wavelet transform (DWT), and Scale-Invariant Feature Transformation (SIFT). The watermark is embedded in the DWT-DCT domain, in the middle band of the discrete cosine transform (DCT) coefficients of the HL1 band of the discrete wavelet transform (DWT), to withstand image processing operations. The SIFT feature points are then recorded and used to rectify the geometric alterations introduced during the extraction procedure. This demonstrate its excellent resistance to common image processing attacks and geometric alterations while maintaining a high level of imperceptibility. The proposed method used images include the most commonly used images in the watermarking literature of size 512×512 standard gray-scale natural images which are: Baboon, Pepper, Cameraman, Lena, Goldhill, Walkbridge, Womanblonde, Livingroom, Pirate, and Lake.

It was noticed that the DCT technique in frequency domain watermarking was fragile in the case of tampering, less imperceptible, had higher computational complexity, and was less robust against cropping operations. The DCT technique has been getting more effective in recent years, and researchers are trying to use other methods with the DCT, as in Shieh et al. [34] who used DCT-based GA-watermarking. Also, Abraham and Paul [36] used the mid frequency coefficients for the watermark integration. Nandini, and Divya [37] merged different methods, like DCT, DWT and FFT, to utilize the wavelet transformation on an image, which is going to be de-composed to group of the components that have limited bands that may be re-arranged for the construction of the original image with no errors. Hamidi et al. [39] merged DCT with the DWT and SIFT. All of that ensures robustness against attacks.

4.3 DWT

Hsu and Wu [40] proposed a system of wavelet watermarking in which a binary logo was incorporated as a watermark that used the image 'peppers' of size 512x512. The watermark was inserted in the wavelet sub-bands' mid frequency add-ons. This strategy was a defense against the most prevalent snapshot processing attack. Its resistance to geometric aberrations isn't even mentioned. The challenge was that it was non-blind, requiring the use of a normal photograph to detect the presence of the watermark.

Lu and Liao [41] proposed a novel multipurpose watermarking scheme, in which robust and fragile watermarks are simultaneously embedded, for copyright protection and content authentication. The technique uses grayscale and binary images. The watermark was embedded using all of the coefficients from the LL, HL, LH, and HH sub bands at all four levels. This was shown to be sufficient against several attacks, and the performance is indeed superb in terms of

robustness and fragility. The degree of fragility was verified using the gray-scale "MonaLisa" image, size 256x256, and the beach image, size 512x512.

Ray-Shine et al. [42] proposed two methods which are the main components of the watermark are embedded into the original image using discrete cosine transform (DCT), and those are embedded in the original image using discrete wavelets transform (DWT). Finding the appropriate scaling factors is done via particle swarm optimization (PSO). This improved the reliability, robustness and high performance. The images used in the experiments are of size 512x512 for the cover images and of size 256x256 for the watermark images.

Sonil [43] proposed a relational databases watermarking based on hybrid model optimization that used DWT for embedding and extracting watermarking and combined with watermarking optimization techniques based on Genetic Algorithm (GA)-Bacterial Foraging Algorithm (BFO). It employs a 5-level DWT for the spatial transform, resulting in a more precise watermark. The owner's identity is secured cryptographically and used as an embedded watermark. Both the watermark imperceptibility and watermark robustness requirements are considered and can improve the process of watermarking.

Bousnina et al. [44] proposed a multimodal biometric watermarking algorithm to protect and authenticate biometric data. It employs the DTCWT-DCT, which combines two domain transform techniques to integrate face and fingerprint modalities and insert the quantized spectral minutiae representation used as a watermark into the face image. Face images of size 512x512 pixels and fingerprint images of size 374x388 pixels were used for the experimental results.

Evsutin et al. [45] proposed the development of data-hiding strategies and algorithms in digital images to classify current problems and experiments in digital steganography and digital watermarking fields. It concentrates on recent works that demonstrate current research directions. This is the distinguishing trait that sets it apart from previously published review papers.

It was noticed that the DWT technique in frequency domain watermarking was less robust against cropping, scaling, and other transformations. The DWT technique is becoming more viable in recent years, and researchers are trying to attempt to utilize other strategies with the DWT. Ray-Shine et al. [42] used particle swarm optimization (PSO). Sonil [43] combined DWT with genetic algorithm (GA)-Bacterial foraging algorithm (BFO) based optimization techniques for watermarking. Also, Bousnina et al. [44] used a multimodal biometric watermarking algorithm to ensure and well verify biometric information.

4.4 SVD

Dili and Mwangi [46] proposed SVD and wavelet be used to construct an image watermarking system. A reliable image watermarking approach that embeds a binary picture in the singular values of particular blocks of DWT in the vertical and horizontal sub bands of a gray-scale image's 1-level decomposition. To improve imperceptibility, the embedded blocks are picked using a secret key. It can withstand attacks like cropping, gaussian noise, and low-pass filtering. It is also JPEG compression resistant. The results obtained by MATLAB simulation were noted to be independent of the test image. The test image is based on the 256x256 8-bit Lena test image and the watermark is a 16x16 binary image.

Mathew [47] proposed an SVD-based image watermarking system that uses non-fixed orthogonal bases and leverages D and U components for embedding watermarks. This provides the SVD with good accuracy, robustness, and imperceptibility in determining who owns a watermarked image. A set of gray scale images of size 512×512 were chosen as input images, such as Barbara, Lena and Liftingbody images. A 32x32 jpeg image is used as a watermark image.

Loukhaoukha [48] proposed a watermarking method based on Lifting Wavelet Transform (LWT) and Singular Value Decomposition (SVD) applying Multi-Objective Ant Colony Optimization (MOACO). The binary values of the watermark are embedded in a detailed subband of the host image. An ant colony-based multi-objective optimization method is applied. According to experimental data, this outperforms other watermarking schemes in terms of transparency and robustness. Furthermore, to avoid the problem of a large probability of false positive watermark detections, computer simulations were run using the six 256×256 gray-scale test images and a 32× 32binary (black-and-white) watermark, Baboon, Boat, Cameraman, Lena, Man, Peppers, and letter A.

Zhang et al. [49] proposed the SVD-based watermarking scheme along with a study of the mathematical properties of SVD, and described a resilient image watermarking scheme, in which a binary watermark is inserted into the biggest singular value of each image block in the spatial domain. It has been resilient to a variety of attacks. It also avoids the problem of false positives and has a lower computational complexity. In the experiments, several grayscale images with a size of 512×512 were adopted as the host images, and the binary logo of Shandong University with a size of 64x64 was selected as a watermark image.

Begum [50] proposed different schemes in SVD that are used alongside several attacks, in terms of security and robustness. The SVD and homomorphic transform were used. The performance of this watermarking system was evaluated by normalized cross correlation (NCC), PSNR, and mean-structural similarity-index-measure (MSSIM) to ensure its resilience and invisibility.

Nguyen [51] proposed a fragile watermarking scheme for image authentication based on the combination of discrete wavelets transform (DWT), singular value decomposition (SVD), and discrete cosines transform (DCT). The feature coefficients are retrieved and employed in the quantization index modulation (QIM) process to embed the authentication code. The Gram-Schmidt procedure is used to change the feature coefficients to ensure that the derived authentication code is correct. The testing findings show that the system produces high-quality watermarked images and delivers excellent tamper detection accuracy under a variety of attacks, including direct cropping and object insertion attacks. Five 512 × 512 images were used to illustrate the performance of the proposed scheme.

It was noticed that the SVD technique in frequency domain watermarking was not robust against rotation and scaling, the low capacity of data embedding, and major changes in singular values led to small changes in the image. The SVD technique has shown much improved performance in recent years in terms of robustness compared to other watermarking techniques and provides good quality watermarking. Non-fixed orthogonal bases are used in Mathew [47], giving the SVD good accuracy, robustness, and imperceptibility. Loukhaoukha [48] used SVD and Lifting Wavelet Transform (LWT) utilizing Multi-Objective Ant Colony Optimization (MOACO) and showed considerable improvement in the performance concerning robustness and transparency. SVD and homomorphic transform were employed in Begum [50]. Nguyen

[51] combined SVD with DCT and DWT to create high-quality watermarked photos with high tamper detection accuracy.

4.5 Attacks on Watermarking

The main purpose of watermarking techniques is to prevent attacks. Since, no watermarking technique has been discovered that can withstand all types of digital media attacks [52] and [53]. A strong watermarking technology has a lot of potential. Gonge et al. [54] proposed a combination of DCT-SVD techniques for watermarking with an advanced encryption algorithm for the security of digital image against various attacks. Soualmi et al. [55] proposed digital watermarking based on the DCT transform with an Arnold chaotic map which can improve the robustness against several scenarios of attacks. Allaf and Kbir [56] proposed watermarking techniques in medical images, and also offered the general scheme of watermarking with the two essential phases and different types of attacks. Jialing et al. [57] proposed a watermarking method based on analysis of original image and a genetic algorithm that can significantly increase the image quality, security, and robustness of the watermarked image. Aside from that, it had a significant impact on transparency and robustness. In addition, Megalingam et al. [35], Abraham and Paul [36], Ko et al. [38], Hamidi et al. [39], Hsu and Wu [40], Lu and Liao [41], Mathew [47], and Loukhaoukha [48] have all mentioned it

5. Discussion

The review shows that in the spatial domain watermarking is resistant to attacks such as cropping, noise, and lossy compression in the spatial domain. However, a pixel-by-pixel attack can entirely reveal the watermark, which is the system's fundamental flaw. The key advantages of LSB-based approaches are that they are conceptually simple and have very low computing complexity, making them popular in picture watermarking applications where real-time speed is crucial. Several methods about LSB were mentioned, as well as attempts to combine them with others, such as using the third and fourth LSB or Adaptive LSB in order to make watermarking systems more resilient against attacks over time, to improve the quality of the watermarked image to assess the integrity of digital images, and to secure watermarks without altering or forging. Frequency domain (DCT, DWT, SVD) watermarking techniques are more robust than spatial domain watermarking techniques because information can be spread across the entire image. In the frequency domain, DCT-based techniques provide robustness against low-pass filtering, brightness and contrast modification, and blurring, but they are more difficult to design and more expansive. Geometric attacks such as rotation, scaling, and cropping are not resistant to DCT. The DWT, on the other hand, embeds the watermark in high-frequency sub-bands, making it more undetectable, while putting it in low-frequency sub-bands makes it more impervious to attacks. Filtering, lossy compression, and geometric distortions do not affect watermarks encoded with the wavelet transform. In the SVD the mathematical background of this method is very clear, and the error between the original image and the watermarked image can be estimated. How to establish the location of the watermark? and how much energy to insert? These questions can be answered easily. Other unitary transformations, unlike DCT and DWT, use fixed orthogonal bases. The SVD uses non-fixed orthogonal bases. It is a one-way, non-symmetrical decomposition. DCT, DWT, and SVD techniques have been getting more effective in recent years. Researchers are trying to combine other methods, as in using DCT-based GA-watermarking. They also used the mid-frequency coefficients for the watermark integration. Besides merging different methods with the DCT, like DWT and FFT, the also merged the DCT with DWT and SIFT. The DWT with particle swarm optimization (PSO) was used. Genetic algorithm (GA)-Bacterial foraging algorithm (BFO) based optimization methodologies also incorporate watermarking techniques. The SVD is used with lifting wavelet transform (LWT) and multi-objective ant colony optimization (MOACO). All of this assures

security against attacks and demonstrates significantly improved transparency and robustness. These characteristics contribute to the innovative algorithm's high security and robustness. (Table 1) shows the comparison between spatial and frequency domain watermarking.

Table 1: comparison between spatial domain and frequency domain watermarking

Criteria	Spatial domain watermarking	Frequency domain watermarking
Computational complexity	Simpler in implementation	Difficulties in implementing
Robustness	Low robust against attacks	More robust against attacks
Perceptual quality	High control	Low control
Computational time	Taken less time	Taken more time
Capacity	High, depends on the size of the host image	Low, depends on the size of the subband
Application	Mainly authentication	Copy rights

6. Conclusion

This paper provides a technical overview of many types of digital watermarking systems. It thoroughly discusses the most significant approaches, including LSB, DCT, DWT, and SVD, and will be useful in future studies. It provides a listing and presenting useful data concerning the challenges of image watermarking methods and attacks. Watermarking techniques' robustness can be improved in the future by using different robust features and appropriate embedding approaches. It is necessary to build techniques that are genuinely transparent, secure, and strong. Several optimization strategies can be used to locate watermark imbedding locations.

References

[1] S. A. Kadhim," A Proposed Watermark Approach for Uncompressed Digital Audio," *PhD. thesis, University of Technology, Computer Science Dept.,* 2017.

[2] N. F Hassan, et al., "Review: Video Watermarking, Theories and Robustness Issues," *Journal of Al-Ma'moon College*, vol. 36, pp. 355-394. 2021.

[3] R. A. Azeez, et al. "Design a System for an Approved Video Copyright over Cloud Based on Biometric Iris and Random Walk Generator Using Watermark Technique," *Periodicals of Engineering and Natural Sciences (PEN),* vol. 10, no. 1, pp. 178-187, 2021.

[4] N. F Hassan, et al. "Video Mosaic Watermarking Using Plasma Key," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 22, no. 2, 2021.

[5] F. G. Mohammed and H. M. Al-Dabbas," The Effect of Wavelet Coefficient Reduction on Image Compression Using DWT and Daubechies Wavelet Transform," *Science International*, vol. 30, no. 5, pp.757-762, 2018.

A. Preeti, et al. "A Review on Different Digital Watermarking Techniques," *International Journal of Signal Processing, Image Processing and Pattern Recognition,* vol. 8, no. 10, pp. 129–136, 2015.

[6] N. Deshpande, et al. "Implementation of LSB Steganography and Its Evaluation for Various Bits," *IEEE Xplore,* pp. 173-178, 2007.

[7] A. Mohanarathinam, et al. "Digital Watermarking Techniques for Image Security: A Review," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 8, pp. 3221–3229, 2019.

[8] F. G. Mohammed and H. M. Al-Dabbas, "Application of WDR Technique with different Wavelet Codecs for Image Compression," *Iraqi Journal of Science*, vol. 59, no.4B, pp: 2128-2134, 2018.

[9] J. Cox, et al., "Digital Watermarking and Steganography," *ScienceDirect,* 2008.

[10] N. F. Hassan, "Proposed Algorithm for Digital Image Watermarking Survival against JPEG Compression," *Eng. & Tech. Journal*, vol.32, no.1, 2014.

[11] R. Arkadip, and S. Roy, "Recent Trends in Image Watermarking Techniques for Copyright Protection: A Survey," *International Journal of Multimedia Information Retrieval*, vol. 9, no. 4, pp. 249–270, 2020.

[12] S. J. Vaishali and R. G. Sachin, "Literature Review of Wavelet Based Digital Image Watermarking Techniques," *International Journal of Computer Applications*, vol. 31, no. 7, pp. 28–35, 2011.
[13] S. Agreste, et al. "An Image Adaptive, Wavelet-Based Watermarking of Digital Images," *Journal of Computational and Applied Mathematics*, vol. 210, no. 12, pp. 13–21, 2007,
[14] S. Kumar, et al. "A Recent Survey on Multimedia and Database Watermarking," *Multimedia Tools and Applications*, vol. 79, no. 27-28, pp. 20149–20197, 2020.
[15] C. Jin and S. W. Jin, "Wavelet Packets-Based Robust Blind Digital Watermark Scheme," *IEEE Xplore*, pp. 724-728, 2008.
[16] K. C. Rushit, and D. M. Gautam, "Digital Watermarking: Techniques, Applications, Attacks," *International journal of engineering development and research (IJEDR)*, vol. 1, no. 7, pp. 1-8, 2014.
[17] M. Kumar, and M. P. Malhotra, "Digital image watermarking: a review," *International Journal of Recent Research Aspects*, vol. 2, no. 2, pp. 137-142, 2015,
[18] A. Dixit, "A Review on Digital Image Watermarking Techniques," *Image, Graphics and Signal Processing*, pp. 56-66, 2017.
[19] N. Deshpande, et al., "Implementation of LSB steganography and Its Evaluation for Various Bits," *In proceeding of first International Conference on Digital Information Management*, pp. 173-178, 2006.
[20] T. S. Nguyen, "Fragile watermarking for image authentication based on DWT-SVD-DCT techniques," *Multimedia Tools and Applications*, pp. 25107-25119, 2021.
[21] S. Kumar, "A Recent Survey on Multimedia and Database Watermarking," *Multimedia Tools and Applications*, pp. 20149-20197, 2020.
[22] C. Song, et al., "Analysis of digital image watermark attacks," *In proceeding of seventh IEEE consumer communications and networking conference*, pp. 1–5, 2010.
[23] S. Kumar and A. Dutta, "A study on robustness of block entropy based digital image watermarking techniques with respect to various attacks," *IEEE International conference on recent trends in electronics, information & communication technology (RTEICT)*, pp. 1802–1806, 2016.
[24] S. Van, et al., "A digital watermark," *IEEE Proc Int Conf Image Process*, vol.2, no. 7, pp. 86–90. 1994.
[25] G. B. Rhoads, "Identification/authentication coding method and apparatus," *World Intellectual Property Organization*, vol. 7, pp. 14289-14298, 1995.
[26] S. C. Byun, et al. "A SVD-based fragile watermarking scheme for image authentication," *International Workshop on Digital Watermarking*, vol. 2613, pp. 170-178, 2002
[27] W. C. Yang, et al., "Applying public-key watermarking techniques in forensic imaging to preserve the authenticity of the evidence," *In proceeding of International Conference on Intelligence and Security Informatics. Springer*, pp. 1-15, 2008.
[28] A. Bamatraf, et al., "Digital watermarking algorithm using LSB," *In proceeding of international conference Computer Applications and Industrial Electronics (ICCAIE)*, pp. 155-159, 2010.
[29] M. G. Almutiri, "Digital Image Watermarking based on LSB Techniques: A Comparative Study," *International Journal of Computer Applications*, vol. 181, no. 26, pp. 0975 – 8887, 2018.
[30] S. S. Roy, et al, "On the implementation of a copyright protection scheme using digital image watermarking," *Multimedia Tools and Applications*, pp. 13125-13135, 2020.
[31] E. Koch, and J. Zhao, "Towards robust and hidden image copyright labeling," *IEEE Workshop Nonlinear Signal Image Process*, vol. 1, pp. 123–132. 1995.
[32] A. G. Borg and I. Pitas, "Image watermarking using DCT domain constraints," *In Proceedings of 3rd IEEE International Conference on Image Processing (INSPEC)*, vol. 5591048, pp. 1-7, 1996.
[33] C. S. Shieh, et al., "Genetic watermarking based on transform-domain techniques," *Pattern Recognition* vol. 37, no. 3, pp. 555–565, 2004.
[34] R. K. Megalingam, et al., "A Comparative Study on Performance of Novel, Robust Spatial Domain Digital Image Watermarking with DCT Based Watermarking," *International Journal of Computer Theory and Engineering*, vol. 2, no. 4, pp. 1793-8201, 2010.
[35] J. Abraham and V. Paul, "Image Watermarking using DCT in Selected Pixel Regions," *In proceeding of International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT) IEEE*, pp. 1- 7, 2014.

[36] D. Nandini, and S. Divya, "A Literature Survey on Various Watermarking Techniques," *International Conference on Inventive Systems and Control (ICISC) IEEE*, pp. 1-8, 2017.
[37] H. J. Ko, et al. "Robust and Blind Image Watermarking in DCT Domain Using Inter-Block Coefficient Correlation," *Information Sciences*, vol. 517, pp. 128–147, 2020,
[38] M. Hamidi, et al. "A Hybrid Robust Image Watermarking Method Based on DWT-DCT and SIFT for Copyright Protection," *Journal of Imaging*, vol. 7, no. 10, 2021.
[39] C. T. Hsu, and J. L. Wu, "Multi-resolution watermarking for digital images," *IEEE Trans Circ Syst II Analog Dig Signal Process*, vol. 45, no. 8, pp. 1097–1101, 1998.
[40] C. S. Lu and H. Y. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans Image Process*, vol. 10, no. 10, pp. 1579–1592, 2001.
[41] R. Ray-Shine, et al., "An improved SVD-based watermarking technique for copyright protection," *Expert Systems with Applications*, vol. 39, no. 1, pp. 673-689,2012.
[42] S. Sonil, "Digital Watermarking Using Hybridization of Optimization Techniques: A Review," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 4, 2014.
[43] N. Bousnina, et al. "DTCWT-DCT Watermarking Method for Multimodal Biometric Authentication," *In proceedings of the 2nd International Conference on Networking, Information Systems & Security - NISS19*, pp. 1-12, 2019.
[44] O. Evsutin, et al. "Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions," *IEEE Access*, vol. 8, pp. 166589–166611, 2020,
[45] R. Dili and E. Mwangi, "An image watermarking method based on the singular value decomposition and the wavelet transform," *IEEE AFRICON*, pp 1–5. 2007.
[46] D. Mathew, "SVD based Image Watermarking Scheme," *Evolutionary Computation for Optimization Techniques* (*ECOT)*, 2010.
[47] K. Loukhaoukha, "Optimal Image Watermarking Algorithm Based on LWT-SVD via Multi-Objective Ant Colony Optimization," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 4, 2011.
[48] H. Zhang, et al., "A Robust Image Watermarking Scheme Based on SVD in the Spatial Domain," *Future Internet*, pp. 1-17, 2017.
[49] M. Begum and S. Mohammad, "Digital Image Watermarking Techniques: A Review," *Information*, vol. 11, no. 2, 2020.
[50] T. S. Nguyen, "Fragile Watermarking for Image Authentication Based on DWT-SVD-DCT Techniques," *Multimedia Tools and Applications*, vol. 30, pp. 25107–25119, 2021.
[51] N. A. Hamza, et al., "Encrypt 3d model using transposition, substitution, folding, and shifting (tsfs)," *In proceeding of 2nd Scientific Conference of Computer Sciences*, pp 126-130, 2019.
[52] M. E. Abdulmunem and A. B. Ameer, "Fragile Audio Watermark Based on Empirical Mode Decomposition for Content Authentication.," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2017.
[53] S. S. Gonge and A. Ghatol, "Composition of DCT-SVD image watermarking and advanced encryption standard technique for still image," *In proceeding of the international symposium on intelligent systems technologies and applications*, pp 85–97. 2016
[54] A. Soualmi, et al, "A new blind medical image watermarking based on weber descriptors and Arnold chaotic map," *Arab J Sci Eng.*, vol. 43, no. 12, pp. 7893–7905, 2018.
[55] A. H. Allaf and M. A. Kbir, "A review of digital watermarking applications for medical image exchange security," *In: The proceedings of the third international conference on smart city applications*, pp 472–480. 2018.
[56] H. Jialing et al., "A digital image watermarking method based on host image analysis and genetic algorithm," *J Ambient Intell Hum Comput*, vol. 7, no. 1, pp. 37–45, 2016.