*electronics*

MDPI

*Review*

# Secure Watermarking Schemes and Their Approaches in the IoT Technology: An Overview

**Raniyah Wazirali [1], Rami Ahmad [2,*], Ahmed Al-Amayreh [3], Mohammad Al-Madi [4] and Ala' Khalifeh [5]**

[1] College of Computing and Informatics, Saudi Electronic University, Riyadh 11673, Saudi Arabia; r.wazirali@seu.edu.sa
[2] The School of Information Technology, Sebha University, Sebha 71, Libya
[3] Department of Information Technology, University of Technology and Applied Sciences, Suhar 311, Oman; ahmeda.soh@cas.edu.om
[4] Faculty of Computer Studies, Arab Open University, Riyadh 23437, Saudi Arabia; m.almadi@arabou.edu.sa
[5] School of Electrical Engineering and Information Technology, German Jordanian University, Amman 11180, Jordan; ala.khalifeh@gju.edu.jo
* Correspondence: r_a_sh2001@yahoo.com

**Abstract:** Information security is considered one of the most important issues in various infrastructures related to the field of data communication where most of the modern studies focus on finding effective and low-weight secure approaches. Digital watermarking is a trend in security techniques that hides data by using data embedding and data extraction processes. Watermarking technology is integrated into different frames without adding an overheard as in the conventional encryption. Therefore, it is efficient to be used in data encryption for applications that run over limited resources such as the Internet of Things (IoT). In this paper, different digital watermarking algorithms and approaches are presented. Additionally, watermarking requirements and challenges are illustrated in detail. Moreover, the common architecture of the watermarking system is described. Furthermore, IoT technology and its challenges are highlighted. Finally, the paper provides the motivations, objectives and applications of the recent secure watermarking techniques in IoT and summarises them into one table. In addition, the paper highlights the potential to apply the modified watermark algorithms to secure IoT networks.

**Keywords:** watermarking technology; embedding and extraction; IoT security; WSN security; perception layer



**Citation:** Wazirali, R.; Ahmad, R.; Al-Amayreh, A.; Al-Madi, M.; Khalifeh, A. Secure Watermarking Schemes and Their Approaches in the IoT Technology: An Overview. *Electronics* **2021**, *10*, 1744. https://doi.org/10.3390/electronics10141744

Academic Editors: Il-Gu Lee, Kyungmin Go and Jung Hoon Lee

Received: 16 June 2021
Accepted: 17 July 2021
Published: 20 July 2021



## 1. Introduction

As the concept of Internet of Things (IoT) has emerged as a powerful and flexible infrastructure for a wide range of services, which in turn significantly increased the volume of generated data. However, this large volume of data is digitally preserved and accompanied by a number of complications, such as copyright infringement and authentication [1], through data manipulation, copying and redistribution processes [2,3]. Such data processes are implemented in either a legal or illegal manner, and different approaches are used to hide data such as watermarking, cryptography and steganography [4]. Steganography is the art and science of undetectable communication that is accomplished when hiding information through other available information. Therefore, it is extremely effective in securing the process of access control [5]. Moreover, cryptography is one of the old techniques used in authentication to overcome illegal manipulations of data [1,6]. Nonetheless, the main risk of such an approach is that data can be decrypted causing an unprotected classified content. To mitigate such issues, the so-called digital watermarking is proposed and is considered one of the focal points of research for many researchers recently [7–10].

Digital watermarking has also become a significant subject in the field of multimedia signal processing, where it can be defined as an invisible change to a piece of data. Addi-

tionally, it can be considered as an enhanced method that can provide protection to the ownership of the digital media against digital piracy [2].

Recently, digital watermarking technology became essential for different fields as it offers various lightweight solutions for several techniques and applications, including cloud computing, electronic health and IoT [11,12]. Furthermore, confidentiality, integrity and availability are completely supported for sensitive data/information [13]. In the same context, the IoT is widely used in the future, and the IoT security highlights different issues, meantime, the Wireless Senior Network (WSN) approach is considered as a vital spirit and heartbeat infrastructure for several IoT applications and domains [14]. This approach uses a variety of low-cost and low-power internet-connected devices such that these devices sense their surrounding data from different situations and forward them to the Internet [15]. Therefore, energy consumption and security remain the two main challenges in WSNs that need improvement due to their limited resource and outdoor operation. Moreover, sending and broadcasting sensitive information over unsafe network media are still considered to be challenging issues as well [12]. In addition, the traditional security mechanism relying on public key, private key, digital signature, and digital certification in transport layer sockets is not suitable for such types of devices due to the cost of encryption and decryption operations. These challenging issues make techniques such as lightweight security algorithms and watermarking systems a viable choice for these types of devices. Furthermore, these limitations encouraged researchers to study and investigate the domain of various watermarking methods in fields related to IoT [15,16]. However, different watermarking attacks still need mitigation handling such as rotations, copping and compression [17,18] that can be available within the acceptable limits.

The watermarking method is executed based on three consecutive processes, comprised of generation, embedding, and extraction. These processes are illustrated in Figure 1.

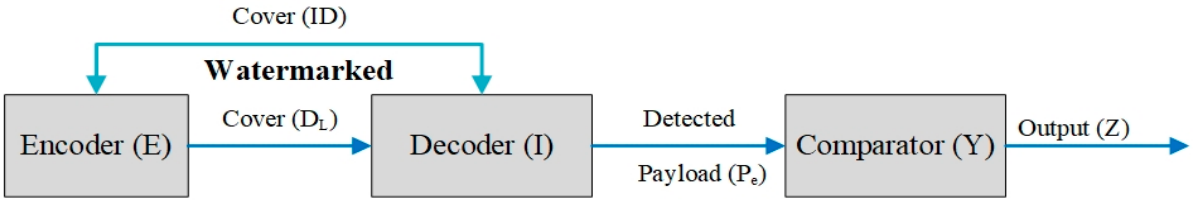


**Figure 1.** General watermarking system for multimedia objects [19].

First, the payload is encoded into a cover object (D) for generating an object that is watermarked. Last, the payload is identified through a decoder. The payload ($P_L$) is considered as a confidential message or information, which is embedded through a cover and the entire information or watermarked image ($D_L$) is forwarded through to a decoder while the payload detection procedure is involved. Following the detection process, the output message is decoded. Moreover, in the embedding domain, watermarking techniques are categorised into time or frequency domains [20]. The hiding algorithms use different related algorithms such as Singular Value Decomposition (SVD), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT). In the extraction domain, the watermark retrieval process is defined as the reverse process that is based on the embedding process [21]. These processes use low weight calculations, which cause low consuming energy [16]. Therefore, the advantages of using watermarking methods in IoT include:

- No additional overhead is added on the wireless frame.
- Data security is always guaranteed.
- Reduce the end-to-end delay.
- Low power consumption is attained due to the utilized lightweight calculations.

Furthermore, the watermarking technique is beneficial when protecting digital data, although after its decryption process. Therefore, such a technique assists in averting the

illegal usage of personal information and defends it from illegal and fraudulent users. Nonetheless, cryptography is based on protecting the contents at the time of transit and not following the time of completing the decryption process. Digital watermarking can embed the digital data through a covered digital data for copyright protection, authentications and annotation purposes. Watermarking must be effective based on many different processes, such as geometrical manipulation, re-encryption and decryption [22].

An overview of different watermark techniques, which are related to different approaches, is presented in [20,23–30]. However, none of these studies discussed the use of the watermark field in IoT applications. Therefore, the main contributions of this paper can be summarized as follows:

- A comprehensive survey is provided on various secure watermarking schemes within the IoT networks that have been proposed to deliver robustness and integrity throughout the watermark and security environments. In particular, the paper highlights the most recent studies in watermarking with different approaches such as: hashing, deep learning, encryption, and fragile.
- Several challenges that can be addressed in IoT network traffic with the help of watermark technology have been examined.

In this paper, we provide a comprehensive background on watermarking technology in Section 2. In Section 3, a background on the IoT and its challenges is presented. Section 4 demonstrates a number of modern studies that use different watermarking schemes within different IoT applications. A discussion and open issues are clarified in Section 5. Finally, Section 6 draws the conclusion of this paper.

## 2. The Concept of Watermarking

In general, the watermarking technique involves embedding and extraction phases [31] as illustrated in Figure 2. The embedding process allows users to include watermarks within their digital content (multimedia objects) for a variety of reasons such as authentication, copyright protection, etc. After that, the secret key is added to the embedding process in order to insert the secret data into the multimedia object by using a number of relevant transformations or spatial techniques [32]. Moreover, another technique can be used along with the secret key for improving data authentication such as encryption, hashing and encoding [33]. The watermarked object is defined as the output, which is produced from the embedding algorithm where the same secret key is used to embed the watermark that is used again for extracting the data from the watermarked object.

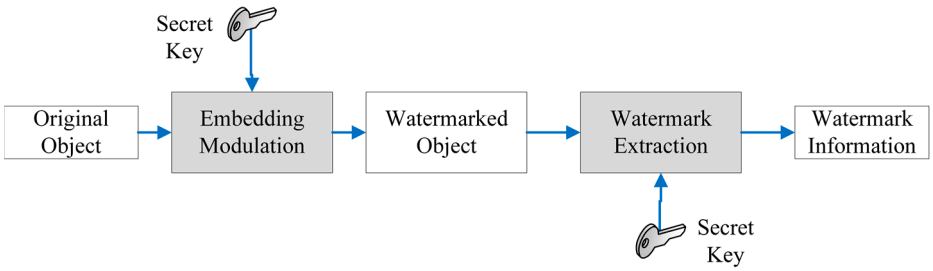


**Figure 2.** The watermarking Technique.

The extracted watermark may or may not resemble the pristine watermark due to the encountered attack. Therefore, there are three types of watermarking procedures, which are used to measure the properties of these procedures. These types include: non-blind, blind and semi-blind procedures. In the non-blind procedure, the pristine object and secret key are essential in determining the extracted watermark, while in the blind procedure the pristine object does not necessarily determine the extracted watermark. In the semi-blind procedure, the secret key is only by means applied for extracting the data [34].

The two phases of watermarks are discussed in detail as follows.

### *2.1. Embedding Domain*

In the embedding phase, the watermarking techniques can be categorised into spatial domain (time) or transform domain (frequency). Therefore, the aim of hiding information is to preserve the availability of the secret message, which is usually being undetermined by an unauthorised access [35]. Various hidden algorithms are used in embedding watermarks that range from as simple as Least Significant Bit (LSB) to sophisticated transformation techniques, such as DWT, Discrete Fourier Transform (DFT), SVD and Discrete Cosine Transform (DCT) (see Figure 3).

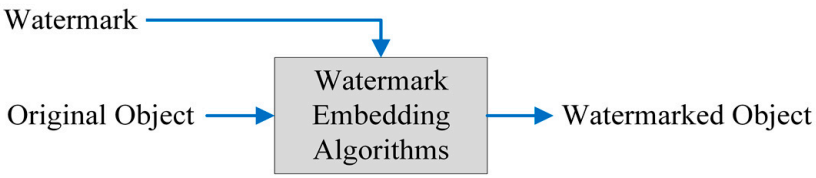


**Figure 3.** The Watermark Embedding process.

As illustrated in Figure 3, the original object represents the input, and the hidden algorithm is applied through the process of embedding the watermark. Following that, the output represents the watermarked object. The hidden algorithms are discussed in detail as follows:

#### 2.1.1. Singular Value Decomposition

The SVD technology converts an object from an array into three arrays that are similar in their sizes to the original matrix. Assume that $A$ is an object and that the SVD is defined by Equation (1) [36–38].

$$A = USV^T \tag{1}$$

where the $U$ and $V$ components denote the orthogonal metrics with small singular values and the $S$ denotes the diagonal matrix with larger singular value entries as given in Equation (2).

$$S = \begin{bmatrix} \sigma_1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 2 & \dots & \sigma_n \end{bmatrix} \tag{2}$$

where, $\sigma$'s (diagonal elements) denote the singular values that satisfy Equation (3) as follows:

$$\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_n \geq 0 \tag{3}$$

Typically, the methods that rely on the SVD technology can explore the decomposition of a single value, which is related to an object. After that, the singular values are replaced by its surrounding watermark.

#### 2.1.2. Discrete Wavelet Transform

DWT technique is applied for many different applications, which include the signal processing domain. The main idea of DWT technique is to split objects into a number of frequency channels. Nonetheless, the bandwidth is preserved through the technique according to a logarithmic scale, i.e., the 'Multi-resolution analysis' [39]. Thus, several steps are considered when applying the conversional process. Different approaches such as the diagonal or High–High (HH), vertical or High–Low (HL), approximation or Low–Low (LL), and horizontal or Low–High (LH) entirely represent different sub-bands related to an object that is decomposed by using the 1-level DWT technique (see Figure 4). In the rows of the DWT, the first letter represents the high or low-pass frequency. In the columns of the DWT, the second letter represents the filter. The first three sub-bands, which include the HL, LH, HH and sub-bands, are based on the best scale of wavelet coefficients.

The last sub-band, LL, is based on rough scale wavelet coefficients. The LL functions efficiently once an additional level is gained during the decomposition procedure where it is persistently analysed for a determined objective until the required number within the level of decomposition is provided [40].

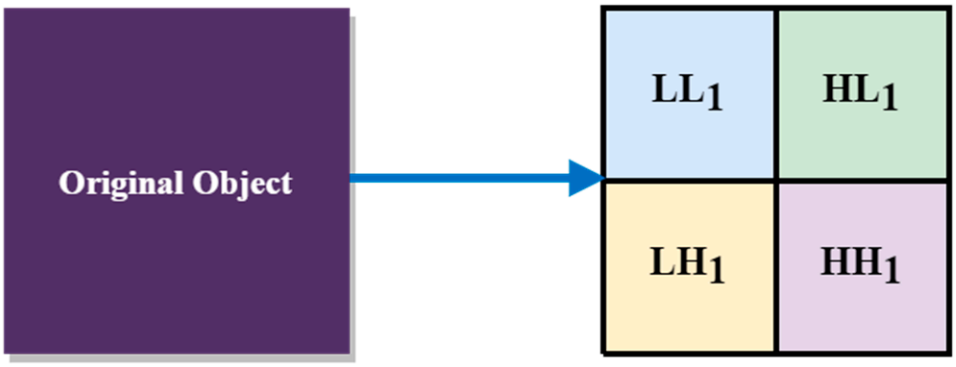


**Figure 4.** One Level Decomposition with the DWT technique.

#### 2.1.3. Discrete Fourier Transform

Fourier Transform (FT) is a functioning method, which transforms an incessant task into its own frequency components. The corresponding transform pertaining to the valued task, which is discrete, should obtain the DFT technique. In the domain of digital object processing, the even tasks are demonstrated as the cosine's integral part if these tasks are aperiodic. These functions are multiplied by weighing function where this function performs the coefficients, which are in relation to the signal FT. The analysis and processing of a signal are conducted by the Fourier transform technique through its frequency domain by replacing and analysing relevant coefficients [41].

#### 2.1.4. Edge Detection

The exploration and development of the Edge Detection Technique (EDT) represent an integral part of algorithms, which are based on object detection as the EDT introduces the object outline [42]. The EDT hides data, which represents an efficient approach that should be taken into account since it assures perceptual transparency when the embedding capacity is found sufficiently huge [43]. Many different edge detection algorithms are produced for applying them to solve issues related to data hiding as Sobel and Canny detectors [3].

#### 2.1.5. Discrete Cosine Transform

The DCT technique considers the frequency domain as a significant feature. An object is shown as a group of sinusoids accompanied by various magnitudes and frequencies. This procedure is performed through many DCT methods. In particular, an object is split into three different frequency chunks that include: Medium Frequency (LF), Low Frequency (LF) and High Frequency (HF). In fact, a datum or message is hidden within a medium frequency region as it is found to be the best region for hiding a datum or message. If keeping a message appears within low frequency regions, it can be obviously viewed by human eyes. Consequently, if keeping a message appears within regions of higher frequencies, an object turns to be inaccurate as its frequency is spread all over the largest block regions along through the corner, which is situated at the bottom right side. Afterwards, this causes a local deformation, which is connected with the EDT. Therefore, the medium frequency regions do not affect the quality of an object [36,44].

#### 2.1.6. Least Significant Bit

This LSB represents a conventional approach that embeds the watermark into the LSB pixels. The approach can be easily exploited through various fields. Furthermore, no distortion is generated via this approach into an object. Nevertheless, the approach is not effectively compared with the encountered attacks. The watermark embedding approach is performed based on determining a subset, which involves an object's pixels. The least significant bit for each determined object pixel is substituted with different watermark bits. The watermark is disseminated through to an object or through to different identified locations of an object. On the other hand, this approach is found susceptible to various attacks as the watermark is easily demolished. Moreover, the approach encounters different data noises and signal processing. Accordingly, the approach is not implemented through a number of applied applications [45].

#### 2.1.7. Optimal Pixel Adjustment Process

To eliminate the distortion produced by LSB replacement, the authors in [46] suggested a simple and efficient optimal pixel adjustment process (OPAP) approach. If message bits are contained in the right-most $r$ LSBs of an $m$-bit pixel, the other $m - r$ bits are modified by a straightforward assessment, according to their manner. These $m - r$ bits are either replaced by the adjusted result or left unchanged if the adjusted result delivers a lower distortion.

#### 2.1.8. Pixel Pair Matching

Pixel pair matching is another interesting watermarking technology. These embedding algorithms typically employ the pixel pair $(p_{i,1},\ p_{i,2})$ as a reference station to find additional positions $(p'_{i,1},\ p'_{i,2})$ inside a preset nearby set of $\phi(p'_{i,1},\ p'_{i,2})$ to satisfy $f(p'_{i,1},\ p'_{i,2}) = SB$. Where $f$ denotes the extraction function and $SB$ is the secret number in the B-ary coding system [47]. Moreover, the authors in [48] proposed the adaptive pixel pair matching approach. As an embedding unit, two pixels are scanned, together with a specifically built neighbouring array.

#### 2.1.9. Discrete Shearlet Transform

In this approach, various band transforms have been evolving till now based on several significant steps that are featured by information processing, which relies on an increased efficiency characteristic, and on the conservation of different conventional approaches, which are based on the multi-resolution analysis. Some examples that are related to this approach include the Contourlet, Shearlet and Curvelet. The Discrete Shearlet Transform (DST) approach represents a well-localised waveforms pyramid, while varied orientations are enclosed by this pyramid involving various locations, scales and shapes when classical wavelets are produced differently from them. Therefore, classical wavelets are applied with the state-of-the-art algorithms within the domains of object and signal processing domains. Furthermore, their processes are efficient in resolving relevant problems, which rely on different multi-scale systems such as the fragile direction that are based on such systems. Shearlet transform [49] is defined as structuring the affine system for detecting different geometrical structures, which are based on various signals of dimensions [50].

In addition, there are other algorithms that are used to embed watermarks in objects such as Patchwork and Intermediate significant bit [20]. Patching is a random statistical method that is invisibly used in an original image by a Gaussian distribution using a repeated mark-up pattern while the intermediate significant bit was developed to improve LSB by replacing the original pixels of the images within the blank/filled area with watermark pixels [51]. Moreover, a histogram shifting can be used to include the secret data into the compressed images [52]. This technique examines the pixel histograms of the cover image and looks for pairs of peak and zero values. During the data embedding process, the pixels between the peak and zero points are changed. The 1-bit hidden data are embedded in each pixel in the peak points. The others have been altered, and no hidden information

has been embedded. The maximum hiding ability for the hidden data to be embedded in this scheme is the number of pixels in the peak points.

### *2.2. Extraction Domain*

The watermark retrieval procedure represents a reverse procedure, which relies on the embedding procedure (see Figure 5). The input of such a procedure refers to an object once the watermark is embedded through to it. The output represents the original watermark, which is created via the generation procedure. Matching should be performed if the embedded object cannot be modified when different attacks are encountered.

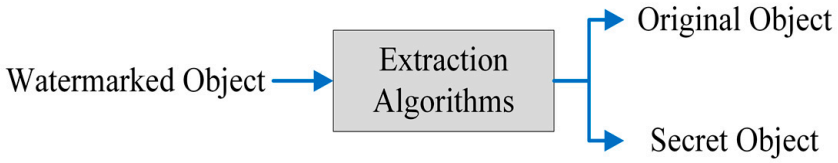


**Figure 5.** The watermark extraction procedure.

### *2.3. The Watermarking Performance Metrics*

Many different performance metrics are used to perform the correlation testing for different types of watermarking procedures (non-blind, blind and semi-blind). Some of the standard performance metrics are discussed in the following subsections.

#### 2.3.1. Bit Error Rate (*BER*)

This metric calculates invalid bits' percentage in comparison with the overall bits' number, which is sent through to the watermarking procedure. If the *BER* reaches 0, this implies that it indicates to the existence of a watermark. However, it can also indicate to the absence of a watermark if the *BER* does not reach 0 [53]. The *BER* is presented in Equation (4) as follows:

$$BER = \frac{number\ of\ invalid\ bits}{total\ number\ of\ bits} \tag{4}$$

#### 2.3.2. Peak Signal to Noise Ratio (*PSNR*)

The *PSNR* represents an effective measure for providing different comparisons among the obtained results of the same objects. However, conducting object comparisons with the *PSNR* is found to be pointless [2]. The *PSNR* is presented in Equation (5) as follows:

$$PSNR = 10log_{10}\left(\frac{R^2}{MSE}\right) \tag{5}$$

where, $R$ denotes the maximum possible value for each pixel within an object, and the Mean Square Error (*MSE*) is represented in Equation (6) as follows:

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M \times N} \tag{6}$$

where, $M$ and $N$ denote the number of rows and columns within the patterns of an object, respectively. $I_1(m, n)$ denotes the value or the intensity that is related to the pixel, and which is exactly situated at the position $(m, n)$ according to the watermarked object. Additionally, $I_2(m, n)$ denotes the relevant pixel intensity within the original object. The *MSE* is related to an object intensity's scaling [54].

2.3.3. Signal to Noise Ratio (*SNR*)

This metric calculates the signal's strength, which is based on the background noise. Additionally, it calculates an object's sensitivity [30]. The formula of calculating the *SNR* can be shown in (7) as follows:

$$SNR = 10log_{10}\left(\frac{P_{noise}}{P_{signal}}\right) \tag{7}$$

2.3.4. Capacity

This metric calculates the maximum bits of data that can be stored in the object without affecting the visibility of data [55]. Capacity is presented in (8) as follows:

$$\text{Capacity} = \frac{number\ of\ secret\ bits}{total\ number\ of\ object\ bits} \tag{8}$$

Moreover, this scale also known as the payload which defines the limitations of the watermark information while ensuring that the watermark is robust and imperceptible. The ability of the watermark is determined by the information available to the attacker, the data encoder and decoder, the distortion restrictions, and the statistical model used in the jacket object [20,56].

2.3.5. Structural Similarity Index (*SSIM*)

This metric calculates the similarity between the watermarked object and pristine object. The SSIM value selects ranges from $-1$ to 1, and when the $SSIM = 1$, this implies that the similarity between them represents the top [5]. The SSIM is presented in (9) as follows:

$$SSIM(x,y) = \frac{\left(2u *_x u_{y+a_1}\right)\left(2o_{xy} + a_2\right)}{\left(u_x^2 + u_y^2 + a_1\right)\left(o_x^2 + o_y^2 + a_2\right)} \tag{9}$$

where $x$ and $y$ are two windows of an object, $u_x$ denotes the average of $x$, $u_y$ is the average of $y$, $o_y^2$ is the variance of $y$, $o_x^2$ is the variance of $x$, $o_{xy}$ is the covariance of $x$ and $y$, $a_1$ and $a_2$ variables use to stabilize the division.

2.3.6. Correlation Coefficient

The Correlation Coefficient (*CC*) is commonly used in signal processing and image processing to find similarity between two signals (or objects) [56]. The correlation coefficient equation is represented in (10) as follows:

$$CC = \frac{\sum_i \sum_j W_{ij} W'_{ij}}{h \times w} \tag{10}$$

where $W_{ij}$ and $W'_{ij}$ are the values in $(i,j)$ of the embedded and extracted watermark as well as set to 1 if the if the watermark bit is 1 otherwise set to $-1$; and $h$, $w$ are the height and width of the watermark, respectively.

*2.4. The Major Classification of Digital Watermarking Techniques*

Different methods of classifying watermarks by a document's type (image, text, video and audio) are designed to increase transparency and durability. Different watermark techniques are classified into the following main types (see Figure 6) [28].

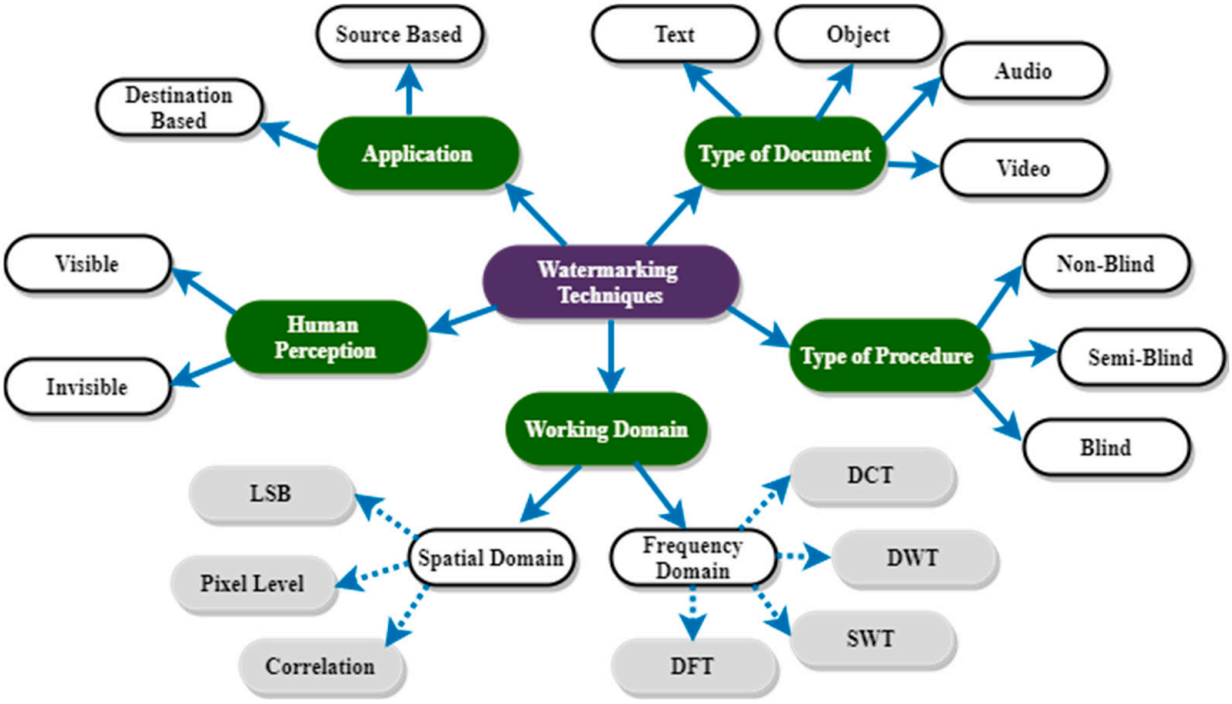


**Figure 6.** The major classification of different watermark techniques [28].

#### 2.4.1. Application's Perspective

The watermark could be source-based or destination-based. The source-based watermark could be used to verify the ownership and recognize authorized people, trace the marked document's publishing through the network, inform users about the rights-holder or the permissible use of the data evidence [57]. The buyer-seller identification is a type of destination-based watermark [58,59] where each distributed copy of the product obtains a unique identification of the watermark that relates to a particular purchaser. Further, the destination-based watermark traces illegal reselling in case a buyer is caught to commit such an action. This act is being used in fingerprinting procedures.

#### 2.4.2. Human's Perception

In this classification, watermarking techniques are categorized into invisible and visible watermark techniques [60]. In invisible watermarking techniques, information is hidden inside the object [42]. The hidden process can be performed based on three techniques, which are: robust, fragile and semi-fragile techniques [61]. The robust technique is mostly used to verify the intellectual property rights as it is resistant to many various attacks. Meanwhile, the fragile technique is used to validate owner authentication and data integrity. The semi-fragile technique combines robust and fragile techniques where fragile techniques function against malicious attacks, while robust techniques function against intentional attacks [62].

#### 2.4.3. Type of Documents

The watermarking principle is implemented by encoding a redundant message based on the use of various low-amplitudes and the modifications of pseudo-noise for the original document. For instance, the hidden message is embedded in the text document by updating various paragraphs of that type of document. An entire line or a multiple text can be shifted up or down using small distances, typically, 0.180 or 0.095 mm.

On the other hand, words that can be shifted might be in the same way placed horizontally where words or blocks of words can be shifted individually [63]. Implementing watermarks for images is performed differently where pixel intensities are typically modified or coefficients can be transformed. Many of the image watermarking algorithms can

be used directly for video since the digital video is considered as a sequence of images. However, the scenario of individual images varies, in large video bandwidth, long messages can be included within that video stream. Due to the large volume of processed data, speed is considered to be a critical issue [25].

#### 2.4.4. Watermarking Work Scope

Watermarking techniques are categorised into spatial and frequency domains. Spatial watermarking domain refers to the modification (or replacement) of the content of an object including an effect that is minimally noticed. For instance, the LSB technique could be an ideal example. This technique functions by substituting some of the information in particular pixels including the information from an object data. The technique is also applied by substituting the slightly less significant bit(s). Nonetheless, this substitution decreases the contrast or intensity of an object [64].

In the frequency domain, the multimedia hidden data domain is converted to other formats, after which it is overwritten based on the hidden data. This domain includes many different techniques such as DCT, DFT, DWT and SVD techniques. The DWT and DCT techniques are two of the most commonly used techniques for watermark conversions. In practice, higher object imperceptibility is provided by these two techniques, which in turn demonstrate a robust action against watermark attacks and object manipulation [42].

### *2.5. Watermarking Requirements*

One of the main issues in the field of watermarks is the competition among these requirements [8], which includes imperceptibility, robustness, security, informed or blind detection, fragility, capacity and the cost of the watermark. These requirements are illustrated in Figure 7 and are defined as follows:

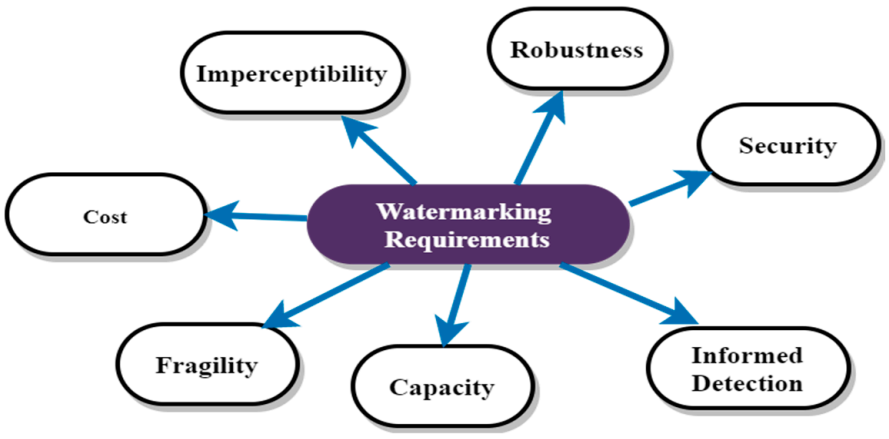


**Figure 7.** The Main Watermarking Requirements.

#### 2.5.1. Imperceptibility

An embedded watermark is considered truly imperceptible if the user is not able to distinguish between the original multimedia and its watermarked form.

#### 2.5.2. Robustness

This means that the watermark should not be altered or removed from the robustness feature without having sufficient degradation in the perceptual quality of the host multimedia [65,66].

#### 2.5.3. Security

This requirement indicates how secure the multimedia coverage and watermark are against unauthorized users. Based on the assumption of Kirchhoff, the security of the encryption techniques must opt for the selection of a key. Kerckhoffs's principle [67] is a

well-known assumption in cryptography which assumes that the encryption algorithm should be public, and the used secrete key is the private and unknown element in the encryption process. Consequently, the security relies on the key secrecy. Watermarking follows this principle since the attacker is assumed to know the extraction and embedding functions used in the watermarking process which have no secrete parameters. Furthermore, the attacker observes the watermark vectors from the contents he has access to. Therefore, the security of watermarking methods follows Kerckhoffs's principle. Additionally, steganography is being improved and an extremely effective technique is being used in order to provide security to the required data. Therefore, there exist three significant and necessary characteristics that are in relation to the security of objects, which include: confidentiality, reliability and availability [8]. However, adding different encoding methods such as hashing, deep learning, encryption, and fragile with watermark will enhance the authentication and data integrity at a lower power level for WSN nodes [68].

#### 2.5.4. Informed or Blind Detection

The original non-watermarked multimedia that is original should exist in some applications through the extraction or detection phase. For instance, it is normal for the owner of the original multimedia to detect how a provided copy is illegally disseminated and by whom in a transaction-tracking application [69]. A non-watermarked multimedia form must still be available with the owner where this form must be given to the extractor including the illegal copy [7].

#### 2.5.5. Cost of Watermark

The economics of regulating watermark extraction and embedding can be extremely difficult and complex to implement in many watermarking companies depending on the business models that are involved. In practice, this problem depends on the speed at which extraction and embedding processes must be done based on the number of extraction and embedding tools to be regulated [70].

#### 2.5.6. Fragility

This requirement measures the ability of digital watermark to detect the original data modification.

### *2.6. Application of Digital Watermarking*

Watermarking algorithms possess many uses and applications, these applications are illustrated in Figure 8 where the followings highlight further details about them:

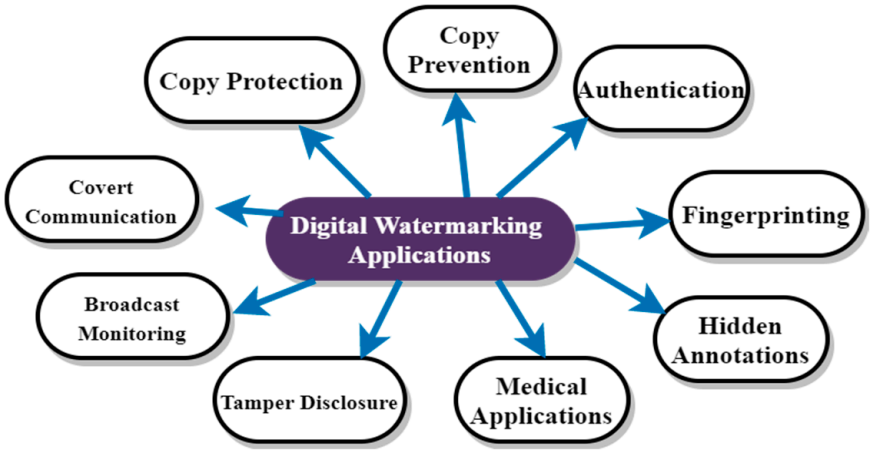


**Figure 8.** The Digital Watermarking Applications.

#### 2.6.1. Copyright Protection

This type of application is very well-known in implementing the digital watermarking technique. The data owner is determined by a few relevant data, which corresponds to it [71].

#### 2.6.2. Copy prevention

Copy prevention of text documents is protected based on the use of different text watermarking algorithms. In fact, such a watermarked information may handle any type of request device related to copying and recording (e.g., a copy and paste order or a printer). The watermark adds a key to represent a copy permission, which forms a bit stream that is realized by a software where a decision is produced once the copy is seen either legal or prohibited. Hence, it persists to proceed along with the legal ones and neglect other illegal ones [72].

#### 2.6.3. Authentication

Changing the content of the data is extremely simple when multimedia editing programs are applied. A digital signature establishes an integral role for the content summary [73]. After that, the signature is changed if any change occurs in the content by indicating a gap to that content [74].

#### 2.6.4. Fingerprinting

It is defined as the process of integrating data and information for every copy obtained from a digital content. The watermarking technique is the most effective technique for this application type. The reason behind this effectiveness refers to the invisible watermarking property, which is accompanied by the content. The significance of this application is based on tracing copies, which are illegally published [42,75].

#### 2.6.5. Hidden Annotations

It is considered to be one of the watermarking's features in medical applications where some hidden explanations or addresses are provided to display the records of the entire patient. Furthermore, it can be applied in various multimedia indexing and retrieval applications [76].

#### 2.6.6. Medical Applications

In this application, the watermarking method is created based on the negotiation on several needs such as the capacity, robustness, privacy and imperceptibility [42]. A patient can obtain some benefits and the right for a cure according to some significant tasks, which are derived by particular reports. A catastrophe might be encountered if many patients possess two mixed reports [8]. The mixture of the DWT and DST apply the edge detection process, which can satisfy different types of objectives.

However, the embedded message has a high degree of importance and this type of host object (i.e., the medical image) is also important. The host object must maintain its quality without distortion, as modifying the patient's medical picture, for example, can have a negative impact on the patient's life by causing errors in diagnosis and treatment. As a result, reversible watermark systems were created to address this flaw by incorporating technology that can restore both the internal watermark and the original image. To authenticate images, reverse watermarking methods can be used. Reverse watermarks will provide workplace optimization for authentication applications; The authentication component ensures the integrity of the image, while the reflection feature maintains the quality [72]. Digital watermark can be thought of as a specific case of reverse watermark.

#### 2.6.7. Tamper Disclosure

A huge number of documents are made available online for reading where such documents can encounter many different attacks such as unauthorized access, redistribution

and copying. Tamper disclosure is an application that uses the watermarking technique for detecting and recovering tampered areas from the original document contents [72].

#### 2.6.8. Broadcast Monitoring

A particular watermark is added into the entire objects (e.g., audios, images, texts and videos) for checking the required broadcast. Additionally, data owners can track the required broadcast based on different communication techniques, such as phone, radio and TV. This information is disseminated through the Internet. Nonetheless, the data are marked by including the owner's name, date, and time, which are entirely added as markers in order to easily identify them [77]. Detectors are embedded in order to obtain and proceed along with the broadcast through routers, stations or hubs. To identify the broadcasting features, the digital watermark is decoded and applied. Information and data are recorded for licensing and financing purposes in the future research. Nevertheless, a comparison is conducted for the information that is broadcasted with the final decisions based on an automatic monitoring [78].

#### 2.6.9. Covert Communication

The following application pertaining to the text watermarking technique represents the transferring process related to the private data (e.g., images or plain texts). Hidden communication represents the addition of a covert message into an unacceptable looking text based on a particular method, which has not yet been discovered in reality, its meaning except for the intended receivers. Further, the related algorithms pertaining to text watermarking techniques are applied for secret communications [72].

### *2.7. Watermark Challenge*

Watermark attacks on digital objects fall into two types, consisting of non-intentional and intentional attacks. The attack aims to degrade the watermark outline if the watermark degrades are extremely apart from the acceptable limits. There are different types of attacks that are categorized as depicted in Figure 9.

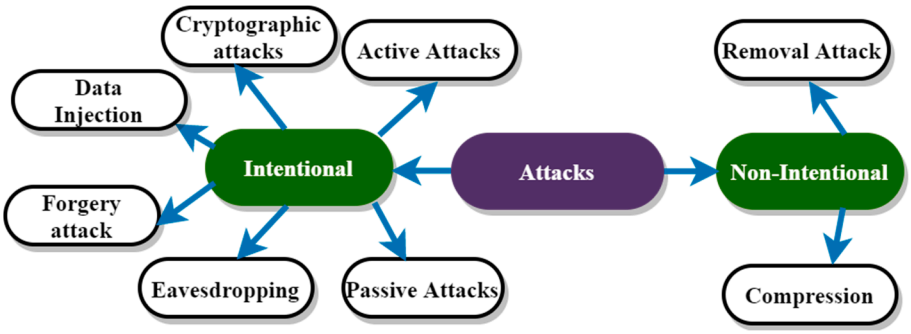


**Figure 9.** Different types of intentional and non-intentional attacks.

Intentional attacks typically involve the use of computer coding or other technical devices, which are designated to cause some unwanted issues. Meanwhile, non-intentional attacks include software bugs that occur during the programming of a computer system or system configuration. However, these divisions are relative and may overlap with each other.

#### 2.7.1. Removal Attack

Removal attacks aim to remove the watermarking data from the watermarking object. Based on these attacks, watermarking represents an additional noise of signals, which are present within the host's signal [79,80].

#### 2.7.2. Compression

The type of this attack represents an unintentional attack, which emerges repeatedly through various applications that involve multimedia. In particular, the whole compressed objects are distributed throughout the Internet. If the watermark technology is required to resist many different compression levels, which are more effective for applying the watermark embedding technique through a similar domain once an object compression happens [18,81].

#### 2.7.3. Data Injection

This type of attack is considered as an intentional attack, which occurs when an attacker inserts fake information to legal documents. Therefore, the dispute occurs each time according to the application of the copyright where this type is used to determine the first character of the registered content.

#### 2.7.4. Eavesdropping

This type of attack is known as snooping or sniffing attack where the attacker takes the advantage of the insecure communication among devices for gaining access data when it is being received or sent by users [82].

#### 2.7.5. Forgery Attack

In this kind of attack, a hacker will enter a new valid watermark instead of removing the old watermark [34].

#### 2.7.6. Active Attacks

The first threat represents a hacker who tries to remove or block the occurrence of a watermark. In few cases such as copy control, fingerprinting, ownership proof and owner realizing. These types of attacks are significant since the mark is removed once it is not identified [83]. It aims to discredit an embedded, unrecognizable watermark. Hence, it is insignificant when authentication and hidden communications are both involved [78].

#### 2.7.7. Passive Attacks

In passive attacks, the aim of the hacker is searching for the watermark within a hidden communication. In fact, the owners are not interested in this type of attack within the majority of the indicated application domains since watermarks are at most visible and are alerting their existence. Nonetheless, it is extremely essential to hide the existence of the prospective watermark. In few cases, these types of active attacks are based on the fact that hackers produce multiple copies derived from a single part of media that are accompanied by various types of watermarks where a copy is produced without the watermark [83]. When being resistant against collusion attacks for fingerprinting applications, the process is considered vital since it puts various labels for many different copies of a single particular part. The number of copies for which a hacker can accomplish relies on the property's type. A few users must join at the same time so that they can be robbed within a collusion attack, which is a bit impossible.

#### 2.7.8. Cryptographic Attacks

Cryptographic attacks are probably a security attack that cracks the security through different watermarking techniques by eliminating the information, which is related to the embedded watermark. The secret information is embedded by a brute-force searching technique by misleading the watermark itself. A further attack that creates a non-watermarked signal, including the involvement of an existing public watermark detector device is called an 'Oracle attack' [20]. A number of applications should limit such kinds of attacks, which are implemented within the cryptography domain for their increased computational complexity.

## 3. The Concept of IoT

The primary advantage of the IoT is global awareness, intelligent processing and reliable transfer of information. The key is the realisation of information's interactions between a human and a device or device-to-device. These devices consist of the embedded systems, control and automation systems, WSNs and others that share information among each other in different environments for enabling the IoT [84]. Therefore, the data can be transferred over different networks without the need for human intervention. In the real environment of IoT applications, smart city and home are the most popular fields. These applications mostly consist of three layers, which include: the perception, the network and the application [16]. Network and application layers are implemented in high-power devices that will keep data secure, while the perception layer is implemented in a low-power WSN. The WSN consists of multiple sensor nodes, which are communicating among each other by using different radio frequencies that are capable of performing various tasks of sensing, surveillance, measuring, and tracking [85]. These wireless nodes are resource-constrained devices that are characterised by their low processing power, narrow bandwidth, limited battery life, and restricted memory capacity [86]. The communication between IoT layers is depicted in Figure 10.

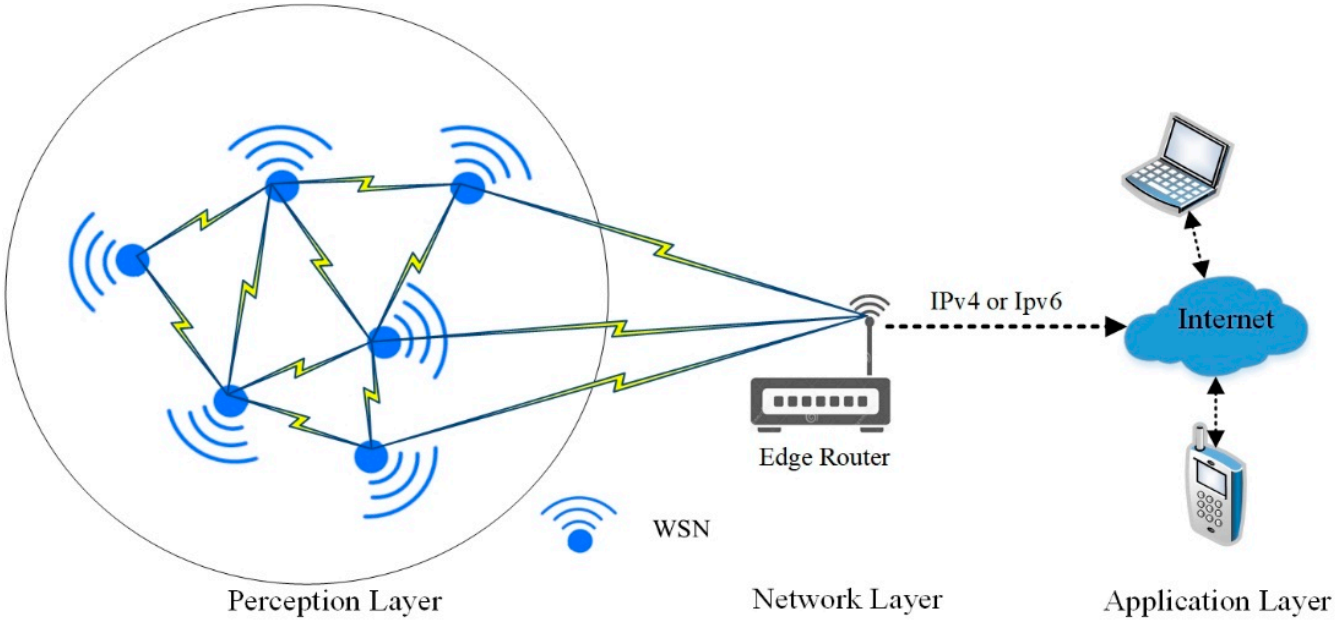


**Figure 10.** The communication among the IoT layers.

Based on Figure 10, WSNs are responsible for plotting the network topology and routing table in the perception layer based on the use of different protocols [87]. After that, the WSN starts collecting data from different locations and forwards it to the network layer (edge-router). However, the WSN nodes can normally function within untrusted environments, which are not periodically monitored. This makes the WSN networks extremely vulnerable to various attacks, and therefore, valuable data can be easily disclosed to unauthorized parties resulting in serious security and privacy risks [88].

### *3.1. Perception Layer's Limitations*

In the perception layer, the WSN nodes have two major limitations, which are the computing power and energy [89]. Since the WSN is designed to work in different environments, some of these environments are difficult to provide a charger. To overcome this limitation, the battery's capacity should be increased or security requirements should be reduced. Additionally, green energy such as light, wind and heat can be used to charge nodes [90]. However, these solutions seem impossible to meet since a battery's capacity

might not be easily raised due to the WSN's size and green power usage, which needs more hardware equipment. To reduce the security requirements, the data must be compromised. Consequently, a suitable solution to use robust and lightweight security algorithms leads to propose different encryption technologies [91].

### *3.2. Perception Layer Security Challenge*

The IoT technology relies on the WSN layer to sense, collect and transmit the real-time data through to the back-end layer for further analysis and processing. Therefore, the limitations of the WSN nodes and their reliance on public wireless channels lead to many challenges in the IoT architecture. One of these challenges is related to security and privacy in the perception layer. In the security domain, one of the main issues is to protect the data communication between the WSN nodes against eavesdropping, spoofing by an illegal WSN node and alteration [14,91]. Moreover, the authentication represents another important issue in the WSN security domain. For instance, the authentication method aims to protect the WSN network from being exploited by illegal WSN nodes. Moreover, different encryption and decryption methods are used in the security domain, while the limitations of WSNs lead to search through various secure technologies. Therefore, the watermarking technology is considered a candidate method that is used in the perception layer for protecting the owner's authentication and data integrity as illustrated in Figure 11.

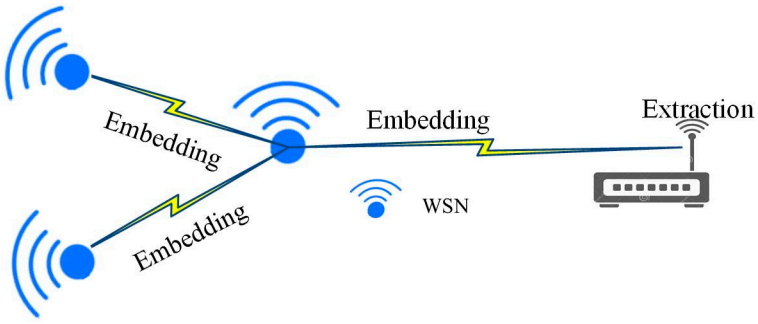


**Figure 11.** WSN with watermarking technique.

Watermark authentication policy calculates the watermark bits and inserts into the following WSN nodes before transmission. Moreover, the Access point syncs the data and checks the watermark bits from computing and extraction. Finally, the original data are restored. Furthermore, the watermarking technique is beneficial when protecting digital data, although after its decryption process. Furthermore, the watermarking technique is beneficial when protecting digital data, although after its decryption process. Accordingly, the IoT ecosystem should cover, the confidentiality, privacy and integrity of sensitive information [92], thus the use of watermarking techniques as traditional methods will not achieve them all [68]. Therefore, such a technique assists in averting the illegal usage pertaining to the personal information and defend it from illegal users and fraudulent. However, encryption focuses on protecting the contents during transmission and not after decoding [22]. The researchers in in [15,16,93–97] reviewed the use of the watermark technology in IoT security-related topics.

## 4. Related Research: Modified Watermarking Approaches in the IoT Applications

Several studies have been investigated to propose a particular method, which can deliver robustness and integrity throughout the watermark and security environments. Accordingly, the section addresses several studies that are based on the watermarking technique with different approaches such as hashing, deep learning, encryption, and fragile. These different approaches are illustrated in Figure 12.

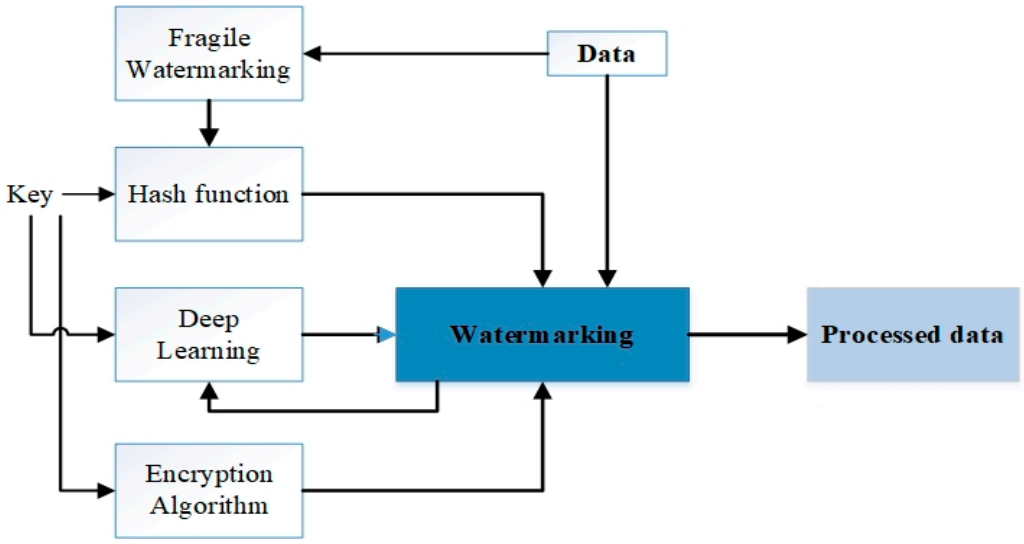


**Figure 12.** Different watermarking approaches in IoT.

Therefore, existing studies are grouped together according to the similarity of their approaches. Furthermore, there is no restricted separation for each group, which usually contains only one technique or a parameter for the watermarking technique.

### *4.1. Robusteness Image*

In order to improve the transfer of images amongst IoT layers, the authors in [97] propose a new watermarking approach based on the use of the biorthogonal family. The proposed approach uses Biorthogonal 2.2, Biorthogonal 3.5 and Biorthogonal 5.5 of different wavelet transforms. Symlets and coiflets wavelet transforms are also used. Different types of attacks are mitigated by the proposed scheme, so the piracy has been forbidden against digital images authentication in the emerging IoT-based systems. To investigate the proposed watermarking scheme robustness. multiple attacks are applied. In the same context, Biorthogonal wavelet transforms are used to preserve the authenticity of the image in the IoT. The researchers in [98] propose a new technique that uses four levels of the DWT where each level consists of a Biorthogonal wavelet, discrete meyer wavelet, reverse biorthogonal wavelet, coiflets wavelet transform and symlet wavelet.

Additionally, the researchers in [32] describe a DCT digital image watermarking method, which mainly depends on embedding the watermark technique by using two different coefficient groups of the host image when using the DCT on the selected DWT coefficient groups. In [55], the data privacy and confidentiality are preserved while being transmitted in an IoT where a robust and secure framework are presented for hiding the required data. The random selection of both the coefficient and block approaches are implemented for embedding the data in order to improve the embedded data's robustness, and avoid the fragility weakness through different cyber-attacks, particularly, geometric attacks. A threshold factor can determine the strength of the robustness, which is optimally selected to maintain the perceptual quality of the watermarked image. The distribution of data over various areas of the watermarked image is confirmed by using multiple randomly selected DCT coefficients for embedding the watermark bits.

### *4.2. Deep Learning*

Another technique that uses the deep learning technology in dynamic watermarking is proposed in [94]. The researchers employ the Long Short-Term Memory (LSTM) blocks along with the dynamic watermarking technique in order to find cyber-attacks. This process extracts random features such as diffraction, spectral flatness, central moments and kurtosis from the IoT signal, and watermarks these features within the pristine signal in the embedding process. In [99], the researchers improve the embedding technique by

applying the Deep Reinforcement Learning (DRL) approach through virtual intellectual property watermarks in order to improve the attack detection and reduce the computational overhead. The neural networks algorithm is used to generate the intellectual property watermark positions that are close to the original resource. When verifying the intellectual property ownership, the DRL model can directly determine the range of different default watermarking locations. After that, the map position of embedding the relationship can be calculated in a supervised manner in order to realise the rapid location of the real ownership information within an intellectual property circuit.

### 4.3. Engryption

Another different technique that is used as a key management in watermarking methods is proposed in [100], where the researchers produce a lightweight watermarking algorithm, which relies on a dynamic random key for preserving the WSN privacy and data integrity. Two dynamic random key algorithms are developed, which i the global and local algorithms. In the global algorithm, the system initialises the random key j bits through to all WSN nodes, and according to this key, the embedding position is shifted to the right by j bits per round. In the local algorithm, a random key is generated in every WSN. Consequently, a key generator protocol along with the watermark scheme is required. Additionally, the researchers demonstrate that their algorithm is effective due to lower delay, low complexity, and high accuracy. On the other hand, the researchers in [96] combine between the lightweight Elliptic Curve Cryptography (ECC) algorithm and the fragile zero watermarking algorithm rather than the digital signature in the standard ECC. This combination overcomes the standard ECC limitations in the IoT's authentication by reducing the power consumption and memory costs.

### 4.4. Hashing

Regarding the data integrity, the hash function is used in the watermarking method in [101–103]. The authors in [101] propose the double-authentication strategy in the watermarking technology in order to secure the transfer of data from the source-drone along to the edge-router. The first authentication occurs between the source-drone and master-drone. The master-drone is a cluster technology that allows neighbouring drones to identify a suitable one and use it as a broker in sending and receiving data. This authentication uses hash with a key in order to compute the watermarking sequence. Following that, it inserts it with the source-data within the embedding process. However, the watermark embedding position is accounted for based on the timestamp of the work. The second authentication executes between the master-drone and the edge-route. In the master-done, data are received and aggregated where the fragile watermarking algorithm is applied for generating a random key. This random key is embedded with the data that are aggregated before they are sent through to the edge-router. When the edge-router receives packets, it starts to verify authenticity and integrity, and extracts the original data. This proposal demonstrates the resistance to tampering and data replay. In [102], the researchers propose a lightweight watermark algorithm by using a homomorphic encryption and hash function along with the WSN data in order to embed the watermarking data. In [103], the watermark embedding locations and mechanisms are determined based on different channel conditions for ensuring the watermark security and energy efficiency. One of these methods: such as DCT, DFT and DWT will be randomly selected in the embedding process. After that, a hashing algorithm is used to generate a synchronised coefficient variation factor, which defines how different the watermarked image is compared to the original image.

### 4.5. Fragile

The researchers in [104,105] produce a number of chained fragile watermarks that aim to reduce the computational overhead and to detect unauthorized modification attacks. This technique starts by dividing the WSN data into a number of fixed size groups. Fol-

lowing that, the hash function is used to associate the group data along with the key and group serial numbers. The output of the hash function is used to generate the watermarked segment in each group. Finally, the watermarked segment is warehoused in the former group as a linked list model. The proposal experiments show the improvement in reducing the computational overhead, which reflects on the WSN's lifetime.

The researchers in [16] propose a fragile watermarking technique in order to maintain data integrity among the three IoT layers. In fact, this technique relies on computing the hash value for data, which are collected by the WSN in the perception layer. After that, a random location-based watermark approach is applied to compute the embedding position. Finally, the watermarked object is sent to the network layer. This technique contributes to secure data blocks from different attacks such as forwarding, tampering, replaying and spoofing. In [106], the researchers propose a lightweight fragile watermarking technique for improving the data integrity among the communication WSN nodes. This algorithm is based on the use of the MAC address node and hash function along with the embedding scheme.

Furthermore, the researchers in [107] produce a semi fragile watermarking method for recovery and attack detection. It mainly uses the IWT and DCT for identifying malicious attacks and recovery where it mainly focuses on enhancing the Enterprise Multimedia Security mechanism. To implement the tamper detection and recovery purposes, two different types of watermarking techniques are generated, which comprise: the recovery watermark and the authentication watermark. The embedding method of the proposed watermarking generation creates an acceptable PSNR of the watermarked images. Additionally, the proposed tamper detection mechanism is tested against various types of content preserving manipulations. These types include the addition of salt, speckle and pepper noise, wiener filtering, scaling, geometric attacks, gamma correction, image brightening and blurring. The findings show a correctly verified image authenticity.

In [61], the researchers propose a self-embedding authentication process in watermarking technology in order to discover and recover different tampered locations. Two types of detection processes are proposed, which comprise the pixel-wise and block-wise processes. In the pixel-wise process, the authentication data are created per pixel while it is created per block in the block-wise process. Therefore, the length of authentication data in the block-wise process is attuned according to the size of each block. Moreover, the two processes use six 512_512 grayscale images in order to validate their methodology, and they produced results that show better performance on the tamper discovery and image recovery within various heavily tampered images.

### 4.6. Reversible

Another technology that is related to authentication in the watermark is called the reversible approach. In this approach, the WSN data are grouped where watermarked bits are counted for each group. After that, the data are embedded with watermark bits before being sent to the upper layer. In the upper layer, the watermarked packets are extracted, and watermark bits are checked in order to restore the original data [108]. The researchers in [109] propose a reversible security framework, which is able to embed the Electronic Patient Record (EPR) securely throughout the medical images. These images are afterwards stored to a mobile cloud-based e-healthcare system where cloud administrators do not have privileges to gain access through the data and the client privacy can be preserved. This approach implements an integral method as the Optimal Pixel Repetition (OPR) where a pixel's permutation embeds the data in a reversible manner. On the other hand, the original image is not required to extract the EPR from the stego image. The proposed approach is resilient to statistical attacks where its histogram invariances between the cover and stego images. Moreover, the researchers in [110] propose a reversible algorithm, which is based on a prediction-error that can reduce the watermark load. Further, the WSN node attempts to group the streaming data into two different sets. In the first set, the watermarked bits are accounted and embedded into the other set. After that, the node sends the watermarked

packets through to the edge-router and then through to the edge-router directly that checks the packets and restores the original data. Hence, this research focuses on removing the watermarks' complications during the verification process where this removal reduces the delay in removing any additional unwanted information.

### 4.7. Extra Parameters

In the same context of the WSN data integration, the researchers in [15] propose the Randomized Watermarking Filtering (RWF) algorithm along with a clustering approach in order to achieve the data filtering on its involved traffic instead of an end-to-end filtering. This process eliminates all data implanted at an early step of communication and reduces the encountered overhead. Moreover, the watermark generation depends on four factors, which include: the WSN-ID, pre-shared keys, an encrypted payload and data capture time. These factors are added to the watermark during the embedding process. Moreover, the embedding positions use the Pseudo Random Number Generator (PRNG) algorithm in order to generate them randomly. Finally, the integrity of the watermarked object is verified by the WSN master node in the perception layer and after that is sent to the upper layer. The researchers in [111] suggest a zero-watermarking algorithm in order to preserve the data integrity between the source WSN and edge router (an end-to-end protection). In this algorithm, the watermark generation depends on three factors: the frequency of data occurrence, data length and data capture time. After generating a secret watermark, the WSN adds it to their original data and forwards it to the edge router through the successor of multiple WSNs. The edge router that possesses the authority can verify and extract the data. The results of the algorithm demonstrate a better performance and lower energy consumption.

### 4.8. Physical Security

In [45], the researchers present a hybrid watermarking algorithm for protecting the integrity of an object while it is being transmitted through the Long-Term-Evolution (LTE) physical layer. This algorithm starts by classifying the object based on the use of the Support Vector Machine (SVM) in order to discover different important and unimportant regions. Following that, the DWT and SVD techniques are used to embed the scrambled data into a number of coefficients. Finally, the output of the embedding data is embedded into unimportant regions. Nonetheless, the algorithm shows that the improvement is made for the quality of an object when the complexity is high. A similar way for using the watermark technology in the WSN physical layer is investigated in [82] where a new protocol, namely, the 'Watermarked-based Blind Physical Layer Security (WBPLSec) protocol is proposed in order to secure the encountered communication among existing nodes. In fact, this protocol combines a blind watermark algorithm with the jam receiver over an acoustic channel in order to interchange a key of 128 bits with an adjacent equipment. The process starts by modulating the message with the Direct Sequence Spread Spectrum (DSSS) technique and embeds this message with a shifting key to represent a watermarked segment. After that, the segment is encoded in a waveform audio file format and is transmitted by an amplifier. The receiver can restore the cleaned code by using the information in the watermark. Nevertheless, this proposal requires a private and covert channel among existing nodes where this reduces the wireless bandwidth. In [112], the researchers merge the MAC layer parameters within a watermark technique in order to improve the attack detection in the WSN. The MAC address and CSMA/CA collision time are combined together to act as a watermarking key. The watermarking key is added to the DCT and DWT to embed the WSN data. Finally, the watermarked data are sent to the edge-router and edge-route, which reverses the watermarking process.

## 5. Discussion and Issues

In this section, a comprehensive summary of the previously indicated watermarking techniques is discussed based on the type of technique, medium, key contribution,

performance metrics, advantages and attacking types for each technology. Table 1 shows this summary where all these schemes are designed to produce an effective watermarking procedure through different layers of the IoT. However, there are still no ideal solutions. As noted by the aforementioned studies, the modified watermarking process is nominated to be used in future Internet flows for several advantages, such as including the lightweight calculation, minimizing lags and guaranteeing data security. Additionally, the steganography can be involved with the cryptography technique in order to provide security for transmitting data. Several studies in the literature attempt to assist security in the IoT technology as the lightweight algorithm. Furthermore, the algorithms that are enhanced in the literature demonstrate that the embedding process represents an essential process, which is based on the watermarking technique. At the same time, this technique forms the basic module, which is implemented in some research domains like the DCT, DWT domain, Complex Wavelet Transform, spatial, DWT, DCT and DFT domains. Several researchers state that using the LSB technique for hiding the secret message within the LSB image provides an efficient method for embedding the information into all objects. Furthermore, other studies use a hybrid method for combining two or more embedding procedures in order to increase the performance. On the other hand, the computational complexity increases. In addition, deep learning with watermarking will give more accurate output but it needs high performance hardware.

**Table 1.** A summary of inspiring and pioneering robust objects watermarking algorithms.

| Authors | Technique Type | Medium | Contributions Key | Metrics | Advantages | Attacks |
|---|---|---|---|---|---|---|
| Al-Shayea et al. [98] | Robust | Image | Four levels of the DWT are used and each level contains different wavelet families. | MSE<br>PSNR<br>SSIM | Improves robustness | Noise, Median, Mean, Gaussian noise, Adjust image, Rotation, and JPEG |
| Al-Shayea et al. [97] | Robust | Image | The biorthogonal family is used in the watermarking process. | MSE<br>PSNR<br>SNR | Improves robustness | Noise, Median, Mean, Gaussian noise, Adjust image, and Rotation |
| Loan et al. [32] | Robust<br>Secure | Image | The DCT with the Arnold transform and chaotic encryption. | Capacity<br>PSNR<br>SSIM<br>BER | | Salt and pepper noise, Gaussian noise, Median, and sharpening |
| Hurrah et al. [55] | Robust<br>Secure | Image | The coefficient and block approach has been implemented for embedding the data. | PSNR<br>BER | Improves data confidentiality | Rotation, Croppinghistogram equalization, and Sharpening |
| Ferdowsi and Saad [94] | Secure<br>Deep learning | Any data | Long Short-Term Memory blocks along with the dynamic watermarking algorithm | BER | Improves attack detection | Eavesdropping and Data injection |
| Liang et al. [99] | Secure<br>Deep learning | Any type | Combines the neural networks technology and virtual mapping function along with an appropriate watermarking technique. | Detection time<br>Detection speed<br>BER | Improves attack detection<br>Reduces computational overhead. | Hardware |
| T. M. Hoang et al. [100] | Secure<br>Privacy | Any data | Two random keys are used along with the watermarking algorithm | BER<br>Complexity | Improves attack detection | Spoofing |
| Sarwar et al. [96] | Secure<br>Fragile | Any data | Combination between the ECC algorithm and the fragile zero watermarking algorithm. | Memory cost<br>Computational Cost | Reduces the computational overhead | |
| Sun et al. [101] | Secure | Any type | Two different watermarking processes are applied along within a clustering approach. | False positive rate<br>Energy consumption<br>Average delay | Improves data integrity<br>Reduces the computational overhead | Replay, Tamper, and Data forgery |

**Table 1.** *Cont.*

| Authors | Technique Type | Medium | Contributions Key | Metrics | Advantages | Attacks |
|---|---|---|---|---|---|---|
| Babaeer and Al-Ahmadi [102] | Secure | Any type | The homomorphic and random watermarking methods are embedded with each block of data. | Delay<br>Packet delivery ratio<br>Energy consumption | Improves data integrity<br>Reduces energy consumption | Modification, Replay, and Insertion |
| Yaseen et al. [103] | Secure | Image | The DCT, DFT and DWT are used in the embedding phase along with the hash function. | NC<br>PSNR<br>BER | Improves data integrity | Tamper attack |
| Kamel and Juma [105] | Fragile | Any type | Grouping delimiters and hash function are used along with the chained watermarks. | Average embedding time<br>Average extraction time | Reduces the computational overhead<br>Improves attack detection. | Insertion, Modification, and Deletion. |
| Zhang et al. [16] | Fragile | Any type | Hash function along with its dynamic random watermark position. | Capacity<br>Positive rateEnergy consumption | Improves data integrity<br>Reduces the computational overhead. | Tampering, Data forgery, Deletion, and Replay |
| Boubiche et al. [106] | Fragile | Any type | The MAC address and hashed data are xored with the original data in the embedding phase. | Energy consumption<br>Average delay<br>False positive rate | Improves data integrity | Modification |
| Sivasubramanian and Konganathan. [107] | Semi-fragile | Image | Uses semi-fragile IWT and DCT methods for recovery and tamper detection by using the IWT. | PSNR | Improves attack detection | Tampering, Salt, Gaussian blur, and Gamma correction |
| Lee et al. [61] | Fragile<br>Secure | Image | Block-wise and pixel-wise methods have been implemented for the watermarking algorithm. | False positive rate<br>False negative rate<br>Error rate<br>PNSR | Improves attacks detection and recovery | Clipping, Baboon, and Tampering |
| Kaw et al. [109] | Reversible<br>Secure | Image | Implements methods like the optimal pixel repetition method where the pixel permutation is reversibly embedded within the data. | PSNR | Improves data integrity | Statistical attacks |
| Shi and Xiao [110] | Reversible<br>Secure | Image | A reversible watermark technique that is based on the prediction-error expansion. | False positive rate<br>False negative rate | Improves data integrity<br>Reduces computational overhead | Tampering, Deletion, and Insertion |
| Alromih et al. [15] | Secure | Any type | The randomised watermarking filtering algorithm to achieve data filtering on traffic instead of an end-to-end filtering. | Energy consumption<br>Average of filtered packet. | Improves data integrity<br>Reduces the computational overhead | Injection and Physical attacks |
| Hameed et al. [111] | Secure | Any type | Length of data, frequency of digits and time of captured data are all used along with the original data for the embedding process. | Energy consumption<br>Computational time | Improves data integrity | Eavesdropping and Malicious node |
| Rai and Singh. [45] | Robust | Image | The SVM classification and hybrid watermarking technique (DWT and SVD) have been implemented in the embedding process. | BER<br>SNR<br>PSNR<br>SSIM | Improves robustness | Salt, Gaussian noise, speckle, Median, and Crop |
| Soderi [82] | Blind<br>Secure<br>Robust | Audio | Combines a blind watermark algorithm with the jamming technique over the acoustic channel for embedding the data | SNR<br>BER | Improves data integrity<br>Improves robustness | Eavesdropping and confidentiality |
| Nguyen et al. [112] | Secure | Any type | The MAC layer parameters are used along with the DWT and DCT methods for embedding existing watermarks. | Detection probability | Improves attack detection | Clone |

A statistical analysis is performed for the reviewed techniques (see Figure 13). The produced analysis from the figure demonstrates the type of technique, total usage number and its advantages in the IoT.

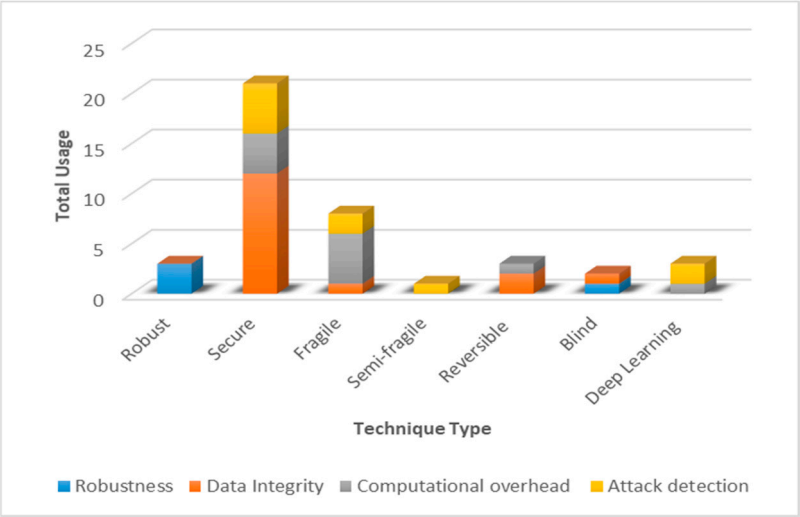


**Figure 13.** Statistical analysis for the reviewed watermarking techniques in IoT.

From Figure 13, security watermarking schemes take the majority over the other sets of watermarking requirements and ensure that data integrity is their most significant advantage in the IoT watermark security. Therefore, data integrity is considered as a serious part of the watermarking technique that relates to quality, reliability and usability. Since the IoT technology allows all users (humans or machines) to share data anytime and anywhere, the main point is to guarantee the data integrity through the Internet. Another issue relates to the object transformation. In multimedia objects, each file has different formats, which may result in watermarked data being lost during configuration change. Therefore, the effect of object transformations on watermarked data needs further analysis to understand their behaviours.

In terms of the performance metrics, most of the watermarking techniques for which their medium type represents an image are evaluated by the MSE, PSNR, BER, and SNR metrics. Meanwhile, other types of media use the energy consumption and computational cost for the evaluation. Furthermore, most of the reviewed studies focus on satisfying one type of the watermarking requirements, such as security, robust or capacity. Hence, finding or developing a new watermark algorithm that unifies these requirements is considered a potential challenge. Another challenge related to attack types can be taken into account by improving the existing watermarking technique for supporting all possible attacks on a single object.

## 6. Conclusions and Future Work

In this paper, the development, design, implementation and testing of the watermarking technique into different data and applications are highlighted. A brief introduction is provided in terms of the digital object watermarking in the IoT environment, displaying major characteristics, different kinds of watermarking techniques, mutual watermark embedding and extraction process, along with many recent applications. Further, various state-of-the-art watermarking techniques, potential issues and existing solutions that are conducted by researchers are summarised. The proposed algorithm can effectively prevent a variety of attacks as found in the security analysis, these attacks include packet forgery attacks, packet forwarding attacks, packet tamper attacks, packet replay attacks and packet delay transmission attacks, which are caused by malicious nodes. Additionally, the proposed algorithms can solve the shortcomings of the existing technologies within

the IoT perception layer. It can only simplify the computational complexity and improve the authentication's efficiency and security. However, it can also ensure the reversible extraction of the watermarking process and the lossless restoration of data. Finally, the paper presents a brief summary around different techniques and draws the future research.

**Author Contributions:** All authors contributed to this manuscript. Conceptualization, R.A., R.W., A.A.-A. and A.K.; investigation, R.A., M.A.-M., R.W. and A.A.-A.; data duration, R.A., R.W. and A.K.; writing-original draft, R.A., A.A.-A. and R.W.; visualization, R.A.; supervision, R.A.; writing-review and editing, R.A., R.W. and A.K. 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. Subba Rao, S. Copyright: Its implications for electronic information. *Online Inf. Rev.* **2003**, *27*, 264–275. [CrossRef]
2. Liu, Y.; Tang, S.; Liu, R.; Zhang, L.; Ma, Z. Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Syst. Appl.* **2018**, *97*, 95–105. [CrossRef]
3. Nikolic, M.; Tuba, E.; Tuba, M. Edge detection in medical ultrasound images using adjusted Canny edge detection algorithm. In Proceedings of the 2016 24th Telecommunications Forum (TELFOR), Belgrade, Serbia, 22–23 November 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–4.
4. Alattar, A.M. Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform. *IEEE Trans. Image Process.* **2004**, *13*, 1147–1156. [CrossRef]
5. Petitcolas, F.A.P.; Anderson, R.J.; Kuhn, M.G. Information hiding-a survey. *Proc. IEEE* **1999**, *87*, 1062–1078. [CrossRef]
6. Eskicioglu, A.M.; Delp, E.J. An overview of multimedia content protection in consumer electronics devices. *Signal Process. Image Commun.* **2001**, *16*, 681–699. [CrossRef]
7. Altaay, A.A.J.; Sahib, S.B.; Zamani, M. An Introduction to Image Steganography Techniques. In Proceedings of the 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Kuala Lumpur, Malaysia, 26–28 November 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 122–126.
8. Otair, M.A. Security in digital images: From information hiding perspective. In *Handbook of Research on Threat Detection and Countermeasures in Network Security*; Information Science Reference: Hershey PA, USA, 2014; pp. 381–394. ISBN 9781466665842.
9. Anand, D.; Niranjan, U.C. Watermarking medical images with patient information. In Proceedings of the Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Hong Kong, China, 1 November 1998; Volume 20 Biomedical Engineering Towards the Year 2000 and Beyond (Cat. No.98CH36286). IEEE: Piscataway, NJ, USA, 1998; Volume 2, pp. 703–706.
10. Tiwari, A.; Singh, V. Digital Image Watermarking Using DWT and Shift Invariant Edge Detection. *Int. J. Comput. Technol. Electron. Eng.* **2013**, *3*, 21–26.
11. Iwendi, C.; Jalil, Z.; Javed, A.R.; Thippa Reddy, G.; Kaluri, R.; Srivastava, G.; Jo, O. KeySplitWatermark: Zero Watermarking Algorithm for Software Protection against Cyber-Attacks. *IEEE Access* **2020**, *8*, 72650–72660. [CrossRef]
12. Singh, L.; Singh, A.K.; Singh, P.K. Secure data hiding techniques: A survey. *Multimed. Tools Appl.* **2020**, *79*, 15901–15921. [CrossRef]
13. Dagadu, J.C.; Li, J. Context-based watermarking cum chaotic encryption for medical images in telemedicine applications. *Multimed. Tools Appl.* **2018**, *77*, 24289–24312. [CrossRef]
14. Glissa, G.; Meddeb, A. 6LoWPAN multi-layered security protocol based on IEEE 802.15.4 security features. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 264–269.
15. Alromih, A.; Al-Rodhaan, M.; Tian, Y. A Randomized Watermarking Technique for Detecting Malicious Data Injection Attacks in Heterogeneous Wireless Sensor Networks for Internet of Things Applications. *Sensors* **2018**, *18*, 4346. [CrossRef]
16. Zhang, G.; Kou, L.; Zhang, L.; Liu, C.; Da, Q.; Sun, J. A New Digital Watermarking Method for Data Integrity Protection in the Perception Layer of IoT. *Secur. Commun. Netw.* **2017**, *2017*, 1–12. [CrossRef]
17. Tanha, M.; Torshizi, S.D.S.; Abdullah, M.T.; Hashim, F. An overview of attacks against digital watermarking and their respective countermeasures. In Proceedings of the Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, Malaysia, 26–28 June 2012; IEEE: Piscataway, NJ, USA, 2012; Volume 4, pp. 265–270.
18. Song, C.; Sudirman, S.; Merabti, M.; Llewellyn-Jones, D. Analysis of Digital Image Watermark Attacks. In Proceedings of the 2010 7th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 9–12 January 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 1–5.
19. Mohanty, S.P.; Sengupta, A.; Guturu, P.; Kougianos, E. Everything You Want to Know About Watermarking: From Paper Marks to Hardware Protection: From paper marks to hardware protection. *IEEE Consum. Electron. Mag.* **2017**, *6*, 83–91. [CrossRef]
20. Begum, M.; Uddin, M.S. Digital Image Watermarking Techniques: A Review. *Information* **2020**, *11*, 110. [CrossRef]

21. Prasetyo, H.; Hsia, C.H.; Liu, C.H. Vulnerability attacks of SVD-based video watermarking scheme in an IoT environment. *IEEE Access* **2020**, *8*, 69919–69936. [CrossRef]
22. Singh, A.K.; Kumar, B.; Dave, M.; Ghrera, S.P.; Mohan, A. Digital Image Watermarking. In *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*; IGI Global: Hershey, PA, USA, 2016; pp. 246–272.
23. Thapa, M.; Sandeep, D.; Meenakshi, A. Digital Image Watermarking Technique Based on Different Attacks. *Int. J. Adv. Comput. Sci. Appl.* **2011**, *2*, 14–19. [CrossRef]
24. Panchal, U.H.; Srivastava, R. A Comprehensive Survey on Digital Image Watermarking Techniques. In Proceedings of the 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 4–6 April 2015; IEEE: Piscataway, NJ, USA, 2015; Volume 82, pp. 591–595.
25. Su, J.K.; Hartung, F.; Girod, B. Digital watermarking of text, image, and video documents. *Comput. Graph.* **1998**, *22*, 687–695. [CrossRef]
26. Vasudev, R. A Review on Digital Image Watermarking and Its Techniques. *J. Image Graph.* **2016**, *4*, 150–153. [CrossRef]
27. Anand, A.; Singh, A.K. Watermarking techniques for medical data authentication: A survey. *Multimed. Tools Appl.* **2020**, *17*, 1–33. [CrossRef]
28. Kumar, C.; Singh, A.K.; Kumar, P. A recent survey on image watermarking techniques and its application in e-governance. *Multimed. Tools Appl.* **2018**, *77*, 3597–3622. [CrossRef]
29. Singh, A.K.; Kumar, B.; Singh, G.; Mohan, A. (Eds.) *Medical Image Watermarking*; Springer: Cham, Switzerland, 2017; ISBN 978-3-319-57698-5.
30. Hua, G.; Huang, J.; Shi, Y.Q.; Goh, J.; Thing, V.L.L. Twenty years of digital audio watermarking—A comprehensive review. *Signal Process.* **2016**, *128*, 222–242. [CrossRef]
31. Agarwal, R.; Santhanam, M.S.; Srinivas, K. Digital watermarking: An approach based on Hilbert transform. In Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 29–30 April 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1035–1042.
32. Loan, N.A.; Hurrah, N.N.; Parah, S.A.; Lee, J.W.; Sheikh, J.A.; Bhat, G.M. Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption. *IEEE Access* **2018**, *6*, 19876–19897. [CrossRef]
33. Singh, D.; Singh, S.K. DCT based efficient fragile watermarking scheme for image authentication and restoration. *Multimed. Tools Appl.* **2017**, *76*, 953–977. [CrossRef]
34. Agarwal, N.; Singh, A.K.; Singh, P.K. Survey of robust and imperceptible watermarking. *Multimed. Tools Appl.* **2019**, *78*, 8603–8633. [CrossRef]
35. Cheddad, A.; Condell, J.; Curran, K.; Mc Kevitt, P. Digital image steganography: Survey and analysis of current methods. *Signal Process.* **2010**, *90*, 727–752. [CrossRef]
36. Yadav, B.; Kumar, A.; Kumar, Y. A Robust Digital Image Watermarking Algorithm Using DWT and SVD. In *Advances in Intelligent Systems and Computing*; Springer: Singapore, 2018; Volume 583, pp. 25–36, ISBN 9789811056864.
37. Hu, H.-T.; Hsu, L.-Y. Exploring DWT–SVD–DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression. *Comput. Electr. Eng.* **2015**, *41*, 52–63. [CrossRef]
38. Chang, C.-C.; Tsai, P.; Lin, C.-C. SVD-based digital image watermarking scheme. *Pattern Recognit. Lett.* **2005**, *26*, 1577–1586. [CrossRef]
39. Lai, C.-C.; Tsai, C.-C. Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition. *IEEE Trans. Instrum. Meas.* **2010**, *59*, 3060–3063. [CrossRef]
40. Boujelbene, R.; Jemaa, Y.B.; Zribi, M. A comparative study of recent improvements in wavelet-based image coding schemes. *Multimed. Tools Appl.* **2019**, *78*, 1649–1683. [CrossRef]
41. Pun, C. A Novel DFT-based Digital Watermarking System for Images. In Proceedings of the 2006 8th international Conference on Signal Processing, Guilin, China, 16–20 November 2006; IEEE: Piscataway, NJ, USA, 2006; Volume 2, pp. 3–6.
42. Singh, R.; Rawat, P.; Shukla, P. Robust Medical Image Authentication using 2-D Stationary Wavelet Transform and Edge Detection. In Proceedings of the 2nd IET International Conference on Biomedical Image and Signal Processing (ICBISP 2017), Wuhan, China, 13–14 May 2017; Institution of Engineering and Technology: Stevenage, UK, 2017; Volume 2017, pp. 1–8.
43. Wang, Y.; Bai, X.; Yan, S. Digital image watermarking based on texture block and edge detection in the discrete wavelet domain. In Proceedings of the 2013 International Conference on Sensor Network Security Technology and Privacy Communication System, Harbin, China, 18–19 May 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 170–174.
44. Singh, S.P.; Bhatnagar, G. A new robust watermarking system in integer DCT domain. *J. Vis. Commun. Image Represent.* **2018**, *53*, 86–101. [CrossRef]
45. Rai, A.; Singh, H.V. A Robust Watermarking Scheme Using Machine Learning Transmitted Over High-Speed Network for Smart Cities. In *Future Generation Computer Systems*; Hassanien, A.E., Elhoseny, M., Ahmed, S.H., Singh, A.K., Eds.; Lecture Notes in Intelligent Transportation and Infrastructure; Springer International Publishing: Cham, Switzerland, 2019; Volume 9, pp. 257–277, ISBN 978-3-030-01559-6.
46. Chan, C.-K.; Cheng, L.M. Hiding data in images by simple LSB substitution. *Pattern Recognit.* **2004**, *37*, 469–474. [CrossRef]
47. Hussain, M.; Wahab, A.W.A.; Idris, Y.I.B.; Ho, A.T.S.; Jung, K.-H. Image steganography in spatial domain: A survey. *Signal Process. Image Commun.* **2018**, *65*, 46–66. [CrossRef]
48. Hong, W.; Chen, T. A Novel Data Embedding Method Using Adaptive Pixel Pair Matching. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 176–184. [CrossRef]

49. Ahmaderaghi, B.; Del Rincon, J.M.; Kurugollu, F.; Bouridane, A. Perceptual watermarking for Discrete Shearlet transform. In Proceedings of the 2014 5th European Workshop on Visual Information Processing (EUVIP), Paris, France, 10–12 December 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 1–6.
50. Gibert, X.; Patel, V.M.; Labate, D.; Chellappa, R. Discrete shearlet transform on GPU with applications in anomaly detection and denoising. *EURASIP J. Adv. Signal Process.* **2014**, *2014*, 64. [CrossRef]
51. Ray, A.; Roy, S. Recent trends in image watermarking techniques for copyright protection: A survey. *Int. J. Multimed. Inf. Retr.* **2020**, *9*, 249–270. [CrossRef]
52. Chang, I.C.; Hu, Y.C.; Chen, W.L.; Lo, C.C. High capacity reversible data hiding scheme based on residual histogram shifting for block truncation coding. *Signal Process.* **2015**, *108*, 376–388. [CrossRef]
53. Singh, A.K.; Kumar, B.; Dave, M.; Mohan, A. Robust and Imperceptible Dual Watermarking for Telemedicine Applications. *Wirel. Pers. Commun.* **2015**, *80*, 1415–1433. [CrossRef]
54. 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]
55. Hurrah, N.N.; Parah, S.A.; Sheikh, J.A.; Al-Turjman, F.; Muhammad, K. Secure data transmission framework for confidentiality in IoTs. *Ad. Hoc. Netw.* **2019**, *95*, 101989. [CrossRef]
56. Verma, V.S.; Jha, R.K. An Overview of Robust Digital Image Watermarking. *IETE Tech. Rev.* **2015**, *32*, 479–496. [CrossRef]
57. Mohanty, S.P.; Bhargava, B.K. Invisible watermarking based on creation and robust insertion-extraction of image adaptive watermarks. *ACM Trans. Multimed. Comput. Commun. Appl.* **2008**, *5*, 1–22. [CrossRef]
58. Ahmed, F.; Sattar, F.; Siyal, M.Y.; Yu, D. A Secure Watermarking Scheme for Buyer-Seller Identification and Copyright Protection. *EURASIP J. Adv. Signal Process.* **2006**, *2006*, 056904. [CrossRef]
59. Khan, A.; Jabeen, F.; Naz, F.; Suhail, S.; Ahmed, M.; Nawaz, S. Buyer seller watermarking protocols issues and challenges—A survey. *J. Netw. Comput. Appl.* **2016**, *75*, 317–334. [CrossRef]
60. Artru, R.; Gouaillard, A.; Ebrahimi, T. Digital Watermarking of video streams: Review of the State-Of-The-Art. *arXiv* **2019**, arXiv:1908.02039.
61. Lee, C.-F.; Shen, J.-J.; Chen, Z.-R.; Agrawal, S. Self-Embedding Authentication Watermarking with Effective Tampered Location Detection and High-Quality Image Recovery. *Sensors* **2019**, *19*, 2267. [CrossRef] [PubMed]
62. Coatrieux, G.; Lecornu, L.; Sankur, B.; Roux, C. A Review of Image Watermarking Applications in Healthcare. In Proceedings of the 2006 International Conference of the IEEE Engineering in Medicine and Biology Society, New York, NY, USA, 30 August–3 September 2006; IEEE: Piscataway, NJ, USA, 2006; pp. 4691–4694.
63. Low, S.H.; Maxemchuk, N.F.; Brassil, J.T.; O'Gorman, L. Document marking and identification using both line and word shifting. In Proceedings of the Proceedings of INFOCOM'95, Boston, MA, USA, 2–6 April 1995; IEEE Comput. Soc. Press: Piscataway, NJ, USA, 1995; Volume 2, pp. 853–860.
64. Singh, A.K.; Kumar, B.; Singh, G.; Mohan, A. Medical Image Watermarking Techniques: A Technical Survey and Potential Challenges. In *Medical Image Watermarking*; Springer International Publishing: Cham, Switzerland, 2017; pp. 13–41, ISBN 9783319576992.
65. Tao, H.; Chongmin, L.; Mohamad Zain, J.; Abdalla, A.N. Robust Image Watermarking Theories and Techniques: A Review. *J. Appl. Res. Technol.* **2014**, *12*, 122–138. [CrossRef]
66. Zhou, X.; Zhang, H.; Wang, C. A Robust Image Watermarking Technique Based on DWT, APDCBT, and SVD. *Symmetry* **2018**, *10*, 77. [CrossRef]
67. Cayre, F.; Fontaine, C.; Furon, T. Watermarking security part one: Theory. In Proceedings of the Security, Steganography, and Watermarking of Multimedia Contents VII, San Jose, CA, USA, 17–20 January 2005; 2005; Volume 5681, p. 746.
68. Bordel, B.; Alcarria, R.; Robles, T.; Iglesias, M.S. Data Authentication and Anonymization in IoT Scenarios and Future 5G Networks Using Chaotic Digital Watermarking. *IEEE Access* **2021**, *9*, 22378–22398. [CrossRef]
69. Sattar, F.; Yu, D. Forensic Watermarking for Secure Multimedia Distribution. In *Socioeconomic and Legal Implications of Electronic Intrusion*; IGI Global: Hershey, PA, USA, 2009; pp. 261–280.
70. Parah, S.A.; Sheikh, J.A.; Loan, N.A.; Bhat, G.M. Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. *Digit. Signal Process.* **2016**, *53*, 11–24. [CrossRef]
71. Umar, M.M.; Mehmood, A.; Song, H.; Choo, K.-K.R. I-Marks: An iris code embedding system for ownership identification of multimedia content. *Comput. Electr. Eng.* **2017**, *63*, 209–219. [CrossRef]
72. Alkawaz, M.H.; Sulong, G.; Saba, T.; Almazyad, A.S.; Rehman, A. Concise analysis of current text automation and watermarking approaches. *Secur. Commun. Netw.* **2016**, *9*, 6365–6378. [CrossRef]
73. Janu, N.; Kumar, A.; Dadheech, P.; Sharma, G.; Kumar, A.; Raja, L. Multiple Watermarking Scheme for Video & Image for Authentication & Copyright Protection. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Jeju Island, Korea, 12–14 March 2021; Volume 1131, p. 012020.
74. Priya, C.V.L.; Raj, N.R.N. Digital watermarking scheme for image authentication. In Proceedings of the 2017 IEEE International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 6–8 April 2017; pp. 2026–2030.
75. Chen, L.; Kong, X.; Weng, B.; Yao, Z.; Pan, R. A Novel Robust Mesh Watermarking Based on BNBW. *EURASIP J. Adv. Signal Process.* **2011**, *2011*, 216783. [CrossRef]

76. Korus, P.; Białas, J.; Dziech, A. A new approach to high-capacity annotation watermarking based on digital fountain codes. *Multimed. Tools Appl.* **2014**, *68*, 59–77. [CrossRef]
77. Jadooki, S.; Mohamad, D.; Saba, T.; Almazyad, A.S.; Rehman, A. Fused features mining for depth-based hand gesture recognition to classify blind human communication. *Neural Comput. Appl.* **2017**, *28*, 3285–3294. [CrossRef]
78. Fadhil, M.S.; Alkawaz, M.H.; Rehman, A.; Saba, T. Writers Identification Based on Multiple Windows Features Mining. *3D Res.* **2016**, *7*, 8. [CrossRef]
79. Su, J.K.; Eggers, J.J.; Girod, B. Analysis of digital watermarks subjected to optimum linear filtering and additive noise. *Signal Process.* **2001**, *81*, 1141–1175. [CrossRef]
80. Zhu, X.-S.; Sun, Y.; Meng, Q.-H.; Sun, B.; Wang, P.; Yang, T. Optimal watermark embedding combining spread spectrum and quantization. *EURASIP J. Adv. Signal Process.* **2016**, *2016*, 74. [CrossRef]
81. Jain, R.; Kumar, M.; Jain, A.K.; Jain, M. Digital Image Watermarking using Hybrid DWT-FFT technique with different attacks. In Proceedings of the 2015 International Conference on Communications and Signal Processing (ICCSP), Melmaruvathur, India, 2–4 April 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 0672–0675.
82. Soderi, S. Acoustic-Based Security: A Key Enabling Technology for Wireless Sensor Networks. *Int. J. Wirel. Inf. Networks* **2020**, *27*, 45–59. [CrossRef]
83. Cox, I.J.; Linnartz, J.-P.M.G. Some general methods for tampering with watermarks. *IEEE J. Sel. Areas Commun.* **1998**, *16*, 587–593. [CrossRef]
84. Al-Emran, M.; Malik, S.I.; Al-Kabi, M.N. A Survey of Internet of Things (IoT) in Education: Opportunities and Challenges. In *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 197–209, ISBN 9783030245139.
85. Yi, L.; Tong, X.; Wang, Z.; Zhang, M.; Zhu, H.; Liu, J. A Novel Block Encryption Algorithm Based on Chaotic S-Box for Wireless Sensor Network. *IEEE Access* **2019**, *7*, 53079–53090. [CrossRef]
86. Khashan, O.A.; Ahmad, R.; Khafajah, N.M. An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. *Ad. Hoc. Netw.* **2021**, *115*, 102448. [CrossRef]
87. Kumar, V.; Tiwari, S. Routing in IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN): A Survey. *J. Comput. Netw. Commun.* **2012**, *2012*, 1–10. [CrossRef]
88. Zhang, X.; Heys, H.M.; Li, C. Energy efficiency of encryption schemes applied to wireless sensor networks. *Secur. Commun. Netw.* **2012**, *5*, 789–808. [CrossRef]
89. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet Things J.* **2017**, *4*, 1250–1258. [CrossRef]
90. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
91. Lee, C.-C. Security and Privacy in Wireless Sensor Networks: Advances and Challenges. *Sensors* **2020**, *20*, 744. [CrossRef]
92. Chatzigiannakis, I.; Vitaletti, A.; Pyrgelis, A. A privacy-preserving smart parking system using an IoT elliptic curve based security platform. *Comput. Commun.* **2016**, *89–90*, 165–177. [CrossRef]
93. Sheikh, J.A.; Akhter, S.; Parah, S.A.; Bhat, G.M. Blind digital speech watermarking using filter bank multicarrier modulation for 5G and IoT driven networks. *Int. J. Speech Technol.* **2018**, *21*, 715–722. [CrossRef]
94. Ferdowsi, A.; Saad, W. Deep Learning-Based Dynamic Watermarking for Secure Signal Authentication in the Internet of Things. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
95. Li, D.; Deng, L.; Bhooshan Gupta, B.; Wang, H.; Choi, C. A novel CNN based security guaranteed image watermarking generation scenario for smart city applications. *Inf. Sci.* **2019**, *479*, 432–447. [CrossRef]
96. Sarwar, K.; Yongchareon, S.; Yu, J. Lightweight ECC with Fragile Zero-Watermarking for Internet of Things Security. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 867–872.
97. Al-Shayea, T.K.; Mavromoustakis, C.X.; Batalla, J.M.; Mastorakis, G.; Mukherjee, M.; Chatzimisios, P. Efficiency-Aware Watermarking using Different Wavelet Families for the Internet of Things. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
98. Al-Shayea, T.K.; Mavromoustakis, C.X.; Batalla, J.M.; Mastorakis, G.; Pallis, E.; Markakis, E.K.; Panagiotakis, S.; Khan, I. Medical Image Watermarking in Four Levels Decomposition of DWT Using Multiple Wavelets in IoT Emergence. In *Artificial Intelligence and The Environmental Crisis*; Springer: Cham, Switzerland, 2020; pp. 15–31, ISBN 9783030449063.
99. Liang, W.; Huang, W.; Long, J.; Zhang, K.; Li, K.-C.; Zhang, D. Deep Reinforcement Learning for Resource Protection and Real-Time Detection in IoT Environment. *IEEE Internet Things J.* **2020**, *7*, 6392–6401. [CrossRef]
100. Hoang, T.-M.; Bui, V.-H.; Vu, N.-L.; Hoang, D.-H. A Lightweight Mixed Secure Scheme based on the Watermarking Technique for Hierarchy Wireless Sensor Networks. In Proceedings of the 2020 International Conference on Information Networking (ICOIN), Barcelona, Spain, 7–10 January 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 649–653.
101. Sun, J.; Wang, W.; Kou, L.; Lin, Y.; Zhang, L.; Da, Q.; Chen, L. A data authentication scheme for UAV ad hoc network communication. *J. Supercomput.* **2020**, *76*, 4041–4056. [CrossRef]

102. Babaeer, H.A.; AL-ahmadi, S.A. Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking. *IEEE Access* **2020**, *8*, 1. [CrossRef]
103. Yaseen, H.A.; Alsalamin, M.; Jarwan, A.; Al-Mistarihi, M.F.; Darabkh, K.A. A Secure Energy-Aware Adaptive Watermarking System for Wireless Image Sensor Networks. In Proceedings of the 2018 15th International Multi-Conference on Systems, Signals & Devices (SSD), Yasmine Hammamet, Tunisia, 19–22 March 2018; IEEE: Piscataway, NJ, USA, 2018; Volume 2, pp. 12–16.
104. Kamel, I.; Juma, H. A Lightweight Data Integrity Scheme for Sensor Networks. *Sensors* **2011**, *11*, 4118–4136. [CrossRef]
105. Kamel, I.; Juma, H. Simplified watermarking scheme for sensor networks. *Int. J. Internet Protoc. Technol.* **2010**, *5*, 101. [CrossRef]
106. Boubiche, D.E.; Boubiche, S.; Toral-Cruz, H.; Pathan, A.-S.K.; Bilami, A.; Athmani, S. SDAW: Secure data aggregation watermarking-based scheme in homogeneous WSNs. *Telecommun. Syst.* **2016**, *62*, 277–288. [CrossRef]
107. Sivasubramanian, N.; Konganathan, G. A novel semi fragile watermarking technique for tamper detection and recovery using IWT and DCT. *Computing* **2020**, *102*, 1365–1384. [CrossRef]
108. Rajeswari, S.R.; Seenivasagam, V. Comparative Study on Various Authentication Protocols in Wireless Sensor Networks. *Sci. World J.* **2016**, *2016*, 1–16. [CrossRef] [PubMed]
109. Kaw, J.A.; Loan, N.A.; Parah, S.A.; Muhammad, K.; Sheikh, J.A.; Bhat, G.M. A reversible and secure patient information hiding system for IoT driven e-health. *Int. J. Inf. Manag.* **2019**, *45*, 262–275. [CrossRef]
110. Shi, X.; Xiao, D. A reversible watermarking authentication scheme for wireless sensor networks. *Inf. Sci.* **2013**, *240*, 173–183. [CrossRef]
111. Hameed, K.; Khan, A.; Ahmed, M.; Goutham Reddy, A.; Rathore, M.M. Towards a formally verified zero watermarking scheme for data integrity in the Internet of Things based-wireless sensor networks. *Futur. Gener. Comput. Syst.* **2018**, *82*, 274–289. [CrossRef]
112. Nguyen, V.-T.; Hoang, T.-M.; Duong, T.-A.; Nguyen, Q.-S.; Bui, V.-H. A Lightweight Watermark Scheme Utilizing MAC Layer Behaviors for Wireless Sensor Networks. In Proceedings of the 2019 3rd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), Hanoi, Vietnam, 21–22 March 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 176–180.