information

MDPI

Review

Digital Image Watermarking Techniques: A Review

Mahbuba Begum [1,*] and Mohammad Shorif Uddin [2]

[1] Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Tangail-1902, Bangladesh
[2] Department of Computer Science and Engineering, Jahangirnagar University, Savar, Dhaka-1342, Bangladesh; shorifuddin@gmail.com
* Correspondence: mahbuba327@yahoo.com

Received: 11 January 2020; Accepted: 13 February 2020; Published: 17 February 2020

Abstract: Digital image authentication is an extremely significant concern for the digital revolution, as it is easy to tamper with any image. In the last few decades, it has been an urgent concern for researchers to ensure the authenticity of digital images. Based on the desired applications, several suitable watermarking techniques have been developed to mitigate this concern. However, it is tough to achieve a watermarking system that is simultaneously robust and secure. This paper gives details of standard watermarking system frameworks and lists some standard requirements that are used in designing watermarking techniques for several distinct applications. The current trends of digital image watermarking techniques are also reviewed in order to find the state-of-the-art methods and their limitations. Some conventional attacks are discussed, and future research directions are given.

Keywords: LSB; DCT; DFT; DWT; SVD

1. Introduction

Image processing and the internet have made it easier to duplicate, modify, reproduce, and distribute digital images at low cost and with approximately immediate delivery without any degradation of quality. Network technology has been developing and progressing so quickly that it threatens the privacy and security of data. Therefore, content authentication, copyright protection, and protection against duplication play an essential role in facing the challenges of the existing and upcoming threats in maintaining digital information. Digital image watermarking is simply the digital watermarking of an image, which provides an alternative solution for ensuring tamper-resistance, the ownership of intellectual property, and reinforcing the security of multimedia documents. Any digital content, such as images, audio, and videos, can hide data. Digital content can easily be illegally possessed, duplicated, and distributed through a physical transmission medium during communications, information processing, and data storage. Digital image watermarking is a technique in which watermark data is embedded into a multimedia product and, later, is extracted from or detected in the watermarked product. These methods ensure tamper-resistance, authentication, content verification, and integration of the image [1]. It is not very easy to eliminate a watermark by displaying or converting the watermarked data into other file formats. Therefore, after an attack, it is possible to obtain information about the transformation from the watermark. To discern the difference between digital watermarking and other technologies such as encryption is essential [2]. Digital-to-analog conversion, compression, file format changes, re-encryption, and decryption can also be survived through digital image watermarking techniques. These tasks make it an alternative (or complementary) to cryptography. The information is embedded in the content and cannot be removed by normal usage [3].

The word "steganography" is derived from the Greek word "steganos." This technique conceals communication and changes an image such that only the sender and the intended receiver can identify

the sent message. This technique makes detection a more difficult task. Instead of encrypting messages, steganography can be used to hide them in other inoffensive-looking objects, so their existence is not discovered and, therefore, can be used as an alternative tool for privacy and security. However, due to the rapid proliferation of internet and computer networks, steganography can be used as a tool for exchanging information and planning terrorist attacks [3]. Steganography hides the existence of a cover image, while a watermarking technique embeds a message into the actual content of the digital signal within the signal itself. Therefore, an eavesdropper cannot remove or replace a message to obtain an output message. To protect content from unauthorized access, embedding information into the original image is essential. Digital image watermarking is imperceptible and hard to remove by unauthorized persons. The technique has been implemented by various algorithms using the spatial and frequency domains, each having their distinct benefits and boundaries. The contributions of this research are as follows:

- We identify the limitations of existing watermarking techniques;
- We present the current trends of image watermarking techniques;
- We investigate the techniques that meet some of the requirements of image watermarking techniques perfectly;
- We point out the challenges that must be addressed by future researchers.

In this paper, the framework of general watermarking methods, separated into the processes of embedding and extracting watermarks, along with a general background, is shortly revised in the first section. Some standard design requirements for evaluating the performance of watermarking systems are listed in the following subsections. Related applications that make watermarking systems a highly focused research area are also described. Based on the working domain, a survey of digital image watermarking techniques is subsequently presented. Then, a summary of the research results of the discussed state-of-the-art methods and current trends in the field is described in tabular format. Next, we list some conventional attacks or threats which must be treated as a challenge for designing an efficient system. Performance metrics, such as peak-signal-to-noise ratio (PSNR), structural similarity index (SSIM), mean squared error (MSE), and normalized cross-correlation (NCC), are also briefly described. Finally, the last section concludes the study.

2. Image Watermarking Backgrounds and Frameworks

At present, digital content can be spread easily through communication channels due to the rapid rise of global computer networks, the internet, and multimedia systems. To protect digital information against illegal possession, duplication, manipulation, usage, and distribution through physical transmission media during communications, information processing, and data storage, digital image watermarking makes it possible to construct a platform for researchers by considering it as a research area.

Paper watermarks began as early in 1282 and, therefore, digital watermarking techniques have been improved by integrating paper configuration, quality, and quantity considerations. Watermarking has been used broadly for enhancing security [4]. The computerized technology of digital watermarking appeared in 1988, providing confidentiality, integrity, and availability, and various innovations regarding digital image watermarking have been incorporated since 1995. In watermarking techniques, a symbol of owner authenticity (watermark) is embedded into the host signal and, later, this watermark data can be extracted. The watermark data, which may be visible or invisible, can contain a single bit, a set of binary data, or a number of samples in the host signal [5].

To imitate the human visual perception system, information entropy plays an essential role in the digital image watermarking scheme. To achieve an optimal balance between imperceptibility, robustness, and capacity of a digital image watermarking technology, information entropy can be used through a Just Noticeable Difference (JND) model [6]. Information entropy can be defined in terms of masking effect and can be utilized to determine the positions at which the data are inserted. This

scenario minimizes perceptual distortion and gives better robustness and good imperceptibility. The entropy of a system with n states can be defined by the following equations [7]:

Information Entropy,

$$ETP = -\sum_{i=1}^{n} P_i \, logP_i \tag{1}$$

where $0 \leq P_i \leq 1$ and

$$\sum_{i=1}^{n} P_i = 1 \tag{2}$$

where P_i denotes the probability of occurrence for the event i.

For the secured communication of a message, the process begins with a cover image (host image). The host image can be considered purely as noise, noise with side information, or as a multimedia message that must be transmitted. The watermarked data passes through a communication channel, which may be lossy, noisy, or unreliable. Hence, the watermarked data may suffer from possible attacks, including lossy compression, geometric distortion, signal processing operations, and signal conversion, among others; that is, there may be a difference between the original watermarked data and the received data [8]. A watermarked image passes through a communication channel, which incurs noise. This noise maximizes the information entropy [9], which increases the uncertainty or ambiguity of the average information contained in an image. Watermarking techniques can, thus, only be applied to high-resolution and complex-patterned images that have higher information entropy. Therefore, to improve security, the encoded image must be processed such that the image reconstruction will be robust. A new optical image encoding method obtains the encoded image by a random-phase encoding technique in both the input and the Fourier planes [10], in which the two random phase plates at the input and the Fourier planes are replaced by two deformable mirrors, respectively. Thus, the system can achieve arbitrary beam shaping in the amplitude and phase information of the image [11].

For a secure communication model, the digital image watermarking process consists of a watermark embedding part and a watermark extraction part. In the watermark embedding part, at first, the cover image is pre-processed, and then, its entropy is evaluated to find the integrating capacity information of the image. Then, using an optical image encoding method, the encoder embeds a watermark image into the high entropy value of the host image by using a secret key. Then, the system achieves the amplitude and phase shaping information of a laser beam and generates the watermarked image. The watermark embedding part is depicted in Figure 1a. Finally, in the watermark extraction step, the watermarked image is pre-processed. After that, the system extracts the amplitude and phase shaping information of the laser beam patterns. Then, the entropy of these beam patterns is evaluated. A high entropy value is selected for extracting the watermark, in order to ensure better robustness and imperceptibility. A decoder detects the watermark image as output from the watermarked image using the same key, as depicted in Figure 1b. The system demonstrates that image reconstruction of the watermark image from the watermarked image is simple, robust, and imperceptible.

The watermark embedding process generates a watermarked image, D_W, which can be described by the following function:

$$Watermarked\ Image,\ D_W = E(I,\ ETP, W,\ K), \tag{3}$$

where E is the encoding algorithm, I is the cover image, ETP is the information entropy, W is the watermark image, and K is the security key.

The watermark extraction process extracts the watermark image, W', which can be described by the following decoder function, where $e(.)$ is the decoding algorithm:

$$W' = e\ (D_{W,}\ K,\ ETP,\ I). \tag{4}$$

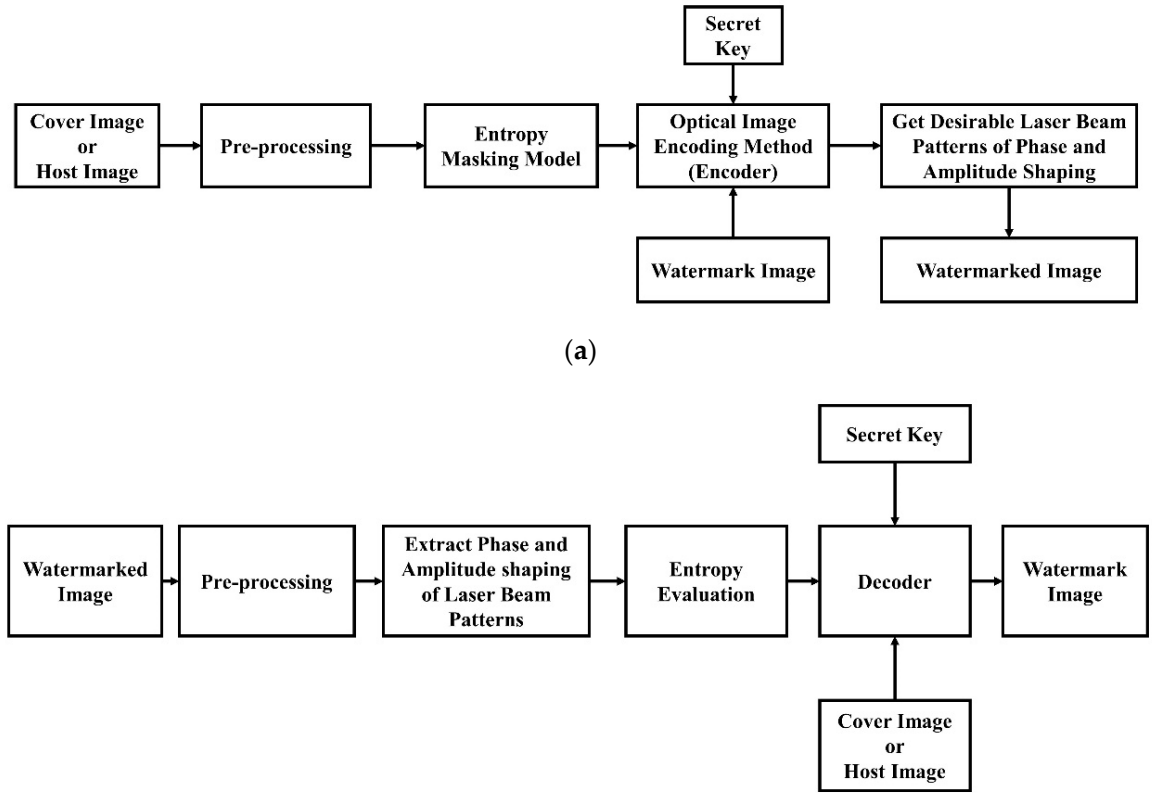

Figure 1. (**a**) Watermark embedding and (**b**) watermark extraction.

3. Design Requirements of Image Watermarking System

Digital image watermarking techniques add a watermark into multimedia data to ensure authenticity and to protecting a copyright holder from the unauthorized manipulation of their data [12]. Hence, it is necessary to define the requirements or characteristics of a watermarking system, which are listed in the following subsections. Figure 2 illustrates the requirements of watermarking techniques. Based on applications, these requirements evaluate the performance of watermarking systems.

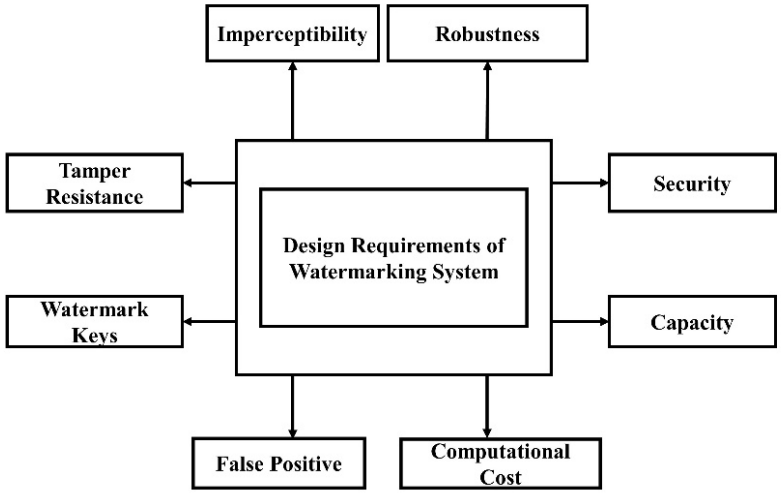

Figure 2. Design requirements for an image watermarking system.

3.1. Imperceptibility

Imperceptibility is key in evaluating the performance of a watermarking system. It is represented by invisibility and fidelity. In this case, the watermarked image must appear the same as the original image. They should be perceptually indistinguishable to humans, despite a minor degradation in brightness or image contrast. Thus, the image quality must not be affected. There are different methods for evaluating the imperceptibility of a watermarking system. Yang et al. [13] have proposed a new method based on the masking features of the human visual system. Their proposed method, Masking-based Peak Signal to Noise Ratio (MPSNR), performed better in evaluating the imperceptibility of watermarking systems. Their experimental results showed that higher masking strength provides less quality degradation in the watermarked image. For improving watermark imperceptibility, larger singular values are selected for inserting the watermark image, based on watermark capacity [14]. In this regard, the structural similarity index (SSIM) is used to evaluate watermark imperceptibility. The quality of the watermarked image may be lost due to the watermark embedding process. However, in invisible watermarking, it is often unnoticeable by the human visual system. High peak-signal-to-noise ratio (PSNR) results imply better imperceptibility. The best watermarking techniques ensure better imperceptibility, meaning that they generate no visual difference between the host image and the watermarked image. One method [15] selects the best region of the cover image for watermark insertion to achieve better imperceptibility. A visible watermark in an image is sometimes preferred [16]. However, invisible watermarking systems are more popular. Imperceptibility may be used in digital imaging, telemedicine, digital documents, and so on.

3.2. Robustness

Robustness is the requirement that a watermark is able to be detected after some common signal processing manipulation operations in digital image watermarking systems have been applied. These operations include spatial filtering, color mapping, scanning and printing, lossy compression, scaling, translation, and rotation. They also include other operations, such as analog to digital (A/D) conversions, digital to analog (D/A) conversions, image enhancement, cutting, and so on [2]. There exist several general approaches to achieving high robustness, such as redundant embedding, spread spectrum, and embedding watermarks, among others. Therefore, a good digital image watermarking system should be robust against various attacks, such that unauthorized distributors cannot remove or exclude watermark data. Depending on the application, not all watermarking algorithms may have robustness at the same level. Some are robust against different image processing operations, while some fail against other attacks [17]. Therefore, robustness can be classified into robust, fragile, and semi-fragile.

- Robust: A robust watermark prevents various noisy attacks, as well as geometric or non-geometric attacks, without altering the watermark data. The watermark remains the same even after some attacks and provides authorization by detecting the watermark [18]. This watermark is used in such areas as copyright protection, broadcast monitoring, copy control, and fingerprinting [16].
- Fragile: Fragile watermarks are mainly used for integrity verification and content authentication of multimedia data where signature information can be added. This watermark validates whether it has been tampered or not [16]. A fragile technique is typically easier to implement than a robust one [19]. In [20], binary authentication information was inserted into the host image where, for identifying tampering and localization, a pixel-based fragile watermarking technique was used. It resulted in an acceptable visual effect (in terms of the human eye).
- Semi-fragile: This type of watermark resists some transformations but fails after malicious transformations. A semi-fragile watermark can be used for image authentication [21].

An all phase bi-orthogonal transform (APBT) and Singular Value Decomposition (SVD)-based algorithm has been proposed [22] to achieve better robustness and imperceptibility of the watermarking

system, where the block-based APBT algorithm is applied in a certain neighborhood obtained by selected candidate feature points. The coefficients of APBT generate the coefficient matrix for SVD to embed the watermark. Furthermore, a Discrete Wavelet Transform (DWT), all phase discrete cosine biorthogonal transform (APDCBT), and SVD-based method has been proposed [23] to enhance the imperceptibility and robustness, where the direct current (DC) coefficients of high-frequency sub-bands (LH and HL) are used to insert a watermark image. This method has been shown to be robust against many signal processing operations.

3.3. Security

Watermarking algorithms that are not secure cannot be applied in copyright protection, data authentication, fingerprinting, and tracking of digital content. Therefore, security is a significant concern in digital image watermarking techniques. Security can be confirmed by various encryption methods, where the key decides the degree of security. Several methods, such as chaos-based, Discrete Cosine Transform (DCT), and logistic map-based encryption techniques, have been used to ensure the security and confidentiality of the embedded watermark [24]. The security of functional magnetic resonance imaging (fMRI) images is important, as they are related to brain activities. A watermarking method has been proposed for ensuring the integrity and authenticity of fMRI images [25], where a fragile reversible watermarking scheme was introduced to characterize fMRI images which are free from any format. The scheme is not dependent on using external metadata. In [26], binary pseudo-random sequences were used to encrypt the watermark before embedding, enhancing the security of the watermarking algorithm. The security requirement can be applied in telemedicine, digital imaging, telecommunications, multimedia data, etc.

3.4. Capacity

Watermarking capacity (also known as payload) evaluates how much information can be inserted into the host image, based on the size of the original data. The capacity is defined by the number of bits carried by each host image after inserting the watermark image. However, it is a difficult task to insert more watermark information, which needs a pre-requisite based on practical applications [1]. In other words, the capacity determines the limitations of the watermarking information while satisfying watermarking robustness and imperceptibility. The available information to attackers, data encoder and decoder, distortion constraints, and the statistical model used in the cover image determine the watermarking capacity [27]. Various methods exist for evaluating watermarking capacity problems under attacks. These include game-theoretic and parallel Gaussian channels (PGC) approaches.

On the other hand, watermark extraction is successful only when the channel capacity is higher than the number of bits that are embedded into the host image [28]. The watermarking capacity has been defined by the probability of detection, the probability of false alarm, and the mean square error. When more watermark data is inserted into the host image, more distortion is visible. However, distortion is not tolerable in military and medical applications. Watermarking techniques, therefore, must be implemented to minimize the distortion with less data embedding capacity. In this regard, the combination of IWT (Integer wavelets transform), the bit-plane method, and a QR (Quick Response) code has been proposed [29], where the watermark is converted into a QR code. Thus, the proposed method reduces the embedding capacity.

3.5. Computational Cost

The computational cost for embedding a watermark into a host image and extracting the watermark from the watermarked image should be minimal. This cost includes two main issues—the total time required for embedding and extracting the watermark, and the total number of embedders and detectors involved in the watermarking technique. A good trade-off between robustness and computational complexity must be maintained. It has been implemented in reference [30] to ensure the security and robustness of microscopy images.

3.6. False Positive

The false positive rate is the characteristic used to identify watermarks in an image where there is no watermark image. This problem occurs when the embedded watermark is different from the extracted watermark [31]. The test has been carried out by various schemes. This characteristic has mainly been used for copy control and ownership. If a watermark image W has length l and the extracted watermark is W', then the false positive rate (FPR) is defined by the following equation [32]:

$$FPR = \frac{l'}{l} \tag{5}$$

where l' is the Hamming distance of W and W'.

3.7. Watermark Keys

The watermark key is the secret key that determines certain parameters of the embedding function. This key includes the subset of image coefficients, the embedding direction, and/or the embedding domain. The estimation and mapping of the watermark key are important, as it determines the degree of security of the watermarking system and depends on certain parameters, such as the embedded message and watermarked image [33]. Therefore, for the embedding and extraction process, a secret key is needed to ensure security. The secret key includes a private key, a detection key, and a public key. The private key is available only to the user, the detection key is acknowledged in a court of law, and the public key is extracted by the public [34]. A study by Chopra et al. [35] used an Exclusive OR operation for the watermark key, such that that the system inserts the watermark into a defined location in the biometric signature template. The locations for different images are different from each other. This characteristic reduces the probability of the occurrence of various attacks. Therefore, the robustness of the system is increased.

3.8. Tamper Resistance

Tamper-detection in the watermarking system can be used to check authenticity. Any change to the watermark data results in tampering of the image. Therefore, by testing integrity, the system determines whether the watermark data has been tampered or not [36].

3.9. Reversibility

The reversibility characteristic ensures the extraction of the watermark and exact reconstruction of the host image. However, for medical imaging, the modified image is used as a host image and the reconstructed image is used for diagnosis [37]. In the reversible digital watermarking method, the system takes the original image and obtains the watermarked image. Then, with the help of the extraction algorithm, the system recovers the original image and watermark image using the secret key.

3.10. Techniques that Meet Requirements Simultaneously

From the above discussions, it can be summarized that it is impossible to satisfy imperceptibility, robustness, and capacity simultaneously due to their conflicting and limited characteristics [1]. For any watermarking system, imperceptibility may be decreased by increasing the properties of robustness and capacity, and vice versa [38]. On the other hand, robustness may be decreased by increasing the payload capacity. Therefore, a good trade-off among these types of requirements must be maintained. The trade-off among these three requirements is illustrated in Figure 3 [39].

However, there is no unique set of properties that are satisfied by all watermarking systems. Currently, some techniques exist that meet some of the above-discussed requirements simultaneously. These techniques are shown in Table 1. For example, in [40], a DCT, DWT, and SVD-based study, based on multiple watermarking techniques for securing online social network content, was proposed. A three-level DWT was applied to the host image for embedding the watermark, and a back-propagation

neural network (BPNN) algorithm was applied to the extracted watermark image to minimize the distortion between the host image and the watermarked image. Thus, the robustness of the system was enhanced. For increasing security, multiple watermarks were embedded into the host image by using a selective encryption method. The experimental result showed superior performance over existing methods. In another study [41], a DCT, DWT, and SVD-based algorithm was proposed, which used multiple watermarking to ensure robustness, imperceptibility, capacity, and security simultaneously. To enhance security, the Arnold transform was applied to the host image before embedding. The quality of the watermarked image was satisfactory for diagnosis, in terms of human perception. Thus, the system ensures better imperceptibility at different gain factors. Phadikar et al. [42] proposed a reversible watermarking technique for Digital Imaging and Communications in Medicine (DICOM) images. The watermark was embedded into the host image in the lifting-based DWT domain. The experimental results showed that the technique ensures high embedding capacity along with better imperceptibility and robustness.

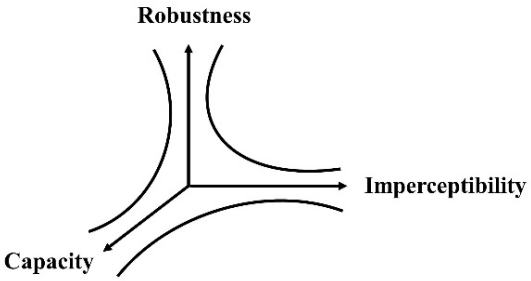

Figure 3. The trade-off among imperceptibility, robustness, and capacity.

Table 1. Techniques that meet some requirements simultaneously.

Used Techniques	Factors	Results	Applications
Hybrid transform domain and Particle Swarm Optimization (PSO) algorithm [15]	Imperceptibility and robustness	Performs better than existing methods	Image Authentication
APBT-based algorithm and SVD [22]	Imperceptibility and robustness	Better imperceptibility and good robustness	Authenticity and integrity of copyright protection
DWT, APDCBT, and SVD [23]	Imperceptibility and robustness	Performs better than existing methods	Copyright protection
Spatial domain technique [30]	Robustness and computational complexity	Guarantees of security and robustness	Protection of Microscopy Images
BPNN [40]	Robustness, security, and capacity	Better robustness and security	Protection of digital contents
DWT, DCT, and SVD [41]	Robustness, imperceptibility, capacity, and security	Acceptable visual quality for diagnosis	Healthcare
Lifting and companding [42]	Imperceptibility, capacity, and security	Performs better than existing reversible watermarking techniques	DICOM images

4. Digital Image Watermarking Applications

Digital image watermarking is a highly focused research area, due to its potential use in media applications such as copyright protection, annotation, privacy control, data authentication, device control, media forensics, and medical reports (e.g., X-rays). Some associated applications of digital image watermarking are shown in Figure 4.

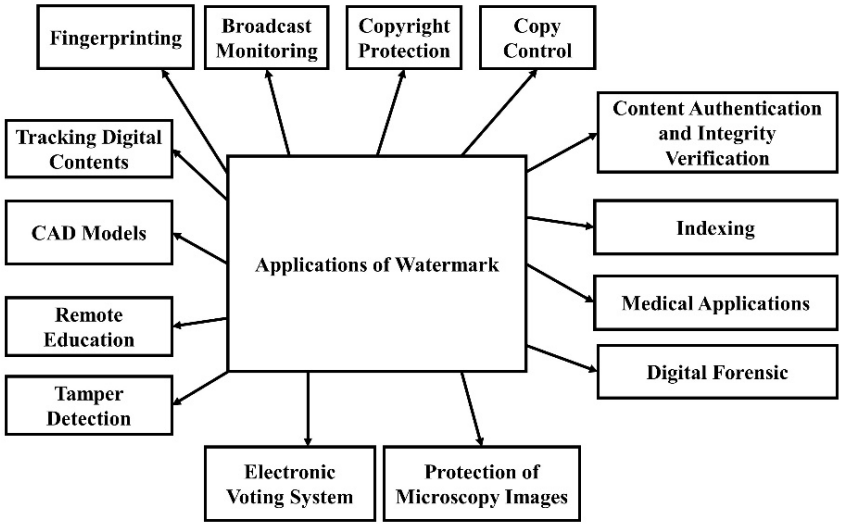

Figure 4. Related applications of digital image watermarking.

The identified applications, according to design requirements, are shown in Table 2.

Table 2. Design requirements and their corresponding applications.

Requirements	Applications
Imperceptibility	Copyright protection and fingerprinting.
Robustness	Copyright protection, content authentication, and integrity verification.
Security	Copyright protection, data authentication, fingerprinting and tracking to digital contents, indexing, medical applications, and telemedicine data exchange.
Capacity	Tamper detection and integrity of medical images.
Computational cost	Protection of microscopy images.
False positive	Copy control and ownership.
Watermark keys	Copyright protection.
Tamper resistance	Authenticity and copyright integrity.
Reversibility	Medical applications.

Some important and recent potential applications are described in the following subsections.

4.1. Broadcast Monitoring

This application allows a content owner to verify when and where the content was broadcast. It also checks for the exact airtime of broadcasting content through satellite television and transmission media. Before the broadcast, a unique watermark can be inserted into each sound or video clip [8]. It is useful for several organizations and individuals when advertisers want to ensure that the content is broadcasted at exact airtime agreed by the customer and the advertisement company [43]. This application can be used to ensure the legal transmission of TV products such as news items [44]. In broadcast monitoring, the broadcast monitoring service provides the watermark data to the studio. The watermark data is embedded into the host media using the watermark embedding algorithm and the secret key. Then, the watermarked data is used by the studio. Finally, the TV station transmits this watermarked data as a TV program [45]. The basic framework of broadcast monitoring is shown in Figure 5.

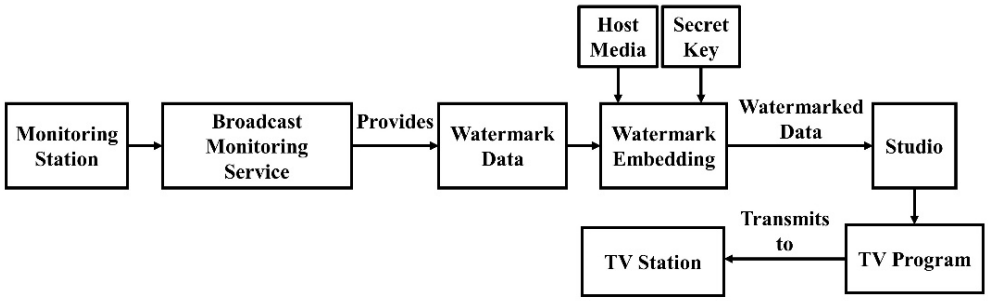

Figure 5. Broadcast monitoring using digital watermarking.

4.2. Copyright Protection, Ownership Assertion, or Owner Identification

In copyright protection (or copyright holder identity) applications, a visible watermark identifies the copyright owner and ensures the proper payment of royalties. In this case, the owner can protect multimedia data by making the ownership mark visible when being used commercially, if it is available on the internet [46]. An invisible and inseparable watermark is the best solution for identifying copyright ownership. This application proves ownership by extracting the embedded information from the watermarked document, compared to easily removable text marks. It requires strong robustness, such that the watermarked image cannot be removed without data distortion [44]. In reference [47], a fragile and robust watermark image was embedded into the host image for copyright protection and tampering detection. For copyright protection, the author's logo was inserted into the host image as a robust watermark. However, an attacker may try to remove the tough watermark. The experimental results showed that the proposed system could extract the tough watermark even when half of the image was cropped. Thus, the author's logo can be seen. A three-dimensional (3D) mesh watermarking scheme has been proposed by Hamidi et al. [48], which protects copyright information based on mesh saliency and a wavelet transform. Wavelet analysis was performed on the original 3D mesh and the wavelet coefficients were obtained using mesh saliency. The watermark data was inserted into the original 3D mesh using a quantization index modulation (QIM) technique and secret keys, and watermark extraction was done in a reverse manner. The method demonstrated better imperceptibility and good robustness. To ensure the secure storage and transmission of satellite imagery, digital image watermarking techniques play an important role. To ensure copyright protection, one study [49] proposed an SHA-3-based novel reversible invisible watermarking scheme, which uses the hash function and an adaptive prediction algorithm.

4.3. Copy Control and Finger Printing

Copy control prevents people from making illicit copies of content. In this regard, a watermark can be used to restrict copying by informing hardware devices or software. In copy protection, a pirate knows the status of hidden messages, which is the real threat. The message contains "Copy No More," "Copy Once," or "Copy Never." On the other hand, in fingerprinting or transaction tracking schemes, an innocent user cannot be framed by the collusion of pirates, and at least one pirate can be traced by the detector [50]. Similar to fingerprinting, which identifies an individual, transaction tracking uniquely identifies each copy of the work. The watermark accounts for the recipient of each legal dissemination of the work and it has been verified that invisible watermarking performs better, as compared to visible watermarking [51].

4.4. Content Authentication and Integrity Verification

Digital images can be modified with the help of widely available sophisticated image processing tools. For secure communication, information must be protected from unauthorized access—this property is known as integrity. A watermark verifies the authenticity of an image. Any significant modification of the image can also change the watermark. These changes can be detected [52], which

indicates that the data has been tampered with. The basic framework of content authentication and integrity verification is shown in Figure 6.

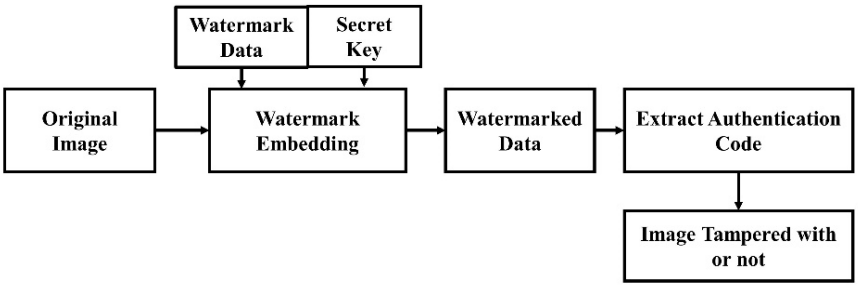

Figure 6. Content authentication and integrity verification.

In reference [53], a three-level image watermarking embedding technique has been proposed for integrity verification. The visible and invisible watermarks are embedded in the first two levels, respectively, and alpha channel watermarking in the third level is used for integrity verification. This scheme has been shown to detect the tampered regions successfully. Another study [54] has proposed a method which detects and localizes the tampered region. The experimental results demonstrated that the quality of the recovered image was high.

4.5. Indexing

This technique uses comments and markers or key information, which is embedded as a watermark into videos, movies, and news items. Then, the technique retrieves the required data used by the search engine [36].

4.6. Medical Applications

Image watermarking can be applied to protect the copyright of medical images. Patient's information can be protected from illegal access by watermarking techniques. These applications include medical imaging, telehealth, and telemedicine, among others. Medical imaging visualizes tissues, organs, or some other parts of the body, by using information and communications technologies. Telehealth involves telesurgery, telediagnosis, teleconferences, and other medical applications. Telemedicine connects specialists and patients separated by a physical distance [55]. Therefore, to ensure the confidentiality, authenticity, integrity, and availability associated with Electronic Patient Record (EPR) data exchange, suitable watermarking techniques can be used. In these applications, the image quality must not be affected by the watermark data [36].

4.7. Other Applications

Digital image watermarking can be used for proof of authenticity of the object's originator. Additionally, digital counterfeiting, fraud, identify theft, secured electronic voting, and deployable remote education, among many others, are all possible applications of digital image watermarking.

5. Survey on Digital Image Watermarking Techniques

Digital image watermarking has gained attention from researchers due to its availability and the delivery of redundant information. These techniques protect digital content from unauthorized access and manipulation. These techniques are required for different applications, such as authentication, operator acknowledgment, material security, and trademark protection. Digital image watermarking techniques can be classified based on the working domain, kinds of documents, nature of the algorithm, human perception, and type of application, as illustrated in Figure 7.

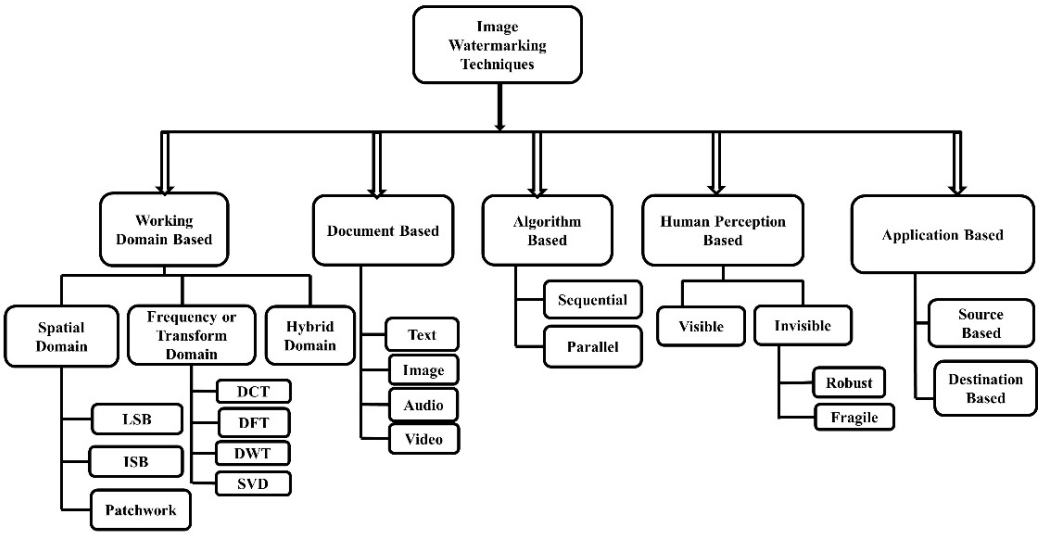

Figure 7. Classification of image watermarking techniques.

All digital image watermarking techniques depend on the type of working domain (i.e., spatial, frequency, or hybrid domain), type of documents (i.e., text, image, audio, or video), nature of the algorithm used (i.e., sequential or parallel), human perceptibility (i.e., visible or invisible), and type of application (i.e., source or destination-based). This section analyzes various digital image watermarking methods, based on the working domain, by summarizing some recent research results in this field. This section will be helpful for future studies on state-of-the-art watermarking methods.

5.1. Spatial Domain Watermarking Techniques

This technique inserts watermark information into the host image, as defined by the owner in the spatial or time domain, using different methods including least significant bit (LSB) modification algorithms, intermediate significant bits (ISB) or patchwork algorithms, and spread spectrum and correlation-based algorithms. These techniques work directly on the original image pixels. The watermark can be inserted by manipulating the pixel values, based on a logo or signature information provided by the author [17]. In the most commonly used designs, pixel intensities at known points in space represent the image, where the lowest-order bit of certain pixels in a color or grayscale image is flipped. Depending on the pixel intensity, the resulting watermark may be visible or invisible. We review various approaches regarding spatial domain techniques that have attracted the attention of researchers due to their optimal balance among imperceptibility, robustness, and capacity, which are the most important requirements of any watermarking technique. These techniques have low complexity, improved efficiency, and faster execution. Furthermore, the watermarked image quality may be controlled [56]. However, these techniques perform well only if the image is not exposed to any noise or human modification. Picture cropping can be used to exclude the watermark, which is a major weakness in spatial domain watermarking. These techniques embed a large volume of data, in terms of capacity, but the inserted data may be easily detected by various attacks [57–59]. Additionally, a small object can be inserted several times. Hence, a single surviving watermark will be considered an achievement, despite losing most of the image due to several attacks.

5.1.1. Least Significant Bit (LSB)

Least significant bit modification is the most commonly used algorithm for spatial domain watermarking. Here, the least significant bit (LSB) of randomly chosen pixels can be altered to hide the most significant bit (MSB) of another. It generates a random signal by using a specific key. The watermark is inserted into the least significant bits of the host image and can be extracted in the same way. Several techniques may process the host image. This type of algorithm is easy to implement and is

simple. The least significant bits carry less relevant information and, thus, the quality of the host image is not affected. It provides high perceptual transparency with a negligible impact on the host image. However, this algorithm can be affected by undesirable noise, cropping, lossy compression, and so on, and may be attacked by a hacker by setting all the LSB bits to "1," modifying the embedded watermark easily without any difficulty. The LSB technique can easily be understood by the example depicted in Figure 8. Suppose two pixel values in the host image are 130 (10,000,010) and 150 (10,010,110). Then, using the LSB technique, if the embedded watermark is 10, then the watermarked pixel values will be 131 (10,000,011) and 150 (10,010,110), respectively.

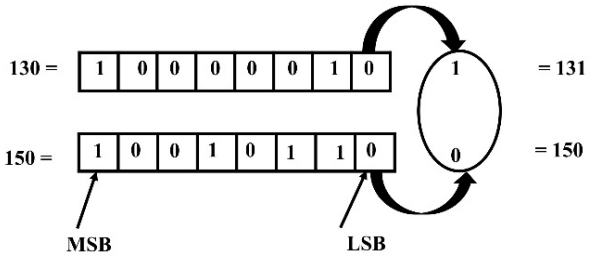

Figure 8. Basic least significant bit (LSB) technique example.

Several researchers have studied modifications of the LSB technique, which are commonly related to the spatial domain. LSB techniques have been developed based on a bit-plane of digital discrete signals (e.g., audio or images). A bit-plane that represents the signal is a set of bits having the same bit position in each of the binary numbers. Most techniques use only one bit-plane for embedding. This technique works on the least significant bit (i.e., the eighth bit-planes), but others have used three bit-planes (i.e., the sixth–eighth bit-planes) or even four bit-planes (i.e., the fifth–eighth bit-planes) for embedding with acceptable image quality. The four least significant bits (i.e., the fifth–eighth bits of the cover image) can be replaced with the chosen bit of the secret image by simply using an OR operation in a specific manner [60]. This method first converts the host image into a stream of binary bits, outputs zero in the embedded bit, and then shifts the secret image to the right by 4 bits. Then, an OR operation is performed on these two (i.e., the host and secret images) to obtain the combined image. This operation is illustrated in Figure 9.

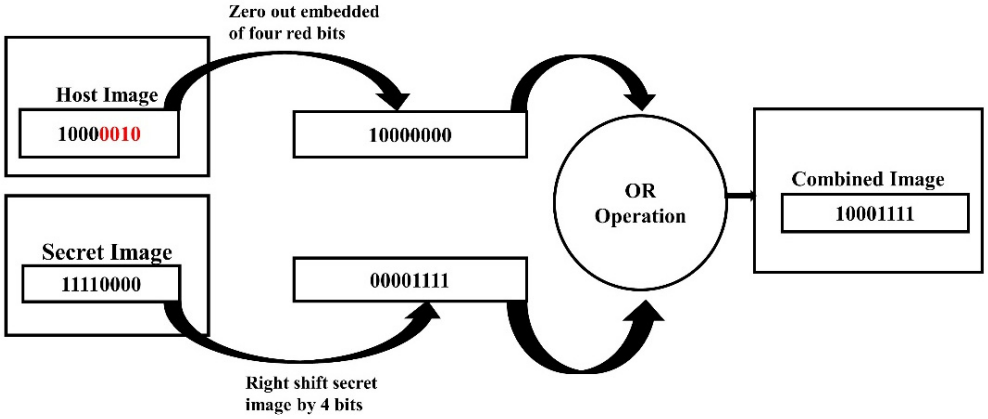

Figure 9. Block diagram of the LSB method (four bit-planes).

An example can best describe the above figure. Let the pixel value of the cover image (or host image) be 130 (10,000,010) and the binary representation of the secret image be 11,110,000. After embedding out zero, the cover image value is 128 (10,000,000). After shifting right by four bits, the secret image value is 15 (00,001,111). Then, an exclusive-OR operation is done to obtain the combined image pixel, which has a decimal value of 143 (10,001,111). Therefore, this method shows the worst scenario when the host image and the secret image seem to be the same [61]. In other words, the

difference between the host image and the secret image is (2*k*-1), where *k* is the number of different bit-planes. To obtain random signals, a specific key (along with an *m*-sequence generator) can be used by the LSB algorithm. Thus, using the Huffman method, a two-dimensional watermark signal can be inserted into the host image with the corresponding pixel value [2]. The method of Fung and Godoy [62] changes the host image pixels—only half of the bits (the least 1–4 bits), on average—with the number of bits of the embedded secret message.

The human visual system cannot recognize this, due of negligible changes in the intensity of colors. Yet, a submissive attacker can easily detect the changed bits, due to the simple operation involved. Manjula and Danti proposed a 2-3-3 LSB insertion method [63], which uses secret data that contains eight bits. These data are inserted into the LSB in a 2-3-3 order, such that two (02) bits are inserted into the R channel, three (03) bits are inserted into the G channel, and the remaining three (03) bits are inserted into the B channel. This method improves the MSE and PSNR values over the hash-based 3-3-2 technique. In a block-based method, the cover image may be processed by splitting it into blocks using certain techniques, such that the secret image can never be extracted. Then, the embedded watermark is encoded by modifying the relationships between neighboring blocks.

The conventional spatial domain watermarking technique has the highest probability of creating a salt-and-pepper noise effect. Hence, a method has been proposed by Abraham and Paul [64] for color image watermarking in the spatial domain without degrading image quality meaningfully and changing the perceptual color, as compared to conventional spatial domain watermarking. To make authentication and/or recovery possible, the watermark is embedded into all image blocks to ensure the higher quality of the image and high robustness against attacks. M1 and M2 ensure that the embedded bits are less disrupting to the human visual system, where M1 is the embedding mask and M2 is the compensation mask. The modified pixels are not noticeable, compared with neighboring pixels. Experimental results showed that their proposed algorithm recovered the watermark data even after the least significant bits were distorted and that the algorithm assured a good PSNR value. Although the LSB technique can easily be modified, understanding how the digital image will be modified, concerning integrity and safety, is a challenging task. The LSB hash algorithm authenticates the digital image using a hashing scheme which hides the hash function. One study embedded LSB hash code to protect the original file and extract the embedded hash code in order to produce an output file that appeared to be the same as the original file. In this case, the embedded watermark, which is used for extracting the data, is invisible [65]. However, LSB techniques can easily be implemented, and, thereby, the associated computational complexity may be reduced [8].

5.1.2. Intermediate Significant Bit (ISB)

LSB techniques are the most common and simple advanced watermarking techniques in the spatial domain, but they do not ensure robustness against attacks. For this reason, alternative methods, such as intermediate significant bit (ISB) methods, have been developed to improve the robustness and preserve the quality of the watermarking system. Several studies have developed ISB methods using different algorithms. One of these methods replaces the classic LSB technique with ISB by finding the best pixel value in between the middle and the edge of the range. In this method, the watermark image is protected from various attacks and alteration of watermarked image is minimized [66]. Another study [67] concentrated on the dual intermediate significant bit (DISB) model, in which two bits are embedded into each pixel of the host image and the remaining six (06) bits are changed to adjust the original pixel. The watermark image can be chosen by selecting the nearest pixel value to the original, if there exists a difference between the original and the embedded one. The proposed model produces a higher quality watermarked image, as compared to LSB methods. Therefore, the DISB method ensures high robustness against attacks and improves the quality of the watermarked images. Robustness and quality are the two most essential requirements for any watermarking system, which can be analyzed by fair normalized cross-correlation (NCC) values.

ISB techniques have been used for image watermarking in the spatial domain. This technique substitutes original image pixels with watermark pixels by keeping the watermark pixels close to a filled or empty region in the original image pixels. The watermark pixel value is tested, according to the range of each bit-plane, and then the original image file pixel is placed outside any of the edges of the range [68]. There are eight (08) bit planes in grayscale images, where the first bit-plane holds the MSB while the eighth contains the LSB, and the remaining (second–seventh) bit-planes are used as ISB [69]. If the pixel value of a grayscale image is 133 (10,000,101), then intermediate significant bits are represented by Figure 10.

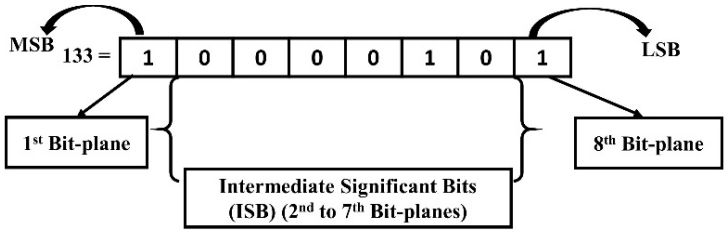

Figure 10. A bit-plane of a digital image.

PSNR and NCC are the most frequently used quality metrics for watermarked images, where PSNR determines the intensities of strength and weakness of watermarking techniques, while the latter validates the strength of the used algorithm applied to a watermarked image after attacks. Considering this issue, the paper [69] revealed the amount of strength and weakness of digital image watermarking techniques by defining the threshold values of PSNR and NCC. The discussed watermarking technique embedded four watermarks to the ISB of six grayscale image files one-by-one by substituting the original image pixels with new pixels and keeping them close to the original pixel values simultaneously. Their proposed algorithm demonstrated better robustness against some common image processing operations, such as filtering, compression, noise, and blurring, based on the PSNR and NCC values. Robustness does not decrease against geometric transformation attacks, such as scaling and rotation, in which pixel intensities are not be affected by their changed locations. Therefore, to increase the robustness of messages against various attacks and to resist geometric transformations (e.g., scaling, cropping, and filtering), ISB techniques can be used, instead of LSB techniques, where the secret message can be embedded in a bit-plane (or bit-planes) [70].

5.1.3. Patchwork

Patchwork is a pseudo-random statistical process, which is embedded into an original image invisibly using redundant pattern encoding by a Gaussian distribution. Two patches A and B are chosen pseudo-randomly, and the image data of the first patch (A) are faded, while those in B are darkened. Patchwork methods show better robustness against maximum non-geometric image modifications and the process is independent of the content of the original image [71]. In this case, the robustness can be increased by either more affine coding, feature recognition, or both, and the code can be lost by scaling, translation, or rotation before decoding. Although patchwork is impartially resistant to cropping, it does degrade its accuracy. The pseudo-random bitstream is generated by selecting pairs of pixels from the original image. A bit of information is encoded into the pair, where d denotes the difference between the two pixels; the encoding is 0 for $d < 0$ and the pixels are swapped for $d > 0$. The next pair can be progressed if d is equal to 0 or greater than a pre-defined threshold [72]. Therefore, the brightness can be increased by one unit at one point and decreased, respectively, at another point. This method is suitable for large areas of random texture, but not for text images. A region of random texture pattern in the image is copied to an area of the image with a similar texture. Each texture region is recovered through autocorrelation [73]. In a study by Yeo et al. [74], a generalized patchwork algorithm consisting of additive and multiplicative patchworks was proposed. This method uses statistical data to embed and detect the watermark. To detect the watermark data, this method uses

the location-shift scheme and the scale-shift scheme. Their proposed method was shown to be robust against compression attacks. Yet, the robustness against various attacks is very high in the patchwork method; a small amount of data can be concealed [75]. The watermark can be embedded by using redundant pattern encoding into an image, and the watermark can be extracted using a secret key concerning the decoding algorithm.

5.2. Frequency (or Transform) Domain Watermarking Algorithms

Spatial domain watermarking techniques are too fragile, as they can be easily manipulated. These techniques are much less robust against different types of attacks, compared to frequency-domain algorithms. These drawbacks have drawn focus to the research of transform-domain watermarking techniques which hide data in the transform space of a signal, rather than time, in a more effective way. This technique converts an image using a pre-defined transform in order to represent the image in the frequency domain. Then, it embeds the watermark by changing the transform domain coefficients of the original image using different transforms, including the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), Hadamard, CAT, FFT, PHT, and Fresnel transform, among others. Finally, it extracts the watermark, with the help of a correct key, using an inverse transformation. Figure 11 describes the above procedure.

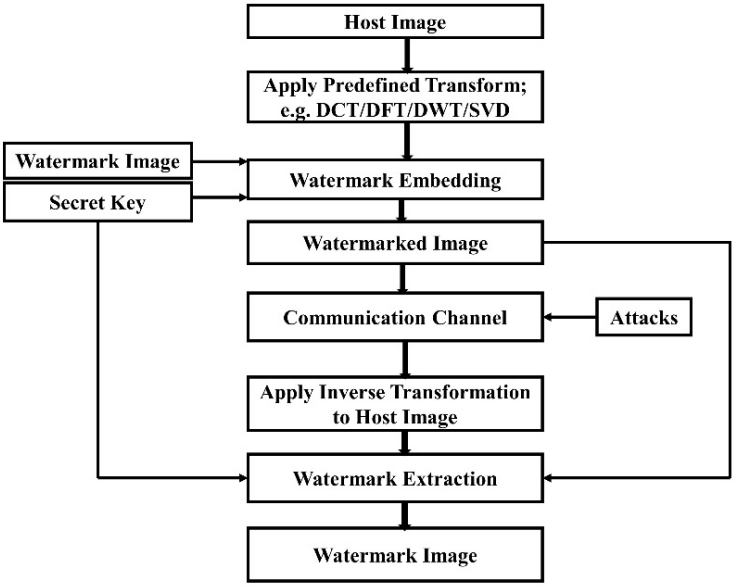

Figure 11. Watermark embedding and extraction in the transform domain.

To recover the original signal in the frequency domain, the frequency components must be recombined by applying phase shift information to each sinusoid of an image [1]. Many studies have been carried out on transform domain image watermarking, proving the better robustness, security, and imperceptibility against various attacks, such as compression, noise, filtering, cutting, and rotation. This section reviews some of those studies, which mostly used frequency-domain transforms, such as DCT, DFT, DWT, and SVD, and touches on hybrid domain methods.

5.2.1. Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) separates an image into its equivalent frequency coefficients by modifying frequency components, which can be expressed as a sum of cosine functions. The DCT is a Fourier-related transform and contains a finite sequence of data points. Only real numbers can be used here. Its variance determines the usefulness of the DCT coefficients. The DCT is important for

image compression; for instance, in the JPEG image format. The one-dimensional (1D) DCT is defined by the following equation [76]:

$$y\,(k) = \alpha(k) \sum_{n=0}^{N-1} x\,(n) \cos(\frac{\pi(2n+1)k}{2N}),\ k = 0,\ 1,\ \ldots,\ N-1 \tag{6}$$

and the inverse transform is given by

$$x(n) = \sum_{k=0}^{N-1} \alpha(k) y(n) \cos(\frac{\pi(2n+1)k}{2N}),\ n = 0, 1, \ldots, N-1 \tag{7}$$

with

$$\alpha(0) = \sqrt{\frac{1}{N}},\ k = 0 \text{ and } \alpha(k) = \sqrt{\frac{2}{N}}, 1 \le k \le N-1 \tag{8}$$

where N is the number of given data samples: $x(0), \ldots, x(N-1)$, $x(n)$ is the input data sample, $y(k)$ is the DCT coefficient, and $\alpha(k)$ is the scaling factor.

Many studies have already been carried out on digital image watermarking methods in the DCT domain. Among these, block-based DCT image watermarking works by dividing the host image into different image blocks, following which the method applies the DCT transform to this image. Then, the method inserts the watermark into the block and DCT-based host image with the help of an algorithm. The inverse discrete cosine transform (IDCT) is then applied to obtain the watermarked image. The above-discussed DCT methods for watermark embedding can be best described by Figure 12. Note that watermark extraction can be done in a reverse way.

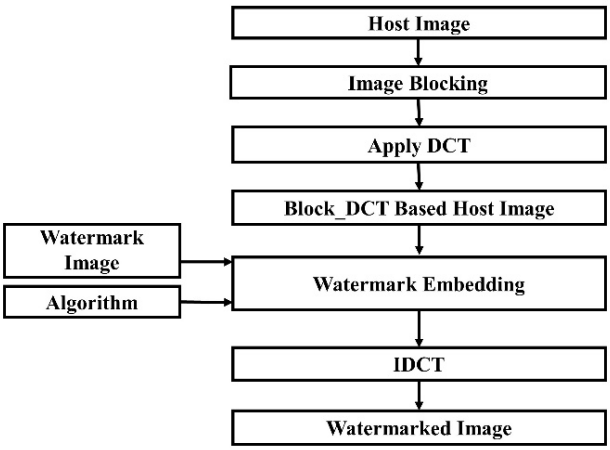

Figure 12. Watermark embedding in a block-based DCT domain.

The method proposed by Kitanovski [77] performs a block-based DCT transform in each of the blocks after dividing an image into P × P blocks and embeds a watermark generated using an image hash as a key in the low-frequency components using quantization index modulation (QIM). In QIM, only one watermark bit is inserted into each DCT block. Their proposed method demonstrated better robustness in image authentication [78]. Another paper [12] introduced a method which was robust against JPEG compression along with a Gaussian low pass filter. This method embeds 4096 bits of information of an image whose dimension is 512 × 512 pixels, where adaptive quantization can be used to select the twelve representative DCT coefficients which embed the watermark. A Chinese Remainder Theorem (CRT)-based watermarking scheme in the DCT domain has been proposed by Jagdish C. Patra, which performs better against brightening, sharpening effects, and JPEG compression, as compared to a CRT scheme based on spatial domain methods, in terms of robustness and security [79]. Although DCT techniques are robust and resistant against common image processing operations, they require

huge amounts of calculation. This is difficult to implement and shows weak performance against geometric transformation attacks, such as scaling, rotation, and cropping. A DCT/IDCT method has been proposed for ensuring effectiveness [80], in which a digital watermarking encryption algorithm was introduced. For authentication, integrity verification, tamper detection, and protection of digital data, a semi-blind robust DCT watermarking approach has been proposed which uses DCT and linear interpolation techniques [81], which divides the host image into N × N (usual blocks of 8 × 8) pixel blocks, as well as obtaining the corresponding DCT block, and calculates the inverse transform. In this case, the medium-frequency (MF) components can be used, such that a compromise between robustness and watermark visibility can be achieved. The study demonstrated the high robustness of the system against rotational attacks, JPEG compression attacks, noising attacks, and median filtering attacks. At this point, the system can extract the watermark correctly, which was the main contribution of the paper. The studies of Roy et al. [82] presented a DCT-based color watermarking technique for embedding multiple watermarks, designed for copyright ownership and validation. The system demonstrated better robustness and imperceptibility and generated a higher PSNR value by eliminating the main drawback—namely, blocking artifacts (loss of some information)—of block-based DCT methods. One watermark bit was preserved by using an error-correcting code (ECC). However, the system exhibited high computational complexity. A study of Liu et al. [83] presented an improved DCT encryption method for watermarking, where the first encryption of host image is done by fractal encoding, while the second encryption is performed using DCT. This dual encryption method made the proposed system more robust and effective. A differential evolution and kernel extreme learning machine (DE-KELM)-based grayscale image watermarking method in the DCT domain has been presented, where the low-frequency coefficients are selected in a zig-zag manner, such that the watermarked image quality is not compromised [84]. Singh [85] solved the false positive detection problem which arises in the spatial domain by transforming the host image in the DCT domain, where non-overlapping blocks are generated from the DCT coefficients. These blocks create the circulant matrix, which embeds the watermark. Their proposed method extracts the watermark by generating dynamic stochastic resonance (DSR) phenomena, ensuring imperceptibility and robustness against conventional attacks. A chaotic encryption-based blind digital image watermarking technique has been proposed, which works both for grayscale and color images [24]. The method divides the host image into 8 × 8 blocks after performing DCT operation and, then, embeds the watermark using the DCT coefficients of adjacent blocks. To add another layer of security, Arnold transforms along with a chaotic map are used at this time. The results demonstrated the robustness of the system against common image processing operations.

From the above studies, we may conclude that image watermarking is resistant against most attacks when using embedding in the DCT domain. However, it is susceptible to cropping and scaling [65]. Additionally, the DCT-based transform shows better results in concentrating energy into lower-order coefficients than the discrete Fourier transform (DFT) for image data.

5.2.2. Discrete Fourier Transform (DFT)

The discrete Fourier transform (DFT) uses samples that are uniformly spaced. In this case, a sequence of fixed length numbers of uniformly spaced samples of a function is converted into a sequence of the same length of uniformly spaced samples in the discrete-time Fourier transform (DTFT). The DTFT uses a set of harmonically related complex (magnitude and phase) exponential functions. The DFT represents the original input sequence in the frequency domain and produces a signal that is discrete and periodic. Many practical applications, including signal processing, image processing, filters, convolution operations, spectrum analysis of sinusoids, and Fourier analysis, are done by DFT [86]. The one-dimensional (1D) DFT can be defined by the following equation [76]:

$$y(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x(n) \exp\left(-j\frac{2\pi}{N}kn\right),\ k = 0,\ 1,\ \ldots,\ N-1 \tag{9}$$

The inverse transform is given by

$$x(n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} y(k) \exp\left(j\frac{2\pi}{N}kn\right),\ n = 0,\ 1,\ \ldots,\ N-1 \tag{10}$$

with

$$j = \sqrt{-1} \tag{11}$$

where N is the number of given data samples: $x(0), \ldots, x(N-1)$, $y(k)$ is the DFT coefficient, and $x(n)$ is the input data sample.

Many studies have been carried out on the DFT for image watermarking. Tsui et al. [87] proposed two algorithms for color image watermarking that use multidimensional Fourier transforms. The spatial-chromatic discrete Fourier transform was used for embedding a color watermark (yellow and blue). A color image contains chromatic content, which is converted to CIE chromaticity co-ordinates in the frequency domain in this method. Then, the color watermark is inserted into the host image. Another method uses the quaternion Fourier transform to insert a watermark in the frequency domain after encoding the components of a color image. The experimental results demonstrate that the imperceptibility is maximized, and better robustness is exhibited against external attacks and many digital signal processing operations, as compared to other existing algorithms. The method shows the strength of the watermark is best. The DFT approach has demonstrated a strong robustness to geometric attacks, as well, as it is translation invariant. Therefore, a robust, simple, and fast watermarking method based on DFT with an optimal implementation radius has been studied by Poljicak et al. [88], where the watermark was embedded in the magnitude spectrum of the Fourier transform and the quality degradation of the watermarked image was shown to be minimal, by evaluating the PSNR. Their results demonstrated significant robustness against amplitude modulation, the print-scan process (PS), half-toning, the print-cam process (PC), cropping, and attacks from the StirMark benchmark software. Cedillo-Hernandez et al. [89] studied a robust watermarking method in the DFT domain for managing medical images, which ensured high robustness and preserved the quality of the watermarked images. The proposed method inserts the watermark into the magnitude spectrum of the middle frequencies of the DFT of the original medical image. The corresponding electronic patient record (EPR) data cannot be corrupted or detached from the medical images. It was shown that the system is robust against signal processing operations and geometric distortions.

The performance of a watermarking technique is estimated in terms of robustness, imperceptibility, capacity, and detachment detection. Another paper [90] proposed the combination of the QDFT and a log-polar transform, where the QDFT is the quaternion discrete Fourier transform. The QDFT deals with the three channels (red, green, and blue) of color images. At first, the secondary image is computed using a log-polar transform. Then, the image is extracted from the low-frequency components of QDFT. This algorithm uses a secret key to enhance security. The proposed system is sensitive to alterations of image content. This method preserves content and ensures robustness, especially against rotation operations. Studies of DFT-based methods have shown that there exists a conflict problem between the quality and robustness of the systems. For this, a solution to this problem, based on the Fourier transform and characteristics of the visual system, has been presented [91], in which the host image is split into the blocks that do not overlap, and the watermark bits are embedded (inserted) within the selected coefficients of each block by executing certain conditions. Different types of attacks, such as gamma noise, Gaussian noise, sharpness, blurring, and filtering, can be minimized by this method, which exhibits better robustness. A DFT-based semi-fragile watermarking method with a substitution box has been presented by Jamal et al. [92], which embeds watermark bits generated by a chaotic map into the host image. Although this method is complex to compute, it has demonstrated improved robustness and security against different kinds of attacks. Therefore, these methods provide better robustness against geometric attacks (e.g., translation, rotation, scaling, and cropping), which makes DFT domain-based techniques a popular area of research. In this context, two types of DFT-based

watermark embedding techniques have been proposed. The first type inserts the watermark directly by changing phase information within the DFT. The second type is based on a template to judge the transformation factor in the DFT domain. Finally, a detector can be used to detect the embedded spread spectrum watermark [93].

5.2.3. Discrete Wavelet Transform (DWT)

In mathematics, a discrete wavelet transform (DWT) is any wavelet transform that decomposes a signal into wavelets, rather than frequencies. In a DWT, the wavelets are discretely sampled. The temporal resolution is one of the advantages of DWT over Fourier transforms (i.e., DCT and DFT). This makes DWT a more attractive research area, by capturing multiple information aspects, such as location in time and frequency [94]. A set of wavelets, which are mathematical functions, is used to decompose the signal. The wavelet transform is useful in digital signal processing, image compression, and in removing noise from the signal. The key idea in a wavelet transform is the use of a set of basis functions (called wavelets) that offer localization in the frequency domain. High frequency resolution can be obtained at low frequencies, and high time resolution can be obtained at high frequencies when using a wavelet transform.

The DWT of a signal *x[n]* is defined by the following equations [95]:

$$W_\phi[j_0,\ k] = \frac{1}{\sqrt{M}} \sum_n x[n]\phi_{j_0,k}[n] \tag{12}$$

$$W_\psi[j,\ k] = \frac{1}{\sqrt{M}} \sum_n x[n]\psi_{j\ ,k}[n],\ for\ j \geq j_0 \tag{13}$$

where $W_\phi[j_0,\ k]$ are the approximation coefficients, $W_\psi[j,\ k]$ are the detail coefficients, and the inverse DWT is given by

$$x[n] = \frac{1}{\sqrt{M}} \sum_k W_\phi[j_0,\ k]\phi_{j_0,k}[n] + \frac{1}{\sqrt{M}} \sum_{j=\ j_0}^{J} \sum_k W_\psi[j,\ k]\psi_{j\ ,k}[n] \tag{14}$$

with

$$n = 0,\ 1,\ 2, \ldots,\ M-1,\ j = 0,\ 1,\ 2, \ldots,\ J-1,\ k = 0,\ 1,\ 2, \ldots,\ 2^j - 1 \tag{15}$$

where M is the number of samples to be transferred = 2^J, J is the number of transfer levels, $\left\{\phi_{j,k}[n]\right\}$ and $\psi_{j\ ,k}[n]$ are two basis functions, $\phi[n]$ denotes the scaling function, and $\psi[n]$ denotes the wavelet function.

The basic DWT image watermarking technique decomposes the original image into three different levels. The sub-bands LH3, HH3, and HL3, at three different levels, are used to embed the watermark. Sub-bands consist of a wide range of the frequency spectrum of the image. Therefore, the robustness of the watermarking system is increased [96]. A three-level DWT is shown in Figure 13.

After applying the DWT, the system embeds the watermark into the host image by using an algorithm and, then, applies the inverse DWT (IDWT) to obtain the watermarked image. The watermark extraction process takes the watermarked image as input and applies the DWT at the same level. Finally, the process applies the IDWT to get the watermark image. The whole process is depicted in the Figure 14.

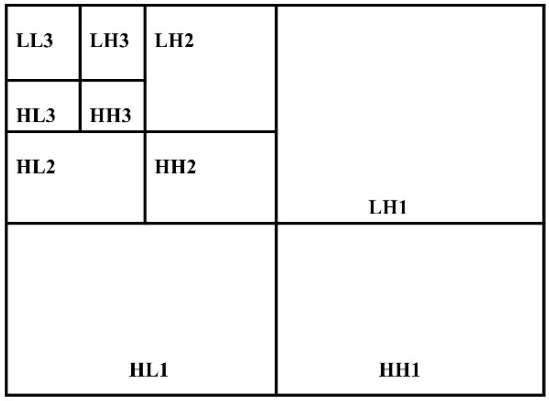

Figure 13. Three-level discrete wavelet decomposition.

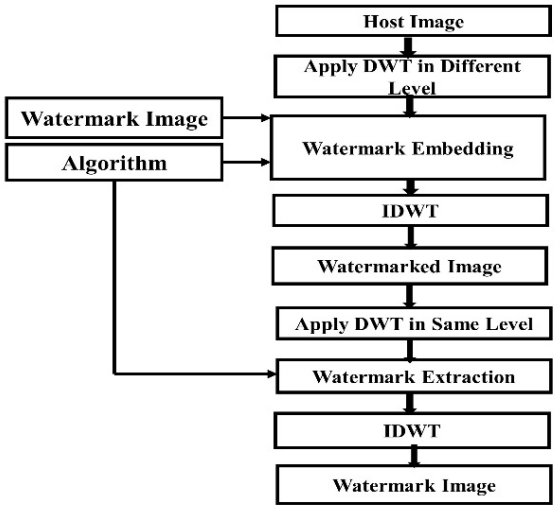

Figure 14. Watermark embedding and extraction in a Discrete Wavelet Transform (DWT) domain.

Many studies have been carried out on the authentication of images in the DWT domain. For example, Chen [97] proposed a digital image watermarking algorithm based on threshold classification in the wavelet domain. The algorithm analyzes the complexity of the images concerning robustness and imperceptibility. The method divides the host image into different blocks, which are selected for embedding the watermark. Then, with the help of the derived optimal sub-bands, the DWT coefficient is classified based on sub-bands that have lower frequencies. Extensive experiments were carried out, and the results demonstrated strong robustness and imperceptibility of the system against some common attacks. Another paper [98] proposed an efficient digital image watermarking technique based on the wavelet transform in HSI color space for protecting copyright holder information, in which a one-level wavelet coefficient (LL) is generated in the host image, and 8×8 blocking operations are used on the grayscale watermark image. For embedding, each block of both images is compared and scaled with a scaling factor α. At the receiver site, the system extracts the watermark image in the opposite manner. The simulation results demonstrated that their proposed scheme is more robust against noise, as compared to existing methods, in terms of PSNR and MSE. A different paper by Jia et al. [99] extracted the watermark without the pre-requisite of the original host image or the original watermark image. A combination of DWT and QR decomposition-based color image watermarking scheme was suggested, where one-level DWT is applied to each component of the host image. The color host image is divided into 4×4 non-overlapping blocks and QR decomposition is used to decompose each selected pixel block. In this way, the watermark can be embedded by measuring the first-row elements in the matrix R. The proposed method has better robustness against the addition of noise, image compression, cropping, and filtering, as compared to related existing methods. For

copyright protection, a new algorithm was studied in the DWT domain [69]. This blind scheme embeds the logo watermark directly into the three-level DWT decomposed sub-bands. Two kinds of security attacks were considered to confirm the security of the system. The simulation results confirmed blind detection, invisibility, and robustness against various geometric and non-geometric attacks.

Another study [100] presented a new watermarking method in the DWT domain, based on a discrete-time chaotic system. The feasibility and robustness of the proposed method were demonstrated. The host image is encrypted by a Henon map and inserted into a discrete-time chaotic system. The resulting ciphered image can be used as a watermark image, and the extracted watermark is passed through the previous chaotic channel for decryption. The proposed technique by Ambadekar et al. [101] was designed to protect copyright information by inserting the watermark in the DWT domain and extracting the watermark through watermark encryption. This method exhibited strong robustness against noise, geometric, and compression attacks. As spatial domain-based image watermarking cannot resist geometric attacks, the transform domain has been considered a more attractive research area. Hence, a new approach has been designed, which can effectively embed a color image into a host image. The technique transforms the color host image and watermarked image from the RGB model to the YIQ model, separately, and the two-dimensional DWT and corresponding selection algorithm are applied. This algorithm ensures the system's robustness against attacks such as lossy compression and Gaussian noise. The method has been applied to ensure image security [102].

5.2.4. Singular Value Decomposition (SVD)

In mathematics, a singular value decomposition (SVD) is the product of a real or complex matrix. This method is the generalization of the eigendecomposition of a symmetric matrix with non-negative eigenvalues to any $m \times n$ matrix through an extension of the polar decomposition. The SVD transformation has been widely used in statistics and digital signal processing. The SVD of a matrix M can be defined by the following equation [103]:

$$M = U \Sigma V^* \tag{16}$$

where M is an $m \times n$ matrix that comes from the field K (either real numbers or complex numbers), U is an $m \times m$ unitary matrix over K, or an orthogonal matrix (if $K = R$), $\sum$ is a diagonal $m \times n$ matrix with non-negative real numbers on the diagonal, V is an $n \times n$ unitary matrix over K, and V^* is the conjugate transpose of V.

In the SVD, the diagonal entries σ_i of $\sum$ are known as the singular values of M.

The one-way and non-symmetric properties cannot be obtained with the above-discussed DCT, DFT, and DWT transformations. Therefore, another transformation, using SVD, has been proposed for watermarking [104]. This method embeds the watermark by discovering the features of D and the relationship of the U component coefficients. This technique can extract the watermark efficiently, even after tampering. Simulation results demonstrated the high quality of the watermarked image and stronger robustness against various attacks, as compared to existing methods. Vaishnavi [105] proposed a method designed for robust and invisible image watermarking in the RGB color space. The method embeds the watermark into the singular values. The watermark is retrieved by engaging SVD on the blue channel of the host image. The proposed method was shown to provide better robustness against Gaussian noise, motion blur, salt-and-pepper noise, median filtering attacks, and JPEG compression attacks, among others, as compared to existing methods, where performance was evaluated using the normalized correlation (NC) and PSNR measures. The existing block-based SVD is not robust against geometric distortions, rotation, and image flipping. Therefore, an alternative solution has been proposed [106] that combines the concept of redistributed image normalization and SVD, where the coefficient magnitude is inserted. The proposed scheme is efficient against various attacks, in terms of robustness and security. Another algorithm has been proposed [107], based on SVD and homomorphic transform. This method ensures the digital security of an eight-bit grayscale image

by embedding an invisible eight-bit grayscale watermark image. The SVD finds the singular values in which the watermark is inserted. The robustness and invisibility of this watermarking system have been guaranteed by evaluating the PSNR, normalized cross correlation (NCC), and mean-structural similarity-index-measure (MSSIM) performance.

5.3. Hybrid Domain Watermarking Algorithms and Current Trends in Watermarking

Hybrid domain watermarking algorithms are usually considered as a combination of spatial- and transform-domain algorithms. These algorithms ensure both robustness and enhanced data embedding properties. Many studies have been carried out on hybrid domain methods. These studies reflect the current trends in watermarking. For example, the authors of reference [108] combined the spatial and frequency domains for image watermarking, such that more watermark data could be embedded into the host image. This method increases the capacity of the host image and splits the watermark into two parts, which doubles the protection. The spatial domain substitutes the LSB bits of the host image with the bits of the watermark image. On the other hand, the frequency domain inserts data into the low-frequency components of the host image. Furthermore, a random permutation of the watermark can be used to enhance robustness against various signal processing attacks, such as image cropping. In reference [109], DCT, DWT, and SVD were combined to achieve better robustness and imperceptibility. This hybrid scheme was shown to be robust against JPEG compression, filtering, salt-and-pepper noise, rotation, cropping, and scaling and translation operations. Another scheme [110] was introduced to protect digital rights in a hybrid domain. The scheme protects digital contents during broadcast over a non-secure channel by using the least significant bits and a wavelet transform (DWT and SVD), where the host image is divided into sub-bands (LL, HL, HH, and LH) by using the transformation method in the frequency domain. The previously defined embedding algorithms are used to extract the watermark. This hybrid scheme provides better quality and robustness against different attacks, such as Gaussian noise and JPEG compression. Another study combined DCT and DWT to improve the robustness of the watermarking system [111]. A hybrid scheme of DWT and SVD has been proposed, which ensures both the robustness and imperceptibility of the watermarking system [112]. Existing watermarking algorithms are less robust to geometric attacks. Hence, to resist geometric attacks, a multi-watermarking algorithm has been proposed for medical images, based on dual-tree complex wavelet transform (DTCWT), DCT and a Henon Map [113]. This algorithm can be used for medical security, security authentication, cloud storage, and cloud transmission.

5.4. Summary of Watermarking Techniques of Working Domain

From the above-discussed research, we can conclude that some watermarking algorithms are simple to implement. Some algorithms minimally degrade the image quality, while others highly distort the image. Some are complex to achieve, and some are highly robust against common image processing operations but are not resistant to geometric attacks. Then again, others are highly robust to geometric attacks but very sensitive to various kinds of noise. Some of them ensure better PSNR and NCC values, while others result in low PSNR. Based on the desired applications, some are robust, while others are fragile. Hence, this section summarizes the findings of the above-discussed state-of-the-art watermarking techniques among current trends in watermarking techniques, with the help of the following Table 3. Table 3 includes techniques in use, image type, image size in pixels, factors, advantages, limitations, and associated applications.

Based on Table 3, we conclude that DCT provides high robustness and imperceptibility, while LSB exhibits the least robustness and imperceptibility. The ranking, in terms of robustness and imperceptibility, can be written as

$$DCT > SVD > DWT > DFT > LSB. \quad (17)$$

Table 3. Summary of state-of-the-art watermarking techniques (continued).

Used Techniques	Image Type	Image Size (pixels) (Host Image and Watermark Image Respectively)	Factors	Advantages	Limitations	Applications
LSB Modification [64]	Color	512 × 512, 64 × 64	Robustness	High quality of the watermarked image -High robustness to attacks -Good PSNR (47.6dB) -Fast speed	The worst scenario for having no difference between the host image and the watermark image -Only B component is used for embedding color	Copyright protection
LSB hash algorithm [65]	-	-	Capacity	Extract watermark data effectively	Less robust to various attacks	Histogram analysis, Hamming distance
ISB [66]	Grayscale	256 × 256, 90 × 90	Robustness	Improve robustness -Minimum distortion of the watermarked image	Less Robust against geometric attacks, like scaling, rotation, filtering, and cropping.	Image authentication
DISB [67]	Grayscale	256 × 256, -	Robustness, Capacity	Better NCC values -Better robustness than LSB -PSNR > 30 dB -Improves capacity over ISB	Less Robust against geometric attacks, like scaling and rotation. -Limited to one pixel	Image authentication
ISB [69]	Grayscale	256 × 256, 90 × 90	watermarked image quality	Improved robustness based on the NCC and PSNR values - Robust against blurring, filtering, compression, and noise.	Less Robust against geometric attacks, like scaling and rotation.	Image authentication
Generalized patchwork [74]	-	-	Robustness	Better robustness against compression attacks	Not robust against random bend attacks	Used for large areas of random texture image
DCT and hash key [77]	-	512 × 512, 64 × 64	Robustness and security	Robust against common image processing operations -Secure	Fragile in case of tampering	Image authentication

Table 3. *Cont.*

Used Techniques	Image Type	Image Size (pixels) (Host Image and Watermark Image Respectively)	Factors	Advantages	Limitations	Applications
DCT [12]	Grayscale	512 x 512, 64 × 64	High capacity and robustness	Capable of embedding 4096 bits -Robust against Gaussian low pass filter and JPEG compression	Less Robust against geometric attacks, like scaling, rotation, filtering, and cropping. -Less imperceptible	Image authentication
DCT and CRT [79]	Grayscale	512 × 512, 64 × 64 or 128 × 64	Robustness, imperceptibility, and security	Less computational complexity than SVD-Improves security -Robust to JPEG compression attacks, brightening, and sharpeningeffects	Less robust to tampering attack	Image authentication
DCT and linear interpolation [81]	Color	256 × 256, 256 × 256	Robustness	Robust against rotational attacks, noising attacks, JPEG compression attacks, and median filtering attacks	Complex	Integrity verification, tamper detection, image authentication, copyright protection
DCT and repetition code [82]	Color	512 × 512, 64 × 64	Robustness, imperceptibility	Higher PSNR value, -Better robustness against filtering, noising and geometric attacks	Higher computational complexity	Copyright ownership
DCT and fractal encoding [83]	Grayscale	1024 × 1024, 256 × 256	Robustness	Better robustness, -Good PSNR, -Improves security	Higher computational complexity	Copyright ownership
Integer DCT, non-linear chaotic map, and DSR [85]	Grayscale	256 × 256, 256 × 256	Robustness, imperceptibility	Solves false positive detection problem, -Better robustness against geometric and non-geometric attacks	Less robust against histogram equalization and wrapping	Image authentication

Table 3. *Cont.*

Used Techniques	Image Type	Image Size (pixels) (Host Image and Watermark Image Respectively)	Factors	Advantages	Limitations	Applications
DCT, Arnold transform, and chaotic encryption [24]	Grayscale and color	512 × 512, 64 × 64	Robustness, imperceptibility, Payload capacity	Robust against JPEG compression, rotation, cropping, Gaussian noise, filtering, and combined attacks, -Highly secure	Less robust against cropping operation	Copyright protection and ownership verification
SCDFT and QFT [87]	Color	512 × 480, -	Robustness, imperceptibility	Robust against geometric transformations, Gaussian noise, and image enhancement, -Maximizes imperceptibility	Not robust against JPEG compression and color conversion, -Higher computational complexity	Copy control and transaction tracking
DFT [88]	Bitmap	512 × 512, -	Quality of watermarked image	Minimizes quality degradation of watermarked image, -Robust against amplitude modulation, PS, half-toning, PC, and attacks from the StirMark benchmark software, -Low complexity	Less robust against cropping	Image authentication
DFT [89]	DICOM Grayscale	512 × 512 × 8 bits, -	Robustness -Quality of watermarked image -Payload capacity	Robust against JPEG compression, sharpening, filtering, and Gaussian noise, -Robust against geometric attacks, like rotation and scaling - Avoids the detachment problem -Better imperceptibility -Good PSNR	Not capable of restoring the EPR data to their original text format	Medical image management

Table 3. *Cont.*

Used Techniques	Image Type	Image Size (pixels) (Host Image and Watermark Image Respectively)	Factors	Advantages	Limitations	Applications
QDFT and log-polar transform [90]	Color	512 × 384 or 384 × 512, -	Robustness, Security	Robust against large angle rotation operations, JPEG compression, average and median filtering, and brightness adjustment, -Secured	Not robust against a type of tampering	Content authentication
DFT [91]	Color	256 × 256, -	Robustness, Image quality	Robust against filtering, Blurring, sharpness, and Gamma noise	Not robust against geometric operations	Copyright protection and authenticity
DFT and Chaotic system [92]	Grayscale	256 × 256, 50 × 50	Robustness, security	Robust against JPEG compression, cropping, and noise	Less robust against rotation operation,-Complex to compute	Cryptology
DWT [97]	Grayscale	256 × 256, 32 × 32	Robustness, imperceptibility	Robust against salt-and-pepper noise, JEPG compression, rotation, and median filtering -Good imperceptibility, -PSNR = 89.1481, NC = 1.0000	Not robust against cropping	Content authentication
DWT [98]	Color and Grayscale	Color 512 × 512, Grayscale 256 × 256	Robustness, image quality	Robust against Gaussian noise, salt- and-pepper noise, speckle noise, and brightness	Less robust against transformation operation	Copyright protection and owner information
DWT and QR Decomposition [99]	Color	512 × 512, 32 × 32	Robustness, imperceptibility	Robust against compression, cropping, filtering, and noise adding, -Better imperceptibility,	Less robust against salt-and-pepper noise and cropping	Copyright protection

Table 3. *Cont.*

Used Techniques	Image Type	Image Size (pixels) (Host Image and Watermark Image Respectively)	Factors	Advantages	Limitations	Applications
DWT and chaotic system [100]	Grayscale	512 × 512, -	Robustness, security	Secured against statistical attacks	Complex	Microcontroller circuits'
DWT and encryption [101]	Color and Grayscale	Color 228 × 228, Grayscale 90 × 90	Robustness, imperceptibility	Robust against rotation, JPEG compression, and salt-and-pepper noise, -Better imperceptibility, -PSNR >50 dB	Not robust against cropping, scaling, and other transformations	Copyright protection, content authentication
DWT and Haar wavelet [102]	Color	256 × 256, 64 × 64	Robustness, imperceptibility	Robust against lossy compression and Gaussian noise	Complex	Security of image information
SVD [104]	Grayscale	512 × 512, 32 × 32	Robustness, image quality, security	Robust against JPEG compression, Gaussian noise, sharpening, and cropping, -Preserves image quality	Not robust against rotation and scaling	Ownership identification
SVD [105]	Color and Grayscale	256 × 256, 256 × 256	Robustness, security	Robust against Gaussian noise, Salt-and-pepper noise, motion blur, median filtering, and JPEG compression	Not robust against rotation, cropping, and scaling	Digital security of an image
SVD and Redistributed image normalization [106]	Grayscale	512 × 512, 64 × 64	Robustness and security	Solves false positive detection problem, -Better robustness and imperceptibility	Does not work for color images	Ownership identification, medical image watermarking, and fingerprinting
SVD and Homomorphic Transform [107]	Grayscale	512 × 512, 512 × 512	Robustness and imperceptibility	Robust against large rotation, cropping, scaling, JPEG compression, salt-and-pepper noise, Gaussian noise, andaverage filtering	Low capacity of data embedding, - Major changes in singular values due to small changes in image	Digital security of an image

6. Challenges of Image Watermarking Methods

At present, information is an asset. With the advent of computers, the usage of multimedia technology is increasing daily. This makes the tasks of protecting information from being accessed by unauthorized parties (confidentiality), ensuring the authenticity of information and protecting against unauthorized changes (integrity), and confirming that information is accessible by authorized users (availability) more challenging. These are the three key security requirements of a system, which are very difficult and challenging to implement. Moreover, robustness, imperceptibility, and capacity are the essential requirements in designing a robust watermarking system. However, keeping a balance among these three conflicting requirements is a difficult task. Imperceptibility can be achieved by embedding a watermark in the high-frequency components; however, this task produces weaker robustness, as robustness occurs in the low-frequency components. Still, security is a big challenge in digital image watermarking. More recently, internet of things (IoT)-based authentication schemes have provided supreme security without human interaction [114], where more encryption can be done outside the image contents. Furthermore, blockchain-based authentication schemes also provide high levels of security. Blockchain technology stores data in a decentralized manner and completely protects data against any tampering [115]. It also detects forgery and differentiates the original image from the tampered image. Therefore, these two schemes can be accommodated in the watermark domain.

6.1. Attacks on Watermarks

The extensive literature of various watermarking techniques reveals that the extraction or alteration of hidden watermark data is not such a difficult task for anyone, as information passes through the communication channel. However, an important trait is that the watermarking system should be robust enough against attacks. In a watermarking system, any processing that may cause the harmful detection of the watermark or impairment of the communication conveyed by the watermark is known as an attack. Then, the processed watermark data is identified as attacked data [116,117]. These attacks (which may be intentional or unintentional) cause distortions in the watermarked image, and include active attacks, passive attacks, geometric attacks, removal attacks, protocol attacks, cryptographic attacks, blind attacks, informed attacks, tampering attacks, simple attacks, attacks based on key estimation, destruction attacks, and synchronization attacks, among others [118]. This sub-section details some of the existing image watermarking attacks.

6.1.1. Active Attacks

Active attacks occur when a hacker finds and exploits the weakness of a watermark detection function by removing or destroying the watermark; that is, simply by accessing the watermark embedding function, an adversary can easily distort the watermarked image. The most common active attacks for image watermarking include elimination, collusion, masking, distortion, forgery, copy, ambiguity, and scrambling attacks. In elimination attacks, the watermark image will never be detected, but the attacker tries to produce a similar output image, where the copy attack produces a copy with no watermark. On the other hand, with a masking attack, the attacked watermarked image still contains a watermark which is imperceptible by existing detectors. In distortion attacks, some processing techniques may be evenly applied to degrade the watermark, either over the whole watermarked image or some part of it. In a forgery attack, an invalid watermark image can be falsely authenticated by the detector for performing unauthorized embedding by an adversary. However, an ambiguity attack sometimes occurs when an adversary produces an output as forgery, even after the watermarked image is validated. A scrambling attack may be caused by detecting a valid watermarked image as a fake image [119]. Defenses must be carried out to protect active attacks, which are used, for example, for fingerprinting, copyright protection, and copy control.

6.1.2. Passive Attacks

A passive attack happens when an attacker tries to find whether a given watermark is present or not without concern for the removal (destruction or deletion) of the watermark. The attacker does not try to modify the watermarking resources but, rather, to obtain the information associated to it. At this time, different levels of passive attacks can be considered for achieving various goals that are important in hidden communication.

6.1.3. Removal Attacks

Removal attacks try to remove the watermark from the host image without using the key used in the watermark embedding. These attacks are essential, and the category includes blind watermark removal, collusion attacks, remodulation, interference attacks, noise attacks, denoising, quantization, and lossy compression, among others. These attacks cannot remove the watermark completely, but attempt to damage the watermark information considerably.

The original owner attempts to make it challenging to detect the watermark due to removal attacks, as it decreases the robustness level of the watermark signal. A remodulation attack modifies the watermark image by using the modulation technique. This attack demodulates the same watermark image with the help of opposite modulation techniques. On the other hand, collusion attacks arise when hackers remove the watermark from the original data and construct a new copy without a watermark from several copies of the same original data. Each original copy contains different watermarking techniques. All types of noise, including Gaussian noise, additive noise, and salt-and-pepper noise, are used in noise attacks, which add a noise signal to the watermarked image, which causes the sender of the data to become confused. An interference attack may occur due to additional noise being added to the watermarked image [120]. These attacks attempt to harm the embedded watermark without deteriorating the document quality [121].

6.1.4. Geometric Attacks

The existing conventional watermarking algorithms are said to be efficient if they are robust against (intentional or unintentional) geometric attacks. These do not try to remove the watermark image itself but, rather, attempt to distort the watermark detector synchronization by using the inserted information. This is opposite in manner to removal attacks, and results in great difficulty in the required synchronization process in recovering the embedded watermark information by the detector. Therefore, synchronization errors between the original watermark and the extracted watermark occur during the watermark extraction process. However, the watermark still exists in the watermarked image, due to changed positions. Hence, image transformation, image degradation, image enhancement, image compression, cropping, and image adjustment are all sorts of geometric attacks, as such manipulation affects the image geometry, which must be rejected to ensure the robustness of the system. Image transformation can prevent the blind detection of a public watermark by only performing rotation, scaling, and translation (RST) operations on an image to reduce the robustness level of that image. Hence, a robust watermarking system for images must be designed which is invariant to RST operations. The algorithm proposed by Lin [122], where an RST-invariant signal is created by taking the Fourier transform of the image and then resampling and integrating along the radial dimension. Additionally, removing some parts of the host image degrades the image quality, resulting in image degradation attacks. Degradation attacks need to be designed for some restoration methods for reducing or eliminating the degradation. Another attack processes a given image by increasing the dynamic range of the chosen features to obtain more suitable results for a specific application. These attacks can be easily detected, and this property is known as image enhancement. Image compression attack reduces the amount of data of the watermark image and cuts the bandwidth required to represent a digital image. Finally, the alteration of brightness, contrast, gamma value, and saturation result in image adjustment attacks, which change the watermark image.

6.1.5. Protocol Attacks

Attacks that are directly aimed at the watermarking application are known as a protocol attacks. A protocol attack can be either an invertible attack, an ambiguity attack, or a copy attack. Non-invertible watermarks may be needed for copyright protection applications, where a watermark can never be extracted from a non-watermarked document. Invertible watermark attacks happen when the watermark is subtracted from the watermarked data by the attacker, who claims they are the owner of the watermarked data, which creates ambiguity about the original owner of the data [123,124]. This scheme results in ambiguity attacks, inversion attacks, deadlock attacks, fake-original attacks, or fake watermark attacks. A copy attack copies the watermark to some other data, called target data, after estimating it from the watermarked data without destroying the watermark or impairing the watermark detection [124].

6.1.6. Cryptographic Attacks

Cryptographic attacks may be either a security attack or an oracle attack, aimed at cracking the security in watermarking schemes by removing the embedded watermark information. A brute-force search embeds secret information which misleads the watermark. Another attack, which creates a non-watermarked signal with an available public watermark detector device, is known as an oracle attack [125]. Applications must restrict these types of attacks used in cryptography due to their high computational complexity.

6.2. Cost-Effectiveness of Different Attacking Scenarios

The cost-effectiveness of different attacks on digital image watermarking, which is usually based on computational complexity, indicates the cost (time and memory space) it requires to complete an attack. Watermarking is mainly involved with key and embedding algorithms, which are also important parameters for an attack. Different attacks are associated with different parameters.

All cost-effective parameters can be best described as in Table 4. Here,

- K: cost of finding the key. This includes the effective length of the key, which measures the security of the watermarking algorithm;
- E: the embedding cost, which affects the robustness and imperceptibility of the watermarking algorithm. This cost estimates the watermark embedding strength;
- R: the cost to remove the watermark by an attacker from the host image without using the key used in the watermark embedding algorithm;
- G: the geometric distortion cost;
- E_1: the new embedding cost generated by an attacker.

Table 4. Cost of different attacks (K: Key, E: Embedding, R: Removal, G: Geometric distortion, E_1: New Embedding).

Attacks	Cost
Active	$K+E+R$
Passive	$K+E$
Removal	R
Geometric	$K+E+G$
Protocol	$K+E+R+E_1$
Cryptographic	K

Cryptographic cost is determined by finding the key K through a brute-force attack.

6.3. Performance Metrics for Evaluating Watermarking System

Quality is an important criterion for recognizing an image-based object. The performance of watermarked image quality is measured by evaluating some performance metrics and benchmark tools, such as PSNR, MSE, Euclidean Distance (ED), SSIM, the Feature Similarity Indexing Method (FSIM), Image Fidelity (IF), Normalized Cross-Correlation (NCC), Normalized Mean Squared Error (NMSE), and Correlation Quality (CQ), among others. PSNR is expressed as the ratio of the maximum possible power of a signal to the power of corrupting noise. PSNR affects the reliability of the system, which is best described by MSE. In statistics, the MSE calculates the average squared intensity differences between the reference watermark and the extracted watermark. A higher PSNR value indicates a more efficient system, which means there exists no visual distinction between an ideal image and a corrupted image. The SSIM and FSIM, which are alternatives to PSNR and MSE, respectively, are used to compare the similarity measures (structures and features) between the original and recovered images, based on perception. The SSIM is used to predict the image quality of color (i.e., RGB) values or chromatic (i.e., YCbCr) values by evaluating how much an ideal image is distorted or degraded. The FSIM measures the similarities between the features of two images. One study [126] showed that SSIM and FSIM provide perception errors based on the human visual system, while PSNR and MSE provide absolute errors. Therefore, the performance metrics SSIM and FSIM are easy to understand for measuring performance, compared to PSNR and MSE. Furthermore, in signal processing, NCC measures the similarity between the reference watermark and the extracted watermark. NCC is defined as a function without subtracting the local mean value of intensities. These benchmark tools are commonly used to assess the performance of watermarking systems.

7. Conclusions and Future Directions

At present, information can be duplicated easily due to the interactive and digital communication of multimedia data. This issue makes digital image watermarking a significant field of research. Digital image watermarking using various techniques has been applied as an important tool for image authentication, integrity verification, tamper detection, copyright protection, and the digital security of an image. In this study, we reviewed the most dominant state-of-the-art watermarking techniques. Through this study, it can be concluded that DWT is a high-quality and robust technique for image watermarking due to its multi-resolution characteristics. Robustness, imperceptibility, and capacity are the essential requirements in designing an efficient watermarking system. However, it is almost impossible to achieve all of these requirements simultaneously. Therefore, a good trade-off between these three requirements must be maintained. However, security remains a big challenge in digital image watermarking technologies, and the accommodation of IoT and blockchain-based authentication schemes provides a challenge for researchers. Therefore, future work can be extended by combining various techniques in different domains to fulfill the above three important requirements. Moreover, to improve robustness along with security, researchers should focus on developing new, advanced techniques.

Author Contributions: M.B. studied and drafted the whole paper; M.S.U. initiated the concept, supervised the study, and fine-tuned the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Tao, H.; Chongmin, L.; Zain, J.M.; Abdalla, A.N. Robust Image Watermarking Theories and Techniques: A Review. *J. Appl. Res. Technol.* **2014**, *12*, 122–138. [CrossRef]
2. Zhang, Y. Digital Watermarking Technology: A Review. In Proceedings of the ETP International Conference on Future Computer and Communication, Wuhan, China, 6–7 June 2009; pp. 250–252.

3. Cox, I.; Miller, M.; Bloom, J.; Fridrich, J.; Kalker, T. *Digital Watermarking and Steganography*, 2nd ed.; The Morgan Kaufmann Series in Multimedia Information and Systems: Burlington, Massachusetts, 2008.
4. Mohanarathinam, A.; Kamalraj, S.; Venkatesan, G.P.; Ravi, R.V.; Manikandababu, C.S. Digital Watermarking Techniques for Image Security: A Review. *J. Ambient Intell. Humaniz. Comput.* **2019**, 1–9. [CrossRef]
5. Cox, I.J.; Miller, M.L. "Review of watermarking and the importance of perceptual modeling". *Proc. SPIE* **1997**, *3016*. [CrossRef]
6. Yang, Q.; Zhang, Y.; Yang, C.; Li, W. Information Entropy Used in Digital Watermarking. In Proceedings of the 2012 Symposium on Photonics and Optoelectronics, Shanghai, China, 21–23 May 2012; pp. 1–4.
7. Yu, C.; Li, X.; Chen, X.; Li, J. An Adaptive and Secure Holographic Image Watermarking Scheme. *Entropy* **2019**, *21*, 460. [CrossRef]
8. Kumar, V.A.; Rao, C.H.S.; Dharmaraj, C. Image Digital Watermarking: A Survey. *Int. J. Adv. Manag. Technol. Eng. Sci.* **2018**, *8*, 127–143.
9. Jaynes, E.T. Prior probabilities. *IEEE Trans. Syst. Sci. Cybern.* **1968**, *4*, 227–241. [CrossRef]
10. Refregier, P.; Javidi, B. Optical Image Encryption based on Input Plane and Fourier Plane Random Encoding. *Opt. Lett.* **1995**, *20*, 767–769. [CrossRef]
11. Wu, C.; Ko, J.; Rzasa, J.R.; Paulson, D.A.; Davis, C.C. Phase and Amplitude Beam Shaping with Two Deformable Mirrors Implementing Input Plane and Fourier Plane Phase Modifications. *Appl. Opt.* **2018**, *57*, 2337–2345. [CrossRef]
12. Pun, C.M. High Capacity and Robust Digital Image Watermarking. In Proceedings of the 5th International Joint Conference on INC, IMS and IDC, Seoul, South Korea, 25–27 August 2009; pp. 1457–1461.
13. Yang, H.M.; Liang, Y.Q.; Wang, X.D.; Ji, S.J. A DWT-Based Evaluation Method of Imperceptibility of Watermark in Watermarked Color Image. In Proceedings of the 2007 International Conference on Wavelet Analysis and Pattern Recognition, Beijing, China, 2–4 November 2007; pp. 198–203.
14. Zhang, H.; Wang, C.; Zhou, X. A Robust Image Watermarking Scheme Based on SVD in the Spatial Domain. *Future Internet* **2017**, *9*, 45. [CrossRef]
15. Takore, T.T.; Kumar, P.R.; Devi, G.L. A New Robust and Imperceptible Image Watermarking Scheme Based on Hybrid Transform and PSO. *Int. J. Intell. Syst. Appl.* **2018**, *11*, 50–63. [CrossRef]
16. Liu, J.; He, X. A Review Study on Digital Watermarking. In Proceedings of the 1st International Conference on Information and Communication Technologies, ICICT, Karachi, Pakistan, 27–28 August 2005; pp. 337–341.
17. Olanrewaju, R.F. Development of Intelligent Digital Watermarking via Safe Region. Ph.D. Thesis, Kulliyyah of Engineering, International Islamic University Malaysia, Selangor, Malaysia, 2011.
18. Yadav, U.; Sharma, J.P.; Sharma, D.; Sharma, P.K. Different Watermarking Techniques & its Applications: A Review. *Int. J. Sci. Eng. Res.* **2014**, *5*, 1288–1294.
19. Cvejic, N. Algorithms for Audio Watermarking and Steganography. Master's Thesis, Department of Electrical and Information Engineering, University of Oulu, Oulu, Finland, 2004.
20. Zhang, H.; Wang, C.; Zhou, X. Fragile Watermarking for Image Authentication. Using the Characteristic of SVD. *Algorithms* **2017**, *10*, 27. [CrossRef]
21. Sang, J.; Alam, M.S. Fragility and Robustness of Binary-Phase-Only-Filter-Based Fragile/Semi fragile Digital Image Watermarking. *IEEE Trans. Instrum. Meas.* **2008**, *57*, 595–606. [CrossRef]
22. Zhang, Y.; Wang, C.; Wang, X.; Wang, M. Feature-Based Image Watermarking Algorithm Using SVD and APBT for Copyright Protection. *Future Internet* **2017**, *9*, 13. [CrossRef]
23. Zhou, X.; Zhang, H.; Wang, C. A Robust Image Watermarking Technique Based on DWT, APDCBT, and SVD. *Symmetry* **2018**, *10*, 77. [CrossRef]
24. Loani, N.A.; Hurrahi, N.N.; Parah, S.A.; Lee, J.W.; Sheikhi, J.A.; MohiuddinBhat, G. Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption. *IEEE Access* **2018**, *6*, 19876–19897. [CrossRef]
25. Castiglione, A.; Pizzolante, R.; Palmieri, F.; Masucci, B.; Carpentieri, B.; De Santis, A. On-Board Format-Independent Security of Functional Magnetic Resonance Images. *ACM Trans. Embed. Comput. Syst.* **2017**, *16*, 1–15. [CrossRef]
26. Wang, C.; Zhang, H.; Zhou, X. A Self-Recovery Fragile Image Watermarking with Variable Watermark Capacity. *Appl. Sci.* **2018**, *8*, 548. [CrossRef]
27. Zhang, F.; Zhang, H. Digital Watermarking Capacity and Reliability. In Proceedings of the IEEE International Conference on e-Commerce Technology, San Diego, CA, USA, 9 July 2004; pp. 295–298.

28. Katti, S.J.; Namuduri, V.R.; Namuduri, K.R. A Practical Approach for Evaluating the Capacity of Watermarking Channel. In Proceedings of the International Conference on Intelligent Sensing and Information Processing, Chennai, India, 4–7 January 2005; pp. 193–198.
29. Kavitha, K.J.; Shan, B.P. Implementation of DWM for Medical Images using IWT and QR Code as a Watermark. In Proceedings of the IEEE Conference on Emerging Devices and Smart Systems, Tiruchengode, India, 3–4 March 2017; pp. 252–255.
30. Pizzolante, R.; Castiglione, A.; Carpentieri, B. Protection of Microscopy Images through Digital Watermarking Techniques. In Proceedings of the International Conference on Intelligent Networking and Collaborative Systems, Salerno, Italy, 10–12 September 2014; pp. 65–72.
31. Ling, H.-C.; Phan, R.C.-W.; Heng, S.-H. Comment on Robust Blind Image Watermarking Scheme Based on Redundant Discrete Wavelet Transform and Singular Value Decomposition. *AEU-Int. J. Electron. Commun.* **2013**, *60*, 894–897. [CrossRef]
32. 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.
33. 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, 2006; pp. 41–72.
34. Bruce, A.M. A Review of Digital Watermarking. Available online: https://pdfs.semanticscholar.org/d6eb/c1a3e1676df1b5a32033417215e8da096ac4.pdf (accessed on 16 February 2020).
35. Chopra, J.; Kumar, A.; Kumar, A.; Marwaha, A. An Efficient Watermarking for Protecting Signature Biometric Template. In Proceedings of the 5th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 22–23 February 2018; pp. 413–418.
36. Singh, A.K.; Kumar, B.; Singh, G.; Mohan, A. *Medical Image Watermarking. Multimedia Systems and Applications*; Springer: Berlin/Heidelberg, Germany, 2017.
37. Qasim, A.F.; Meziane, F.; Aspin, R. Digital watermarking: Applicability for Developing Trust in Medical Imaging Workflows State of the Art Review. *Comput. Sci. Rev.* **2018**, *27*, 45–60. [CrossRef]
38. De Vleeschouwer, C.; Delaigle, J.; Macq, B. Invisibility and Application Functionalities in Perceptual Watermarking-An Overview. *Proc. IEEE* **2002**, *90*, 64–77. [CrossRef]
39. Merrad, A. Implementation of a Biometric Speech Watermarking Based on Wavelet Transform. Ph.D. Thesis, Ziane Achour University of Djelfa, Djefa, Algeria, 2019.
40. Singh, A.K.; Kumar, B.; Singh, S.K.; Ghrera, S.P.; Mohan, A. Multiple Watermarking Technique for Securing Online Social Network Contents Using Back Propagation Neural Network. *Future Gener. Comput. Syst.* **2016**, *86*, 926–939. [CrossRef]
41. 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.* **2016**, *77*, 4863–4882. [CrossRef]
42. Phadikar, A.; Jana, P.; Mandal, H. Reversible Data Hiding for DICOM Image Using Lifting and Companding. *Cryptography* **2019**, *3*, 21. [CrossRef]
43. Yusof, Y.; Khalifa, O.O. Digital Watermarking for Digital Images using Wavelet Transform. In Proceedings of the IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, Penang, Malaysia, 14–17 May 2007; pp. 665–669.
44. Singh, V. Digital Watermarking: A Tutorial. Available online: http://www.cyberjournals.com/Papers/Jan2011/02.pdf (accessed on 16 February 2020).
45. Agbaje, M.; Olugbenga Awodele, O.; Idowu, S.A. Broadcast Monitoring and Applications. *J. Telecommun.* **2012**, *7*, 11–16.
46. Kaur, E.J.; Kaur, E.K. Digital Watermark: A Study. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2012**, *2*, 159–163.
47. Hsu, C.S.; Tu, S.F. Digital Watermarking Scheme for Copyright Protection and Tampering Detection. *Int. J. Inf. Technol. Secur.* **2019**, *11*, 107–119.
48. Hamidi, M.; Chetouani, A.; El Haziti, M.; El Hassouni, M.; Cherifi, H. Blind Robust 3D Mesh Watermarking Based on Mesh Saliency and Wavelet Transform for Copyright Protection. *Information* **2019**, *10*, 67. [CrossRef]
49. Kunhu, A.; Al Mansoori, S.; Al-Ahmad, H. A Novel Reversible Watermarking Scheme Based on SHA3 for Copyright Protection and Integrity of Satellite Imagery. *Int. J. Comput. Sci. Netw. Secur.* **2019**, *19*, 92–102.
50. Furon, T. *A Survey of Watermarking Security*; International Workshop on Digital Watermarking: Siena, Italy, 2005; pp. 201–215.

51. Rashid, A. Digital Watermarking Applications and Techniques: A Brief Review. *Int. J. Comput. Appl. Technol. Res.* **2016**, *5*, 147–150.
52. Adnan, W.A.W.; Hitarn, S.; Abdul-Karim, S.; Tamjis, M.R. A Review of Image Watermarking. In Proceedings of the Student Conference on Research and Development, Putrajaya, Malaysia, 25–26 August 2003; pp. 381–384.
53. Mahajan, J.R.; Patil, N.N. Alpha Channel for Integrity Verification using Digital Signature on Reversible Watermarking QR. In Proceedings of the 2015 International Conference on Computing Communication Control and Automation, Pune, India, 26–27 February 2015; pp. 602–606.
54. Tohidi, F.; Paul, M.; Hooshmandasl, M.R.; Debnath, T.; Jamshidi, H. Efficient Self-embedding Data Hiding for Image Integrity Verification with Pixel-Wise Recovery Capability. In *Pacific-Rim Symposium on Image and Video Technology*; Springer: Cham, Switzerland, 2019; Volume 11854, pp. 128–141.
55. Allaf, A.H.; Kbir, M.A.; Allaf, A.H.; Kbir, M.A. A Review of Digital Watermarking Applications for Medical Image Exchange Security. In *The Proceedings of the Third International Conference on Smart City Applications*; Springer: Cham, Switzerland, 2019; pp. 472–480.
56. Wu, N.I.; Hwang, M.S. Data Hiding: Current Status and Key Issues. *Int. J. Netw. Secur.* **2007**, *4*, 1–9.
57. Celik, M.; Sharma, G.; Saber, E.; Tekalp, A. Hierarchical Watermarking for Secure Image Authentication with Localization. *IEEE Trans. Image Process.* **2002**, *11*, 585–595. [CrossRef]
58. Mukherjee, D.P. Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication. *IEEE Trans. Multimed.* **2004**, *6*, 1–15. [CrossRef]
59. Nikolaidis, N.; Pitas, I. Robust Image Watermarking in the Spatial Domain. *Signal Process.* **1998**, *66*, 385–403. [CrossRef]
60. Habes, A. Information Hiding in BMP Image Implementation, Analysis and Evaluation. *Inf. Transm. Comput. Netw.* **2006**, *6*, 1–10.
61. Abdullatif, M.; Zeki, A.M.; Chebil, J.; Gunawan, T.S. Properties of Digital Image Watermarking. In Proceedings of the IEEE 9th International Colloquium on Signal Processing and its Applications, Kuala Lumpur, Malaysia, 8–10 March 2013; pp. 235–240.
62. Fung, A.G.C.; Junior, W.G. A Review Study on Image Digital Watermarking. In Proceedings of the 10th International Conference on Networks, St Maarten, The Netherlands, 22–23 January 2011; pp. 24–28.
63. Manjula, G.R.; Danti, A. A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography in Spatial Domain. *Int. J. Secur. Priv. Trust Manag.* **2015**, *4*, 11–20.
64. Abraham, J.; Paul, V. An Imperceptible Spatial Domain Color Image Watermarking Scheme. *J. King Saud Univ.* **2019**, *31*, 125–133. [CrossRef]
65. Muyco, S.D.; Hernandez, A.A. Least Significant Bit Hash Algorithm for Digital Image Watermarking Authentication. In Proceedings of the 5th International Conference on Computing and Artificial Intelligence, Bali, Indonesia, 19–22 April 2019; pp. 150–154.
66. Zeki, A.M.; Manaf, A.A. A Novel Digital Watermarking Technique Based on ISB (Intermediate Significant Bit). *World Acad. Sci. Eng. Technol. Int. J. Comput. Inf. Eng.* **2009**, *3*, 444–451.
67. Mohammed, G.N.; Yasin, A.; Zeki, A.M. Robust Image Watermarking Based on Dual Intermediate Significant Bit (DISB). In Proceedings of the 6th International Conference on CSIT, Amman, Jordan, 26–27 March 2014; pp. 19–22.
68. Jane, O.; Elbasi, E. A New Approach in Non-blind Watermarking method Based on DWT and SVD via LU Decomposition. *Turk. J. Electr. Eng. Comput. Sci.* **2014**, *22*, 1354–1366. [CrossRef]
69. Zeki, A.; Abubakar, A.; Chiroma, H. An Intermediate Significant Bit (ISB) Watermarking Technique Using Neural Networks. Available online: https://link.springer.com/article/10.1186/s40064-016-2371-6#citeas (accessed on 16 February 2020).
70. Rathor, B.; Saharan, R. Steganography using Bit Plane Embedding and Cryptography. In Proceedings of the 1st International Conference on Smart System, Innovations and Computing, Jaipur, India, 15–16 April 2017; Volume 79, pp. 319–330.
71. Bender, W.; Gruhl, D.; Morimoto, N.; Lu, A. Techniques for Data Hiding. *IBM Syst. J.* **1996**, *35*, 313–336. [CrossRef]
72. Singh, P.; Chadha, R.S. A Survey of Digital Watermarking Techniques, Applications and Attacks. *Int. J. Eng. Innov. Technol.* **2013**, *2*, 165–175.

73. Wu, X.; Hu, J.; Gu, Z.; Huang, J. A Secure Semi-fragile Watermarking for Image Authentication Based on Integer Wavelet Transform with Parameters. Available online: https://dl.acm.org/doi/10.5555/1082290.1082302 (accessed on 16 February 2020).
74. Yeo, I.N.; Kim, H.J. Generalized Patchwork Algorithm for Image Watermarking. *Multimed. Syst.* **2003**, *9*, 261–265. [CrossRef]
75. Saqib, M.; Naaz, S. Spatial and Frequency Domain Digital Image Watermarking Techniques for Copyright Protection. *Int. J. Eng. Sci. Technol.* **2017**, *9*, 691–699.
76. Meyer-Baese, A.; Schmid, V. Feature Selection and Extraction. In Proceedings of the Pattern Recognition and Signal Analysis in Medical Imaging, Nasreen, Shamila, 27 August 2014; pp. 21–69.
77. Kitanovski, V.; Taskovski, D.; Bogdanova, S. Watermark Generation using Image-Dependent Key for Image Authentication. In Proceedings of the International Conference on "Computer as a Tool", Belgrade, Serbia, 21–24 November 2005; pp. 947–950.
78. Chen, B.; Wornell, G.W. Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding. *IEEE Trans. Inf. Theory* **2001**, *47*, 1423–1443. [CrossRef]
79. Patra, J.C.; Phua, J.E.; Rajan, D. DCT Domain Watermarking scheme Using Chinese Remainder Theorem for Image Authentication. In Proceedings of the International Conference on Multimedia and Expo, Suntec, Singapore, 19–23 July 2010; pp. 111–116.
80. Xu, Z.J.; Wang, Z.Z.; Lu, Q. Research on Image Watermarking Algorithm Based on DCT. *Procedia Environ. Sci.* **2011**, *10*, 1129–1135. [CrossRef]
81. Laouamer, L.; Tayan, O. A Semi-Blind Robust DCT Watermarking Approach for Sensitive Text Images. *Arab. J. Sci. Eng.* **2015**, *40*, 1097–1109. [CrossRef]
82. Roy, S.; Pal, A.K. A Blind DCT Based Color Watermarking Algorithm for Embedding Multiple Watermarks. *AEU-Int. J. Electron. Commun.* **2017**, *72*, 149–161. [CrossRef]
83. Liu, S.; Pan, Z.; Song, H. Digital Image Watermarking Method Based on DCT and Fractal Encoding. *IET Image Process* **2017**, *11*, 815–821. [CrossRef]
84. Vishwakarma, V.P.; Sisaudia, V. Gray-scale Image Watermarking Based on DE-KELM in DCT Domain. *Procedia Comput. Sci.* **2018**, *132*, 1012–1020. [CrossRef]
85. Singh, S.P.; Bhatnagar, G. A New Robust Watermarking System in Integer DCT Domain. *J. Vis. Commun. Image Represent.* **2018**, *53*, 86–101. [CrossRef]
86. Discrete Fourier Transform. Available online: https://en.wikipedia.org/wiki/Discrete_Fourier_transform (accessed on 23 October 2019).
87. Tsui, T.K.; Zhang, X.; Androutsos, D. Color Image Watermarking Using Multidimensional Fourier Transforms. *IEEE Trans. Inf. Forensics Secur.* **2008**, *3*, 16–28. [CrossRef]
88. Poljicak, A.; Mandic, L.; Agic, D. Discrete Fourier Transform Based Watermarking Method with an Optimal Implementation Radius. *J. Electron. Imaging* **2011**, *20*, 033008. [CrossRef]
89. Cedillo-Hernandez, M.; Garcia-Ugalde, F.; Nakano-Miyatake, M.; Perez-Meana, H. Robust Watermarking method in DFT Domain for Effective Management of Medical Imaging. *J. Signal Image Video Process.* **2013**, *9*, 1163–1178. [CrossRef]
90. Ouyang, J.; Coatrieux, G.; Shu, H. Robust Hashing for Image Authentication Using Quaternion Discrete Fourier Transform and Log-Polar Transform. *J. Digit. Signal Process.* **2015**, *41*, 98–109. [CrossRef]
91. Gaata, M.T. An Efficient Image Watermarking Approach Based on Fourier Transform. *International J. Comput. Appl.* **2016**, *136*, 8–11.
92. Jamal, S.S.; Khan, M.U.; Shah, T. A Watermarking Technique with Chaotic Fractional S-box Transformation. *J. Wirel. Peers Commun.* **2016**, *90*, 2033–2049. [CrossRef]
93. Raut, S.S.; Mune, A.R. A Review Paper on Digital Watermarking Techniques. *Int. J. Eng. Sci. Comput.* **2017**, *7*, 10460–10463.
94. Discrete Wavelet Transform. Available online: https://en.wikipedia.org/wiki/Discrete_wavelet_transform (accessed on 23 October 2019).
95. Kehtarnavaz, N. *Digital Signal Processing System Design*, 2nd ed.; Elsevier: Cambridge, MA, USA, 2008.
96. Najafi, E. A Robust Embedding and Blind Extraction of Image Watermarking Based on Discrete Wavelet Transform. *J. Math. Sci.* **2017**, *1*, 307–318. [CrossRef]

97. Chen, Z.; Chen, Y.; Hu, W.; Qian, D. Wavelet Domain Digital Watermarking Algorithm Based on Threshold Classification. In *International Conference in Swarm Intelligence*; Springer: Cham, Switzerland, 2015; Volume 9142, pp. 129–136.
98. Haribabu, M.; Bindu, C.H.; Swamy, K.V. A Secure & Invisible Image Watermarking Scheme Based on Wavelet Transform in HSI color space. In Proceedings of the 6th International Conference on Advances in Computing & Communications, Cochin, India, 6–8 September 2016; pp. 462–468.
99. Jia, S.; Zhou, Q.; Zhou, H. A Novel Color Image Watermarking Scheme Based on DWT and QR Decomposition. *J. Appl. Sci. Eng.* **2017**, *20*, 193–200.
100. Hannoun, K.; Hamiche, H.; Lahdir, M.; Laghrouche, M.; Kassim, S. A Novel DWT Domain Watermarking Scheme Based on a Discrete-Time Chaotic System. *IFAC-Pap. Line* **2018**, *51*, 50–55. [CrossRef]
101. Ambadekar, S.P.; Jain, J.; Khanapuri, J. Digital Image Watermarking through Encryption and DWT for Copyright Protection. *J. Recent Trends Signal Image Process.* **2018**, *727*, 187–195.
102. Wang, J.; Du, Z. A Method of Processing Color Image Watermarking Based on the Haar Wavelet. *J. Vis. Commun. Image Represent.* **2019**, *64*, 1–8. [CrossRef]
103. Singular Value Decomposition. Available online: https://en.wikipedia.org/wiki/Singular_value_decomposition (accessed on 24 October 2019).
104. Chang, C.-C.; Tsai, P.; Lin, C.-C. SVD-Based Digital Image Watermarking Scheme. *J. Pattern Recognit. Lett.* **2005**, *26*, 1577–1586. [CrossRef]
105. Vaishnavia, D.; Subashini, T.S. Robust and Invisible Image Watermarking in RGB Color Space Using SVD. In Proceedings of the International Conference on Information and Communication Technologies, Kochi India, 3–5 December 2014; pp. 1770–1777.
106. Ali, M.; Ahn, C.W.; Pant, M.; Siarry, P. A Reliable Image Watermarking Scheme Based on Redistributed Image Normalization and SVD. *Discret. Dyn. Nat. Soc.* **2016**, 1–15. [CrossRef]
107. Verma, D.; Aggarwal, A.K.; Agarwal, H. Watermarking Scheme Based on Singular Value Decomposition and Homomorphic Transform. Available online: https://aip.scitation.org/doi/abs/10.1063/1.5008715 (accessed on 12 February 2020).
108. Shih, F.Y.; Wu, S.Y. Combinational Image Watermarking in the Spatial and Frequency Domains. *J. Pattern Recognit. Soc.* **2003**, *36*, 969–975. [CrossRef]
109. Sridhar, P. A Robust Digital Image Watermarking in Hybrid Frequency Domain. *Int. J. Eng. Technol.* **2018**, *7*, 243–248. [CrossRef]
110. Kumar, A. A Review on Implementation of Digital Image Watermarking Using LSB and DWT. *Inf. Commun. Technol. Sustain. Dev.* **2019**, *933*, 595–602.
111. Abdulrahman, A.K.; Ozturk, S. A Novel Hybrid DCT and DWT Based Robust Watermarking Algorithm for Color Images. *Multimed. Tools Appl.* **2019**, *78*, 17027–17049. [CrossRef]
112. Savakar, D.G.; Ghuli, A. Robust Invisible Digital Image Watermarking using Hybrid Scheme. *Arab. J. Sci. Eng.* **2019**, *44*, 3995–4008. [CrossRef]
113. Liu, J.; Li, J.; Ma, J.; Sadiq, N.; Bhatti, U.A.; Ai, Y. A Robust Multi-Watermarking Algorithm for Medical Images Based on DTCWT-DCT and Henon Map. *Appl. Sci.* **2019**, *9*, 700. [CrossRef]
114. El-hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors* **2019**, *19*, 1141. [CrossRef]
115. Dobre, R.A.; Preda, R.O.; Oprea, C.C.; Pirnog, I. Authentication of JPEG Images on the Blockchain. In Proceedings of the International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO), Prague, Czech Republic, 19–21 May 2018; pp. 211–215.
116. Yongliang, L.; Gao, W. Secure Watermark Verification Scheme. In Proceedings of the International Conference on Multimedia and Expo (ICME), Taipei, Taiwan, 27–30 June 2004; pp. 923–926.
117. Huang, C.; Wu, J. Attacking Visible Watermarking Schemes. *IEEE Trans. Multimed.* **2004**, *6*, 16–30. [CrossRef]
118. Agarwal, N.; Singh, A.K.; Singh, P.K. Survey of Robust and Imperceptible Watermarking. *Multimed. Tools Appl.* **2019**, *78*, 8603–8633. [CrossRef]
119. Nyeem, H.; Boles, W.; Boyd, C. Digital Image Watermarking: Its Formal Model, Fundamental Properties and Possible Attacks. *EURASIP J. Adv. Signal Process* **2014**, *135*, 1–22. [CrossRef]
120. Chitra, K.; Venkatesan, V.P. Spatial Domain Watermarking Technique: An Introspective Study. In Proceedings of the International Conference on Informatics and Analytics, Pondicherry, India, 25–26 August 2016; pp. 1–6.

121. Varshney, Y. Attacks on Digital Watermarks: Classification, Implications, Benchmarks. *Int. J. Emerg. Technol.* **2017**, *8*, 229–235.
122. Lin, C.; Wu, M.; Bloom, J.A.; Cox, I.J.; Miller, M.L.; Lui, Y.M. Rotation, Scale, and Translation Resilient Watermarking for Images. *IEEE Trans. Image Process.* **2001**, *10*, 767–782. [CrossRef]
123. Dittmann, J.; Wohlmacher, P.; Nahrstedt, K. Using Cryptographic and Watermarking Algorithms. *IEEE Multimed.* **2001**, *8*, 54–65. [CrossRef]
124. Kutter, M.; Voloshynovskiy, S.V.; Herrigel, A. Watermark Copy Attack. Available online: http://www.alpvision.com/pdf/ei2000_ol.pdf (accessed on 16 February 2020).
125. Soman, K.P.; Ramachandran, K.I. *Insight into Wavelets, from Theory to Practice*, 3rd ed.; PHI Learning: Delhi, India, 2010.
126. Sara, U.; Akter, M.; Uddin, M.S. Image Quality Assessment through FSIM, SSIM, MSE, and PSNR-A Comparative Study. *J. Comput. Commun.* **2019**, *7*, 8–18. [CrossRef]