future internet

Review

Review on Semi-Fragile Watermarking Algorithms for Content Authentication of Digital Images

Xiaoyan Yu , **Chengyou Wang *** and **Xiao Zhou**

School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai 264209, China; xyy@mail.sdu.edu.cn (X.Y.); zhouxiao@sdu.edu.cn (X.Z.)

* Correspondence: wangchengyou@sdu.edu.cn; Tel.: +86-631-568-8338

Received: 28 August 2017; Accepted: 21 September 2017; Published: 25 September 2017

Abstract: With the popularity of network and the continuous development of multimedia technology, saving of network bandwidth and copyright protection of multimedia content have gradually attracted people's attention. The fragile watermark for integrity authentication of image data and protection of copyright has become a hotspot. In the storage and transmission process, image data must be compressed to save network bandwidth. As a result, semi-fragile watermarking techniques, which can be used to distinguish common image processing operations from malicious tampering, are emerging. In this paper, semi-fragile watermarking algorithms for image authentication are surveyed. The basic principles and characteristics about semi-fragile watermarking algorithms are introduced, and several kinds of attack behaviors are also included. Aiming at several typical image-authentication algorithms, advantages and disadvantages are analyzed, and evaluation indexes of various algorithms are compared. Finally, we analyze the key points and difficulties in the study on semi-fragile watermarking algorithms, and the direction about future development is prospected.

Keywords: image watermarking; semi-fragile watermark; content authentication; tamper detection; recovery; evaluation indexes

1. Introduction

The 21st century is an era with a large amount of information. People can get almost any information they want through the network, and can store, create, edit, and distribute the information freely using powerful computer software. While it brings convenience to us, the related issues are gradually exposed, especially the issue of information security. Using various editing software for multimedia information, such as Adobe Photoshop, Meitu Xiu Xiu, Image Doctor Software, and so on, original digital products can be copied by pirates without losses, and spread through the Internet, which seriously affects the enthusiasm of creators and causes a negative impact on market health. To achieve certain purposes, pirates can tamper with relevant digital products without trace, which seriously threatens the authenticity and integrity of the information. If the tampered contents involve national security, court evidence, historical documents or other important data, adverse social impacts or considerable political and economic losses may be caused. Therefore, authenticity and necessary integrity protection of multimedia information have become an urgent problem.

The intellectual property rights of digital products can be protected effectively by digital watermarks [1], which has attracted widespread attention of international academic circles and become a research hotspot [2]. The robust watermark, fragile watermark, and semi-fragile watermark are three branches of digital watermarks. Among them, the robust watermark is mainly used for copyright protection. Although it has good transparency and robustness, it cannot determine whether the content of a digital product is tampered with and cannot locate the tampered areas. Fragile watermarks and semi-fragile watermarks are primarily used to certificate the integrity and authenticity of image data. The fragile watermark is usually used to achieve accurate authentication. It regards the digital image as an entirety and does not allow any tampering. Even if there is only a one-bit change, the digital image cannot pass the certification system. The semi-fragile watermark, combining the advantages both of the robust watermark and the fragile watermark, is mainly used for fuzzy authentication of digital images [3]. Under the premise that the image content is basically unchanged, the image is allowed to have a certain degree of distortion. In other words, the common image processing operations can be distinguished from malicious tampering. In addition, semi-fragile watermarking technology can locate the tampered areas as well, or even restore them. In many practical applications, people need to confirm whether the image has been tampered, which areas have been tampered and how to restore them. Thus, the application of robust watermarking technology has been limited. For example, in the legal field, photographs that are the basis for judging the cases must be authentic and complete; in the medical field, 3D medical images play a very important role in healthcare. With the improvement of Internet technology, these images can be transmitted and exchanged in a variety of ways, so it is crucial to ensure the integrity and authenticity of 3D medical images. Castiglione et al. [4] proposed a virtual infrastructure-less Cloud solution for secure management of 3D medical images, combining with the secure watermarking technique to generate a lossless dynamic and adaptive compression engine, and the scheme performs well in terms of invisibility, complexity, compression ratio, adaptability, scalability, and energy efficiency. Furthermore, in the process of image storage and spread, due to the large amount of data, people often choose to compress an image, which limits the application of fragile watermarking technology. Therefore, the semi-fragile watermark has a greater advantage and a wider application in digital image authentication.

However, there are few review articles on the semi-fragile watermark for image authentication, so we have written this paper. We classify several typical semi-fragile watermarking algorithms according to whether they have the ability of recovery, and then classify them further in accordance with the spatial domain and the transform domain. Additionally, we make four tables to compare the basic information and performance of these mentioned algorithms, including size of host images, block size or number of layers, content-based watermark or not, embedded position, the type of non-malicious tampering that the algorithms can resist, the quality factor (QF) of the JPEG (joint photographic experts group) compression, the peak signal-to-noise ratio (PSNR) of the watermarked image and recovered image, and the ability for tamper detection and location. Through this paper, readers can have a more comprehensive understanding of semi-fragile watermarking techniques, and can grasp the basic information and performance of a variety of semi-fragile watermark algorithms used for image authentication easily so that they can access to this area more quickly.

The rest of this paper is organized as follows. Section 2 presents the basic principles and characteristics about semi-fragile watermarking algorithms. Several kinds of common attacks are included in Section 3. Section 4 introduces the evaluation indexes of various algorithms. A literature review on semi-fragile watermark is presented in Section 5. Conclusions and future development are given finally in Section 6.

2. Basic Principles and Characteristics of Semi-Fragile Watermark

Semi-fragile watermarking algorithms for image authentication focus on the ability of detection, location and recovery from tamper attacks carried out on images. Because the semi-fragile watermark has a certain degree of fragility, the algorithm can realize the image authentication according to whether the watermarking data is tampered with. When the host image suffers attacks, the watermarking information will make a corresponding change as well. However, for normal image-processing operations, the semi-fragile watermark also has a certain degree of robustness, so that the normal image processing operations and malicious tampering operations can be distinguished. The framework of the semi-fragile watermarking authentication system contains the watermark embedding process and the watermark detection process. The watermark embedding process is shown in Figure 1, and the watermark detection process is shown in Figure 2 (the dashed part may not be needed in some cases).

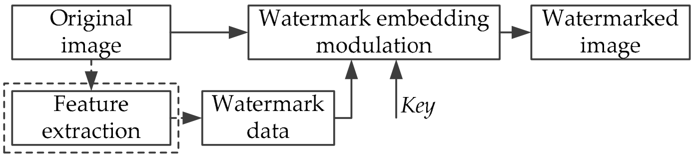

Figure 1. Watermark embedding process.

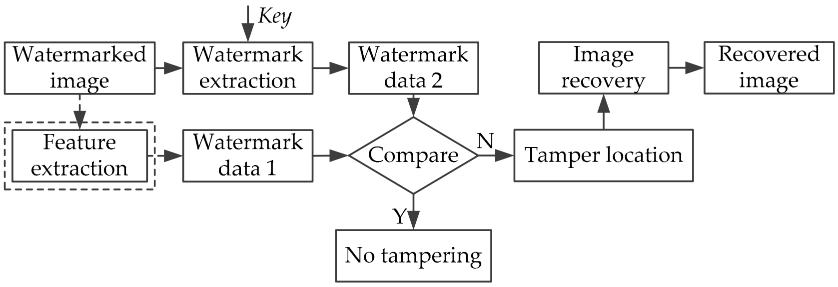

Figure 2. Watermark detection process.

In the embedding process, the watermark can be the information that is determined by the contents of the original image, or the information that is irrelevant to the original image.

In the detection process, the watermarking information in the tested image is extracted and compared with the original watermark. If the two are consistent, we consider that the image has not been tampered with; if the two are inconsistent, we consider that the image has been tampered with. Then the algorithm enters the tamper detection and recovery process. In addition, when the watermarking information is generated using image content features, in the authentication process, there is no need to provide the original watermarking information. Only the comparison between the extracted watermarking information and image content features is needed.

At present, a lot of semi-fragile watermarking algorithms for content authentication have appeared. In general, to achieve good performance, a semi-fragile watermarking algorithm must meet the following characteristics [5]:

- Balance between robustness and fragility.
  On the one hand, after experiencing malicious tampering, such as collage attack, constant average attack, and statistical analysis attack, a watermark should be able to make an alarm response to show its fragility; on the other hand, after experiencing reasonable image-processing operations, such as JPEG compression, brightness adjustment, affine transform, filtering, and noise addition, a watermark should be able to accept them to show its robustness. Therefore, the watermark embedded into the semi-fragile watermarking algorithms must balance the robustness and the fragility well.
- Invisibility.
  After embedding watermark into the image, the quality of the image cannot have obvious degeneration, and the embedded watermark needs to be invisible to ensure that the original image is not damaged.
- Blind detection.
  Sometimes people cannot find the original image in many applications, and even if sometimes the original image is provided by a third party, people still cannot believe it. So this requires that content authentication algorithms can achieve the detection process without original images.
- Localization and recoverability.

If the image has been maliciously tampered with, the algorithm should be able to accurately determine and locate the tampered regions, and then recover it using the recovery data.

- Security.
  Attacks on the security of watermarks are intentional, and the next step is to threaten the robustness of the watermark. Semi-fragile watermarking algorithms should be able to resist malicious tampering, and cannot be easily detected, imitated, tampered with or fabricated by unauthorized parties.
- Versatility.
  Versatility, which is also known as ease of use. If a watermarking algorithm has good performance, it should be applicable to a variety of file formats and media formats.

3. Common Attacks

According to the Kerckhoff principle, it is assumed that the attacker knows all the information about the watermarking algorithm except the secret key. The attacks that threaten the security of watermarks can be divided into three categories: WOA (watermarked only attack), KMA (known message attack), and KOA (known original attack) [6]. Among them, WOA refers to that the attacker only has the data containing the watermark; KMA denotes that the attacker not only has mastered the data involving watermarks, but also grasped some contents of watermarks, and that the secret key can be estimated through a number of observations; KOA means that the attacker knows the data including the watermark and the corresponding original carrier. Additionally, WOA is the most difficult attack to achieve. Because the primary purpose of semi-fragile watermarking technology is to ensure the authenticity and completeness of the digital image content, there has appeared a "pseudo-authentication" attack against the watermark authentication algorithm. That is, while the image content is tampered by this kind of attack, the watermarking information involved in the image will not change, so that the tampered image can still pass the authentication system. According to the existing digital watermarking attack algorithms, the following common attacks are summarized:

3.1. Collage Attack

A collage attack, also known as Holliman-Memon attack [7], is mainly targeted at semi-fragile watermarking algorithms based on block operation. The secret key resource of this attack is limited and the key is independent from the image, the result being that the same location within the images may hide the same watermark information if the secret key and the embedded watermark are exactly the same. The attacker can exchange the blocks in the same position in two of these images, and then splice them to form a new image, which will not affect the extraction of watermarking information. Attackers need to determine whether the watermark information embedded into images is the same, so it belongs to the KMA set. The premise of this kind of attack is that the attacker must collect multiple images that use the same schemes to achieve the embedding of the watermarks.

3.2. Statistical Analysis Attack

Aiming at the situation that the same watermarking information is embedded in lots of different images by using an identical key, the statistical analysis attack has appeared. By analyzing a large number of watermarked images, the attacker can find the law of watermark embedding and estimate the secret key, and then manipulate the content of the images without changing the watermarking information. According to the characteristics of this attack, we can conclude that it conforms to the Kerckhoff principle. In addition, this scheme also needs to determine whether the watermark information embedded in the image is consistent, so it belongs to the KMA set. For this kind of attack, we can embed the watermarking information into different images using different keys, or associate the watermarking information embedded into each authentication unit of the image with the content of other units.

3.3. Vector Quantization Attack

Vector quantization (VQ) attack [8] is another attack algorithm targeting the semi-fragile watermarking algorithm based on block operation. The prerequisite for this attack is that there is no connection between the watermark information embedded in each image block and the contents of the other blocks. The attacker has to know some message of the watermark and classify every sub-block contained in the watermarked image into the corresponding equivalent class, and then the VQ codebook can be generated, so this attack belongs to the KMA set. Through the VQ attack algorithm, other images without watermarks can be faked into watermarked images. Sometimes, in order to make a forged image have a certain meaning, but also has good quality, attackers need to collect and use multiple images. One effective way to resist this attack is to make the watermark information contained in each image block dependent on it in the other blocks. Assuredly, this method may have some bad effects on the tampering and location ability.

4. Evaluation Indexes

For semi-fragile watermarking algorithms applied to authenticate the image content, the indicators, which are used to evaluate their performance, should be able to reflect the invisibility of the watermark, the accuracy of tamper detection, and the ability of recovery. The invisibility of the watermark means that the host image should not undergo significant degeneration after embedding the watermark. The accuracy of tamper detection, which can be reflected by the false positive rate (FPR) and the false negative rate (FNR), is directly related to the quality of the recovered image. The higher the detection accuracy, the better the quality of the image may be recovered.

4.1. Evaluation of the Invisibility of Watermark

The invisibility of the watermark is measured by the quality of the watermarked image. The recovery capability of the algorithm is measured by the quality of the restored image. The higher the quality of the image, the better the invisibility of the watermark will be and the stronger the recovery capability will be. The standard for evaluating the quality of image is the PSNR. Assuming that the size of the image is $M \times N$, the PSNR is defined as Equation (1):

$$\mathrm{PSNR} = 10\log_{10}\frac{255^2}{\mathrm{MSE}}(\mathrm{dB}) \tag{1}$$

$$\mathrm{MSE} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[\boldsymbol{I}(i,j) - \boldsymbol{I}'(i,j)]^2 \tag{2}$$

where $\boldsymbol{I}$ is the original image and $\boldsymbol{I}'$ is the image after processing. The MSE in Equation (2) represents the mean square error between the two parts. The higher the value of the PSNR, the better the image quality will be.

4.2. Tamper Detection Accuracy

The evaluation indexes for tamper detection accuracy of semi-fragile watermarking algorithms mainly include the false positive rate R_{FP}, the false negative rate R_{FN}, and the true positive rate R_{TP}. Among them, R_{FP} is the probability that the unmodified pixels are judged as tampered pixels; R_{FN} refers to the probability that the modified pixels are detected as real pixels; R_{TP} denotes the probability that the modified pixels are correctly defined as tampered pixels [9]. The smaller the values of R_{FP} and R_{FN}, the better the detection accuracy will be, but in general, they cannot be arbitrarily small at the same time. Usually, papers will give the probability of one of them, making it under a certain value, and then make the other value as small as possible. R_{FP}, R_{FN}, and R_{TP} are defined as Equation (3):

$$R_{\mathrm{FP}} = \frac{N_{\mathrm{TF}}}{N_{\mathrm{T}}},\ R_{\mathrm{FN}} = \frac{N_{\mathrm{FT}}}{N_{\mathrm{F}}},\ R_{\mathrm{TP}} = \frac{N_{\mathrm{F}} - N_{\mathrm{FT}}}{N_{\mathrm{F}}} \tag{3}$$

where N_{TF} represents the number of real pixels that are judged to be modified pixels, N_T refers to the number of pixels that have not been tampered, N_{FT} denotes the number of modified pixels that are detected to be real pixels, and N_F indicates the number of modified pixels.

5. Overview on Semi-fragile Watermarking Algorithms

In recent years, with the attention of the international academic community on semi-fragile watermarking technology, more and more algorithms in this field have been designed. As for the methods of semi-fragile watermark, they can be classified according to different starting points. According to the functions of semi-fragile watermarking algorithms, they can be classified into two categories. One is the unrecoverable semi-fragile watermark that can only be used for tamper detection, and the other is the semi-fragile watermark that can recover the tampered areas. According to the embedding position of the watermark, semi-fragile watermark algorithms can be classified into two categories: watermark in spatial domain, and watermark in transform domain. In the following, we will make an overview on semi-fragile watermarking algorithms for image authentication.

5.1. Unrecoverable Semi-Fragile Watermarking Algorithms

The unrecoverable semi-fragile watermarking algorithms can only be used to detect and locate tampered areas. In this paper, we will review them from two aspects: spatial domain and transform domain.

5.1.1. Spatial Domain

For semi-fragile watermarking algorithms in spatial domains, the pixels of digital images are processed directly to achieve the purpose of embedding watermarking information [10–14]. For example, some algorithms embed the watermarking information into the least significant bit (LSB) in the image pixels directly [11,12]. Although the spatial domain algorithms can be implemented easily, it is difficult to balance the invisibility and robustness of the watermark. Schlauweg et al. [10] proposed an authentication algorithm combining multidimensional dither modulation with error-correction coding. By using lattice quantization, the watermarking information associated with the image content is generated by all the pixel values in the image. Then the hash function and multidimensional dither modulation are combined together to encrypt and embed these data. To gain the robustness that can protect against non-malicious distortions without raising security gaps, the algorithm can restore the errors of information bits and the hash values of these error positions in a pre-defined range by combining more complicated multidimensional quantization methods with error correction coding (ECC).

Semi-fragile watermarks can distinguish normal image processing operations from malicious tampering, which is the reason why they are superior to fragile watermarks. In view of this, Xiao and Wang [11] proposed a new semi-fragile watermarking algorithm, which can resist the Laplacian sharpening. The parity of the pixel values and their Laplacian sharpening results are modified to embed the watermark into the spatial domain. This algorithm can tolerate the Laplacian sharpening well. However, it shows fragility when facing the neighborhood averaging and median filter. In addition, since the proposed algorithm only modifies the LSB of pixels, the complexity of it is very low and its fidelity excellent. On the basis of [11], to achieve high robustness for normal image processing operations and good tamper localization precision, Yang et al. used brightness masking, texture masking, and edge masking to advance the development of the human visual system (HVS) in the spatial domain [12]. In the paper, the watermark embedding process is achieved through adaptive LSB replacement. A kind of classification rule for image authentication is proposed, which can effectively distinguish between normal image-processing operations and malicious tampering. Under some mild modifications, the proposed algorithm has a high normalized correlation coefficient (NCC) value and the tampered areas can be located accurately.

To improve the quality of the watermarked image and the accuracy of tampering location, Tiwari et al. [13] proposed a new watermarking algorithm for image authentication based on the vector quantization method. The watermark in the algorithm includes a robust zero-level watermark and a semi-fragile watermark. The two are divided into two stages to complete the watermark embedding process. In the first stage, the algorithm based on the random key combined with the characteristic of indices of the vector quantization image to complete the embedding of the robust zero-level watermark, which enhances security while saving bandwidth. In the second stage, a modified index key based (MIKB) method is used to achieve semi-fragile watermark embedding. In addition, the algorithm adopts the pixel neighborhood clustering method to quantitatively analyze various attacks, thus distinguishing normal image-processing operations from malicious tampering. The algorithm has high watermarking imperceptibility and tampering localization accuracy, and the R_{FP} and R_{FN} of it are very low. Due to the poor robustness of the algorithm in spatial domains, the watermarking information may be destroyed easily.

5.1.2. Transform Domain

The semi-fragile watermarking algorithms in spatial domain perform some kinds of reversible mathematical transforms for the image, and then achieve the watermark-embedding process by modifying the coefficients of the transform domain. The semi-fragile watermarking algorithms in transform domain can take human perception into account, they can balance invisibility and robustness, and they can adapt the compression standard, so they have become a research hotspot in recent years. Among them, the discrete cosine transform (DCT) and discrete wavelet transform (DWT) are the two most commonly used transforms.

- DCT Domain
  Since the block DCT is the basis of JPEG compression, it is possible to embed semi-fragile watermarks into DCT domains to enhance the ability to resist JPEG compression. Lin et al. [3] put forward a semi-fragile watermarking algorithm using spread spectrum technology. The correlation about pixel differences in spatial domains is performed by the detector, which is modified. The watermarking information is embedded into the low- and medium-frequency areas in the DCT domain. Under moderate compression, the tamper detection accuracy of the algorithm in this paper can reach to 75%, while under light compression the accuracy can reach to 90%. In smooth areas, the algorithm can perform well, but in edge or texture areas, its performance is no longer good. To enhance the functions of the algorithm in [3], Al-Mualla proposed a method that can not only adjust to the watermarking strength but the detector type based on the image content characteristics [14]. The algorithm can improve the correlation calculation in edge or texture areas. The watermark embedded in the textured blocks is stronger than in other kinds of blocks. Compared with the algorithm in [3], this algorithm has a much smaller number of false positives, especially in edge and texture areas. However, the switching in the algorithm may lead to lower PSNR.
  Many watermarking algorithms in DCT domains implement the processes of watermark generation and embedding based on important properties of JPEG compression [15,16]. In [15], Ho and Li put forward a watermarking algorithm that embedded watermarks in the DCT domain. The corresponding sign and size of coefficients in the DCT domain are changeless before and after JPEG compression. Based on this point, the feature codes are extracted as watermarking information. To enhance the ability to resist malicious tampering, the algorithm uses the nine-neighborhood system to ensure that the nondeterministic block dependency is implemented. If the host image is quantized to the predetermined QF firstly, it can accept any further compression with the shorter quantization step size. The reason is that the initial quantization coefficients can be accurately re-quantified by using the original step size. According to the invariance principle of DCT coefficients in JPEG image compression process, Tian and Wang carried out the processes of watermark generation and embedding

modulation [16]. Under the condition that the embedding intensity of watermarking information is not increased, the watermarked image can be protected more effectively when faced with transform domain attacks. In this algorithm, the judgment about the false alarm area is added, and the five-neighborhood strategy is combined to realize the correlation between the image blocks, which increases the security of the algorithm and the accuracy of the localization for tampered areas. In addition, this method has the ability to tolerate a certain degree of JPEG compression, but no other non-malignant tampering is involved in the paper.

To avoid cut-and-paste attacks, Preda and Vizireanu [17] proposed a semi-fragile watermarking algorithm based on JPEG compression in the DCT domain. The watermarking information is generated by a pseudo-random sequence that combines the secret key with block-dependent properties, and then it is embedded into the low-frequency DCT coefficients selected by the key based on the modified quantization index modulation method. To resist the JPEG compression with high quality factor, the algorithm quantizes the selected DCT coefficients by using the JPEG quantization matrix before embedding the watermark. The algorithm has good invisibility and high accuracy of tampering localization. In terms of R_{FP} and R_{FN}, it has achieved good performance as well. In addition, the algorithm can be extended into color images easily.

- DWT Domain

  DCT is a global transform from spatial domain to frequency domain for an image, while DWT is a local transform with the capability of multi-scale analysis. Because the DWT has the advantages of both spatial domain and DCT domain, it has become the focus and hotspot in the current research. Zhou et al. [18] combined the spatial domain method with the DWT domain method to propose a semi-fragile watermarking algorithm. The signature is extracted using the spatial domain approach and the watermarking information is inserted by the frequency domain method. The extracted signatures are encoded by the ECC method to eliminate the errors created by normal image processing operations that may bring about changes in the image signatures. To strengthen the security of the watermarking algorithm, the private keys are used to encrypt and decrypt the watermark. This algorithm controls the fragility of the system by adjusting the size of quantization step, and it can resist the traditional image compression. However, since the algorithm extracts the mean value of the pixels in every block as the watermarking information, when the maximum or minimum block is tampered with, the size of quantization step may be altered and then the accurate location of the tampered areas cannot be achieved.

  The algorithms in DWT domains can also be compatible with JPEG2000 compression [19] and JPEG compression [20]. In [19], J. Zhang and C. T. Zhang proposed a semi-fragile digital watermarking method for JPEG2000 image content authentication. This algorithm combined with JPEG2000 encoder and decoder carries out the processes of the watermark generation and embedding modulation based on the invariant parameters in JPEG2000 image compression process. The tampered regions are located by the wavelet transform characteristic so that the reliability of the image authentication system can be improved. This algorithm selects the important coefficients in DWT domain to achieve the embedding modulation of the watermarking information. The size of the macroblock can be adjusted adaptively according to texture features of the image, so the algorithm can be carried out effectively in both the texture areas and the flat areas of the image. The algorithm can tolerate the normal natural images with the compression code larger than 0.5 bits per pixel (bpp). When the code rate is less than 0.5 bpp, there is a significant distortion in a considerable part of image. In [20], according to the fact that the size relationship of the adjacent wavelet coefficients in high frequency is not changed after JPEG compression, Li and Huang proposed a novel semi-fragile watermarking algorithm against the JPEG compression. The algorithm has high watermarking capacity and good anti-JPEG compression performance. At the same time, it can also accurately locate the tampered areas. To obtain a higher PSNR value, the watermarking information is embedded in sub-bands with smaller variance of adjacent coefficients. The algorithm uses parametric integer wavelets to decompose the image and scramble the watermark before embedding. In this way, it becomes difficult for the attacker to get any information about the watermarking information, so the security of the authentication system can be ensured.

To distinguish normal image-processing operations from malicious tampering, Hu and Chen [21] extracted the image characteristics in low-frequency regions of the wavelet domain to obtain two watermarks. One is mainly used to complete the localization of the tampered areas and the other is mainly used to distinguish the normal image processing operations and malicious tampering. Thus, an effective image selection authentication mechanism is provided. The generation and the embedding of the watermark are carried out in the image itself, and two watermark tamper evaluation functions are introduced, which can be used to achieve the purpose of distinguishing attacks. Al-Otum et al. [22] also put forward a semi-fragile watermarking algorithm that can detect and classify the tamper attacks. The algorithm is an improved algorithm based on the quantization approach in the DWT domain, which adopts the multi-scale expansion bits with adjustable watermarking location to embed the random watermarking bit sequence into the DWT low frequency sub-bands of the 2nd DWT levels (LL_2, LL_{LH1}, and LL_{HL1}). It can locate the tampered areas accurately and classify the type of the attacks. However, the algorithm has not been developed to process color images and has not been examined to deal with geometric attacks. Many of the semi-fragile watermarking algorithms based on block operations in the transform domain are susceptible to local tamper attacks.

To eliminate the drawbacks of block-based algorithms, Preda proposed an improved semi-fragile watermarking algorithm that can locate the tampered areas precisely by using the DWT method and permuting wavelet coefficients randomly [23]. Through the quantization, the watermarking data is embedded into DWT coefficients, and the key is embedded into wavelet coefficients of the watermark, which improves the security of the algorithm. Also, the algorithm can resist the mild-to-moderate JPEG compression. In addition, semi-fragile watermarking algorithms not only can be adopted to tamper detection and localization, but also can have other performance. Shefali and Deshpande [24] put forward a semi-fragile watermarking algorithm to protect image information, which not only could detect the tampered areas in images, but also could be used to declare authentication and authorization. By using DWT, the grayscale still image is decomposed into frequency domain, and multiple, multilevel and multi-energy watermarks are embedded in the image for multi-purposes. Additionally, the use of cryptographic keys increases the security of the system.

To improve the security of the watermark, Qi and Xin [25] proposed a semi-fragile watermarking algorithm based on singular value. The watermark in this algorithm is composed of two parts. One is the singular-value-based sequence related to the content, and the other is the private-key-based sequence that is irrelevant to the content. Then the algorithm carries out a series of exclusive-or (XOR) operations on the two parts to obtain the secure watermark. Combined with the adaptive quantization approach, the generated watermark is embedded into a 4×4 block of each approximate sub-band. The authentication system of the algorithm has three levels, containing five measures used to quantify the results of the image content authentication. In addition, after undergoing the mild-to-severe image-processing operations that make no changes to the image content, the algorithm can still detect malicious tampering and locate the tampered areas accurately. However, it cannot resist geometric attacks.

To compare the above-mentioned semi-fragile watermarking algorithms for tamper detection in more detail, Table 1 compares the basic information of the above algorithms, and Table 2 gives the comparisons about the performance of algorithms mentioned above, including the types of non-malicious tampering that the algorithms can resist, the QF of the JPEG compression, the PSNR of the watermarked image, and the ability of tamper detection and location.

Table 1. Basic information of various unrecoverable algorithms.

Algorithm	Domain	Size of Host Image	Block Size or Number of Layers	Content-Based Watermark	Embedded Position
[10]	Spatial	512 × 512	4 × 4	Yes	Spatial domain pixels
[11]		–	3 × 3	No	LSB
[12]		256 × 256	4 × 4	No	LSB
[13]		512 × 512	4 × 4	No	Spatial domain pixels
[3]	DCT	–	8 × 8	No	Low and medium frequency areas in DCT domain
[14]		512 × 512	8 × 8	No	Each block in DCT domain
[15]		248 × 248	8 × 8	Yes	DCT coefficients
[16]		512 × 512	8 × 8	Yes	4 nonzero maximum frequency coefficients in DCT coefficient array
[17]		512 × 512	8 × 8	No	Low frequency areas in DCT domain
[18]	DWT	256 × 256	16 × 16 1 layer	Yes	LL
[19]		512 × 512	5 layers	Yes	DWT main coefficients
[20]		512 × 512	1 layer	No	LH_1, HL_1
[21]		512 × 512	3 layers	Yes	LH_2, HL_2, HH_2
[22]		512 × 512	4 × 4 2 layers	No	LL_2, LL_{LH1}, LL_{HL1}
[23]		Various sizes	3 layers	Yes	LH_2, HL_2, HH_2
[24]		–	2 layers	Yes	LL_2
[25]		512 × 512	4 × 4, 8 × 8 1 layer	Yes	LL of each block in wavelet domain

Table 2. Comparisons of the performance of various unrecoverable algorithms.

Algorithm	Non-Malicious Tampering	QF of Resisting to JPEG (%)	PSNR of Watermarked Image (dB)	The Ability of Tamper Detection and Location
[10]	JPEG	QF ≥ 55	37.1–41.0	–
[11]	Laplacian sharpening	–	57.8	Location accuracy: in units of 3 × 3 pixels
[12]	JPEG, low pass filtering, Laplacian sharpening, and salt and pepper noise	QF ≥ 95	38.01–40.51	–
[13]	JPRG, median filtering, low pass filtering, salt and pepper noise, blurring, and rotation	QF ≥ 70	42.0	R_{FP} = 0.024%, R_{FN} = 0.12%, R_{TP} = 99.8%
[3]	JPEG	QF ≥ 50	36.67	Location accuracy: in units of 16 × 16 pixels. When QF ≥ 60%, R_{TP} ≥ 93%.
[14]	JPEG	QF ≥ 50	35.53	R_{FP} = 13.9%, R_{FN} = 10.4%
[15]	JPEG	QF ≥ 50	37.2	–
[16]	JPEG	QF ≥ 50	–	R_{FP} = 0
[17]	JPEG	QF ≥ 50	44.63	R_{FP} = 0, R_{FN} = 0.26%
[18]	JPEG	–	47.12	–
[19]	JPEG, JPEG2000, median filtering, salt and pepper noise, and Gaussian noise	QF ≥ 40	48.28	–

Table 2. *Cont.*

Algorithm	Non-Malicious Tampering	QF of Resisting to JPEG (%)	PSNR of Watermarked Image (dB)	The Ability of Tamper Detection and Location
[20]	JPEG	QF ≥ 60	30.0–44.2	–
[22]	Gaussian noise, salt and pepper noise, cyclic filtering, median filtering, and JPEG	QF ≥ 50	48.0–56.0	Location accuracy: in units of 8 × 8 pixels
[23]	JPEG	QF ≥ 80	34.26–66.20	Location accuracy: in units of 2 × 2 pixels
[24]	JPEG2000	QF ≥ 40	51.0–62.0	–
[25]	JPEG, JPEG2000, blurring, Gaussian low pass filtering, salt and pepper noise and median filtering	QF ≥ 30	41.39	Location accuracy: in units of 12 × 12 pixels

5.2. Recoverable Semi-Fragile Watermarking Algorithms

The recoverable semi-fragile watermarking algorithms not only can detect and locate the tampered areas, but also can restore them. Such algorithms generally use the compressed version of the image itself or feature data obtained from the image to generate the recovery watermark. Since there are few studies on the spatial domain methods, we will make a review of the semi-fragile watermarking algorithms in transform domains.

5.2.1. DCT Domain

According to the important properties of JPEG compression, a semi-fragile watermarking algorithm based on the JPEG compression's invariant feature of DCT coefficients was proposed by Lin and Chang [26]. The algorithm puts every two image sub-blocks as a block pair, so it can tolerate JPEG compression and distinguish it from malicious tampering effectively. As for the tamper detection accuracy, the algorithm can guarantee a zero false positive rate and get remarkable performance in terms of false negative rate. In addition, the algorithm can tolerate some normal image processing operations, like brightness adjustment. It can identify and locate the tampered areas, and can even recover them by using the original approximation. However, since the authentication performed by this algorithm is independent for any sub-blocks, it must rely on another one or even more sub-blocks in the sub-block pair, which reduces the location accuracy of the watermark. Additionally, there are some defects about the security of the algorithm, and the convergence of watermark-embedding algorithm has not been proved. In [27], Zhong and Jiao proposed an iterative embedding algorithm based on the invariant feature of JPEG compression in the DCT domain. The authentication watermark is obtained by processing the DCT coefficients of the image sub-blocks through the Hash function. At the same time, the image index, block index, and user keys are combined together to resist the VQ attack. This paper offers the effect of the rounding error in the DCT process to the algorithm, and proves the convergence using theory and experimental results. The R_{FP} of the algorithm will be zero after undergoing acceptable JPEG compression. The algorithm can accept JPEG compression when its QF is larger than 50% and channel additive white Gaussian noise (AWGN) with small variance. Local tampering can be effectively detected, located, and recovered. However, the recovery process is only aiming at the direct current (DC) coefficients, and due to the impact of the predetermined quantization table, the block effect may appear in the recovered areas.

To achieve better invisibility under JPEG compression and improve the ability of tampering recovery, Chen et al. [28] used the method of modulo operation based on weight function to realize the hidden purpose. By modulating the seven intermediate frequency DCT coefficients in the range of ±1, the process of watermark embedding is achieved. To enhance security, the algorithm reorganizes the recovery watermark of all the blocks in the host image based on the key, and then embeds them. The quantization step is set by combining the standard JPEG quantization table with the variable scaling factor to achieve the balance between imperceptibility and robustness. At the same time, the algorithm also utilizes the tamper detection method based on the multi-neighborhood feature and multi-threshold optimization to improve the performance of the algorithm. Therefore, the algorithm performs excellently in terms of invisibility, security, and the ability of tampering detection and recovery.

5.2.2. DWT Domain

In this field, Tsai and Chien [29] proposed a low-frequency semi-fragile watermark according to the properties of the DWT. The watermark is embedded into the high-frequency band through the HVS. This algorithm can accurately detect and locate malicious attacks and recover them. In addition, the algorithm can accept moderate modifications, like JPEG compression and AWGN, but does not involve any other types of non-malicious tampering. In [30], Benrhouma et al. proposed a watermarking algorithm combining a cat map with discrete wavelet decomposition approach to ensure security. This algorithm embeds the approximate coefficients of discrete wavelet decomposition, which contain main features of image blocks, in the detail coefficients of the other block, and establishes the association between the two blocks by the cat map. In this way, even if the image is tampered with, the original information can still be retained. In addition, the algorithm can resist moderate tampering, such as JPEG compression, resize, noise addition, and filtering. It can also detect and locate the tampered areas accurately, and recover most of the areas in the original watermarked image.

As block-based semi-fragile watermarking technology is susceptible to local tamper attacks, and the detection accuracy of tampering is often limited to the size of the block, Preda et al. [31] proposed a semi-fragile watermarking algorithm based on wavelet domain with two watermarks. The algorithm uses the random key to permute the wavelet coefficients, and then embeds the authentication watermark. If the key cannot be known, the attacker cannot tamper the watermarked image under the premise that the watermark cannot be destroyed. In addition, the algorithm not only has good robustness for common image processing operations, for malicious tampering it also has high detection accuracy and recovery ability. However, when the tampered areas of the host image exceed to 20%, the recovered image may have poor quality and even cannot be recovered.

Since many existing semi-fragile watermarking algorithms cannot meet important requirements including robustness, security, tampering location and recovery at the same time, Li et al. [32] proposed a novel semi-fragile watermarking algorithm based on group quantization and double authentication. The authentication watermark is extracted from first-order statistical matrix of each image block and embedded into medium-frequency regions of other image blocks. Among them, the embedding process is based on a new group wavelet quantization approach. The algorithm increases the security by permuting the wavelet coefficients in a group randomly. To improve the robustness, the algorithm embeds the watermark into the maximum coefficient in the sub-group by the means of significant difference parity quantization. To improve the accuracy of tampering localization, the algorithm proposed a double authentication ring structure. Since the algorithm is a block-dependent watermarking algorithm, it can resist VQ and collage attacks. The algorithm has medium accuracy ability for tampering localization, but it also can recover the tampered areas. However, the quality of the recovered image needs to be improved further.

5.2.3. Other Transform Domains

In view of the high fidelity requirements for watermarked images, the method of integer wavelet transform (IWT) occurs, and the integer sequence is mapped to integer wavelet coefficients. Phadikar et al. [33] put forward a semi-fragile watermarking algorithm in IWT domain. This algorithm proposes a novel semi-fragile data-hiding technique based on IWT and quantization index modulation (QIM), which is used for tamper detection and correction. Dither modulation (DM) is a kind of special case of QIM. In this paper, the half-toning technology is used to get a watermarking image digest to strengthen the ability of tamper recovery. Since both of the process of embedding and the relatively reliable binary data modulation need to balance the imperceptibility and robustness, the DM-QIM is used to replace the spread-spectrum technique. If the percentage of the tampered areas in the watermarked image is less than 40%, the algorithm can recover the tampered areas effectively. However, the algorithm cannot resist attacks such as collage and VQ attacks. As the embedded space is fixed, the quantity of signal points of the host image used to embed the watermark will be reduced due to the increase of the payload, which may lead to poor detection performance.

The pinned sine transform (PST) can decompose the image into boundary regions and other regions. Since texture features can be reflected well by boundary regions and most legal image processing operations will not change the features, the watermarking data is embedded in the boundary areas to identify and locate the tampered areas. Ho et al. [34] put forward a novel semi-fragile watermarking algorithm using pinned sine transform. The watermark containing the texture features of the original image is embedded into the pinned region of PST, which makes the algorithm extremely sensitive to any changes of texture information in the watermarked image. The key point of this algorithm is to protect the primary texture information of the image, like image edge. If such texture information is destroyed, the watermark cannot survive in the authentication process. As for this authentication algorithm, its probability of tamper detection is higher than 98%, so it can achieve the localization of the tampered areas accurately and recover them approximately. In addition, it has lower sensitivity for acceptable image processing operations than that of the equal algorithms in DCT domain. However, the performance of the algorithm for other non-malicious tampering operations is not involved.

Due to the property that the symbols of the majority of Slant intermediate frequency coefficients can remain unchanged before and after non-malicious tampering, Duan et al. [9] raised a semi-fragile watermarking algorithm in Slant transform domain. The process of watermark embedding is completed by adjusting the values of coefficients in Slant domain, and the process of recovery for the tampered areas is achieved by the LSB algorithm. The algorithm can tolerate the JPEG compression with QF larger than 75% and Gaussian noise with variance less than 0.005. It can also effectively resist the simultaneous implementation of some malicious tampering and non-malicious tampering. However, the algorithm uses a separate block technology, which gives it problems surrounding security and detection accuracy. In addition, the LSB-based recovery algorithm cannot resist the JPEG compression effectively.

To make the algorithm achieve better performance, two different transform domain methods can be used together. Ullah and Ali [35] proposed a smart watermarking image authentication and recovery algorithm by combining the DCT domain method and the IWT domain method together. The HVS based on genetic programming (GP) is used in this algorithm. The watermarking information is generated and embedded in the image by using DCT and IWT domain methods. The generated watermarks include an authentication watermark and a recovery watermark, both of which are independent with each other. Unlike the traditional quantization matrix, the matrix based on genetic programming involves local features of the original image, which is used for compression purposes. In addition, the algorithm can adopt sparse and dense error pixels to restore and define the intensity of tampering. The proposed algorithm can also be adapted to the authentication process of a color image, using the RGB (red, green and blue) channels to generate the image digest. However, for the visual perception of the watermark, this may lead to bad effects.

To compare the above-mentioned semi-fragile watermarking algorithms for tamper detection and recovery in more detail, Table 3 compares the basic information of the above algorithms, and Table 4 gives comparisons about the performance of mentioned algorithms, including the types of non-malicious tampering that the algorithms can resist, the QF of the JPEG compression, the PSNR of the watermarked image, the PSNR of the recovered image, and the ability for tamper detection and location.

Table 3. Basic information of various recoverable algorithms.

Algorithm	Domain	Size of Host Image	Block Size or Number of Layers	Content-Based Watermark	Embedded Position
[26]	DCT	256 × 256	8 × 8	Yes	DCT coefficients
[27]		256 × 256	8 × 8	Yes	Low frequency coefficients in DCT domain
[28]		512 × 512	8 × 8	Yes	Middle frequency coefficients in DCT domain
[29]	DWT	512 × 512	2 layers	Yes	Authentication watermark→LH_2 Recovery watermark→HH_1, HH_2
[30]		256 × 256	4 × 4 1 layer	Yes	High frequency coefficients in the DWT domain
[31]		512 × 512	2 layers	Yes	Authentication watermark→LH_2, HL_2, HH_2 Recovery watermark→LH_1, HL_1, HH_1
[32]		512 × 512	16 × 16, 2 layers	Yes	LH_2, HL_2, HH_2
[33]	IWT	512 × 512	2 layers	Yes	LH_2, HL_2, LH_1, HL_1
[34]	PST	512 × 512	8 × 8	Yes	Each sine transformed pinned-field block
[9]	ST	512 × 512	8 × 8	Yes	Authentication watermark→middle frequency areas of ST domain Recovery watermark→LSB
[35]	DCT and IWT	512 × 512	3 layers	Yes	Authentication watermark→LL_3 Recovery watermark→LH_2, HL_2

Table 4. Comparisons of the performance of various recoverable algorithms.

Algorithm	Non-Malicious Tampering	QF of Resisting to JPEG (%)	PSNR of Watermarked Image (dB)	PSNR of Recovered Image (dB)	The Ability of Tamper Detection and Location
[26]	JPEG and brightness adjustment.	QF ≥ 50	40.7	37.0	R_{FP} = 0. The performance of the R_{FN} is also excellent.
[27]	JPEG and AWGN noise.	QF ≥ 50	39.45	–	R_{FP} = 0. When the number of tampered sub-blocks is large, the R_{FN} will be very low.
[28]	JPEG	QF ≥ 50	36.8–42.6	32.0	$R_{TP} \geq 96\%$
[29]	JPEG and AWGN noise.	QF ≥ 50	39.5	30.7	–
[30]	JPEG, resizing, noising, and filtering.	QF ≥ 80	24.73–40.19	14.22–51.70	R_{FP} = 0.26%, R_{TP} = 56.55%
[31]	Salt and pepper noise, JPEG, Gaussian noise, and brightening	QF ≥ 70	41.5	40.1	Location accuracy: in units of 4 × 4 pixels. R_{FN} = 0
[32]	JPEG and Gaussian noise.	QF ≥ 50	36.0	16.8–20.5	R_{FP} = 0–20%, R_{FN} = 0–55%
[33]	JPEG, filtering, scaling, cropping, deletion, and mixed attacks.	QF ≥ 70	35.02–35.57	31.18–34.92	For JPEG compression and noise attacks, R_{FP} = 0; for smooth attacks, R_{FP} = 0.84%.
[34]	JPEG and wavelet compression.	QF ≥ 40	≥33.0	–	When QF ≥ 40%, $R_{TP} \geq 96\%$.
[9]	JPEG and Gaussian noise.	QF ≥ 75	33.0	–	When the tampered area reaches to 20%, R_{FP} = 0, $R_{FN} \leq 10\%$.
[35]	JPEG	QF ≥ 70	44.0	–	–

Compared with spatial domain algorithms, the image watermarking algorithms in the transform domain have better invisibility and robustness. Therefore, they have been widely used in many situations. In summary, the research status of semi-fragile watermarking algorithms for image content authentication is shown in Figure 3.

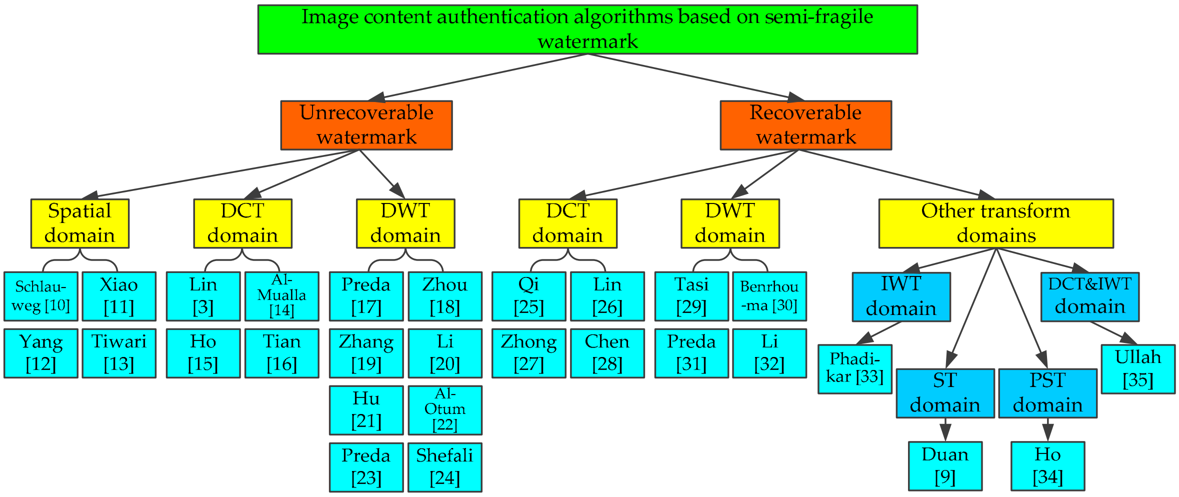

Figure 3. Image content authentication algorithms based on semi-fragile watermark.

6. Conclusions

Along with the high-speed development of computer technology and network technology, various kinds of attacks faced by digital images also show the trend of diversification, which poses a serious challenge to the security of digital images. Therefore, the development and improvement of semi-fragile watermarking techniques for image content authentication are still a focus and hotspot in the digital watermarking area. This paper first introduces the basic principle of semi-fragile watermarking technology and the basic characteristics that it needs to meet. Then evaluation indexes, several kinds of attacks, and algorithm performance are analyzed. Finally, depending on whether the tampered areas can be recovered, we classify and review several typical semi-fragile watermarking algorithms, and then summarize and compare various algorithms from different aspects by making four tables.

Although the research on semi-fragile watermarking algorithms that are used for image content authentication is relatively mature, there are still many difficulties that need to be solved urgently. There is no perfect semi-fragile watermarking algorithm that can meet all the requirements. The existing semi-fragile watermarking algorithm cannot resist all attacks and cannot distinguish all normal image-processing operations from malicious tampering. In addition, many semi-fragile watermarking algorithms are based on image block, which leads to that detection and location for tampered areas are also in block units. This reduces the location accuracy, and it is also not conducive to the recovery of tampered areas. With the introduction of artificial intelligence, semi-fragile watermarking technology has been injected with new vitality. In the future study of semi-fragile watermarks, in addition to solving all above-mentioned difficult problems, researchers will also establish a set of excellent evaluation standards for the watermarking authentication system, making the use of semi-fragile watermarking authentication technology become more extensive in real life.

Acknowledgments: This work was supported by the National Natural Science Foundation of China (No. 61702303, No. 61201371), the Natural Science Foundation of Shandong Province, China (No. ZR2017MF020, No. ZR2015PF004), and the Research Award Fund for Outstanding Young and Middle-Aged Scientists of Shandong Province, China (No. BS2013DX022).

Author Contributions: Xiaoyan Yu and Chengyou Wang reviewed the semi-fragile watermarking algorithms in recent years; Xiaoyan Yu and Chengyou Wang classified the various algorithms, and analyzed the data;

Xiaoyan Yu drafted the manuscript; Xiao Zhou revised the manuscript. All authors have read and approved the final manuscript.

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

References

1. Cox, I.J.; Kilian, J.; Leighton, F.T.; Shamoon, T. Secure spread spectrum watermarking for multimedia. *IEEE Trans. Image Process.* **1997**, *6*, 1673–1687. [CrossRef] [PubMed]
2. Lu, C.S.; Liao, H.Y.M. Multipurpose watermarking for image authentication and protection. *IEEE Trans. Image Process.* **2001**, *10*, 1579–1592. [PubMed]
3. Lin, E.T.; Podilchuk, C.I.; Delp, E.J. Detection of image alterations using semifragile watermarks. In Proceedings of the SPIE—Security and Watermarking of Multimedia Contents II, San Jose, CA, USA, 24–26 January 2000; pp. 152–163.
4. Castiglione, A.; Pizzolante, R.; De Santis, A.; Carpentieri, B.; Castiglione, A.; Palmieri, F. Cloud-based adaptive compression and secure management services for 3D healthcare data. *Future Gener. Comput. Syst.* **2015**, *43–44*, 120–134. [CrossRef]
5. Podilchuk, C.I.; Delp, E.J. Digital watermarking: Algorithms and applications. *IEEE Signal Process. Mag.* **2001**, *18*, 33–46. [CrossRef]
6. Cayre, F.; Fontaine, C.; Furon, T. Watermarking security: Theory and practice. *IEEE Trans. Signal Process.* **2005**, *53*, 3976–3987. [CrossRef]
7. Fridrich, J.; Goljan, M.; Memon, N. Further attacks on Yeung-Mintzer fragile watermarking scheme. In Proceedings of the SPIE—Security and Watermarking of Multimedia Contents II, San Jose, CA, USA, 24–26 January 2000; pp. 428–437.
8. Wong, P.W.; Memon, N. Secret and public key authentication watermarking schemes that resist vector quantization attack. In Proceedings of the SPIE—Security and Watermarking of Multimedia Contents II, San Jose, CA, USA, 24–26 January 2000; pp. 417–427.
9. Duan, G.D.; Zhao, X.; Li, J.P.; Liao, J.M. A novel semi-fragile digital watermarking algorithm for image content authentication, localization and recovery. *Acta Electron. Sin.* **2010**, *38*, 842–847.
10. Schlauweg, M.; Pröfrock, D.; Müller, E.; Palfner, T. Quantization-based semi-fragile public-key watermarking for secure image authentication. In Proceedings of the SPIE—Mathematics of Data/Image Coding, Compression, and Encryption VIII, with Applications, San Diego, CA, USA, 1–3 August 2005; pp. 41–51.
11. Xiao, J.; Wang, Y. A semi-fragile watermarking tolerant of Laplacian sharpening. In Proceedings of the International Conference on Computer Science and Software Engineering, Wuhan, China, 12–14 December 2008; pp. 579–582.
12. Yang, H.F.; Sun, X.M.; Sun, G. A semi-fragile watermarking algorithm using adaptive least significant bit substitution. *Inf. Technol. J.* **2010**, *9*, 20–26.
13. Tiwari, A.; Sharma, M.; Tamrakar, R.K. Watermarking based image authentication and tamper detection algorithm using vector quantization approach. *AEU Int. J. Electron. Commun.* **2017**, *78*, 114–123. [CrossRef]
14. Al-Mualla, M.E. Content-adaptive semi-fragile watermarking for image authentication. In Proceedings of the 14th IEEE International Conference on Electronics, Circuits and Systems, Marrakech, Morocco, 11–14 December 2007; pp. 1256–1259.
15. Ho, C.K.; Li, C.T. Semi-fragile watermarking scheme for authentication of JPEG images. In Proceedings of the International Conference on Information Technology: Coding and Computing, Las Vegas, NV, USA, 5–7 April 2004; pp. 7–11.
16. Tian, B.; Wang, W. New semi-fragile watermarking for JPEG image authentication. *J. Comput. Appl.* **2007**, *27*, 132–134.
17. Preda, R.O.; Vizireanu, D.N. Watermarking-based image authentication robust to JPEG compression. *Electron. Lett.* **2015**, *51*, 1873–1875. [CrossRef]
18. Zhou, X.; Duan, X.H.; Wang, D.X. A semi-fragile watermark scheme for image authentication. In Proceedings of the 10th International Multimedia Modelling Conference, Brisbane, Australia, 5–7 January 2004; pp. 374–377.
19. Zhang, J.; Zhang, C.T. Semi-fragile digital watermarking algorithm for JPEG2000 image authentication. *Acta Electron. Sin.* **2004**, *32*, 157–160.

20. Li, C.; Huang, J.W. A semi-fragile image watermarking resisting to JPEG. *J. Softw.* **2006**, *17*, 315–324. [CrossRef]
21. Hu, Y.P.; Chen, Z.G. Wavelet semi-fragile watermarking algorithm for image authentication. *Acta Electron. Sin.* **2006**, *34*, 653–657.
22. Al-Otum, H.M. Semi-fragile watermarking for grayscale image authentication and tamper detection based on an adjusted expanded-bit multiscale quantization-based technique. *J. Vis. Commun. Image Represent.* **2014**, *25*, 1064–1081. [CrossRef]
23. Preda, R.O. Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain. *Meas. J. Int. Meas. Confed.* **2013**, *46*, 367–373. [CrossRef]
24. Shefali, S.; Deshpande, S.M. Information security through semi-fragile watermarking. In Proceedings of the International Conference on Computational Intelligence and Multimedia Applications, Sivakasi, Tamil Nadu, India, 13–15 December 2007; pp. 235–239.
25. Qi, X.J.; Xin, X. A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization. *J. Vis. Commun. Image Represent.* **2015**, *30*, 312–327. [CrossRef]
26. Lin, C.Y.; Chang, S.F. Semi-fragile watermarking for authenticating JPEG visual content. In Proceedings of the SPIE—Security and Watermarking of Multimedia Contents II, San Jose, CA, USA, 24–26 January 2000; pp. 140–151.
27. Zhong, H.; Jiao, L.C. Semi-fragile watermarking technology in DCT domain. *J. Comput.* **2005**, *28*, 1549–1557.
28. Chen, F.; He, H.J.; Huo, Y.R. Self-embedding watermarking scheme against JPEG compression with superior imperceptibility. *Multimed. Tools Appl.* **2017**, *76*, 9681–9712. [CrossRef]
29. Tsai, M.J.; Chien, C.C. A wavelet-based semi-fragile watermarking with recovery mechanism. In Proceedings of the IEEE International Symposium on Circuits and Systems, Seattle, WA, USA, 18–21 May 2008; pp. 3033–3036.
30. Benrhouma, O.; Hermassi, H.; Belghith, S. Tamper detection and self-recovery scheme by DWT watermarking. *Nonlinear Dyn.* **2014**, *79*, 1817–1833. [CrossRef]
31. Preda, R.O.; Marcu, I.; Ciobanu, A. Image authentication and recovery using wavelet-based dual watermarking. *UPB Sci. Bull.* **2015**, *77*, 199–212.
32. Li, C.L.; Zhang, A.H.; Liu, Z.F.; Liao, L.; Huang, D. Semi-fragile self-recoverable watermarking algorithm based on wavelet group quantization and double authentication. *Multimed. Tools Appl.* **2015**, *74*, 10581–10604. [CrossRef]
33. Phadikar, A.; Maity, S.P.; Mandal, M. Novel wavelet-based QIM data hiding technique for tamper detection and correction of digital images. *J. Vis. Commun. Image Represent.* **2012**, *23*, 454–466. [CrossRef]
34. Ho, A.T.S.; Zhu, X.Z.; Guan, Y.L. Image content authentication using pinned sine transform. *EURASIP J. Adv. Signal Process.* **2004**, *14*, 2174–2184. [CrossRef]
35. Ullah, R.; Alquhayaz, H.A. Intelligent watermarking scheme for image authentication and recovery. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 216–223. [CrossRef]