information

MDPI

Article

Perceptual Hashing Based Forensics Scheme for the Integrity Authentication of High Resolution Remote Sensing Image

Kaimeng Ding [1,2,3], Fan Meng [4], Yueming Liu [2], Nan Xu [5,*] and Wenjun Chen [6]

1 School of Networks and Tele-Communications Engineering, Jinling Institute of Technology, Nanjing 211169, China; dkm@jit.edu.cn
2 Key Laboratory of Resource and Environment Information System, Institute of Geographic Sciences and Natural Resources Research, Chinese Academy of Science, Beijing 100101, China; liuym@lreis.ac.cn
3 Nanjing Innovation Centre of Intelligent Transportation System, Nanjing 211169, China
4 Key Laboratory of Digital Earth Science, Institute of Remote Sensing and Digital Earth, Chinese Academy of Sciences, Beijing 100094, China; mfgenius2000@163.com
5 School of Intelligent Science and Control Engineering, Jinling Institute of Technology, Nanjing 211169, China
6 Nanjing Software Institute, Jinling Institute of Technology, Nanjing 211169, China; chenwenjun@jit.edu.cn
* Correspondence: xunan@jit.edu.cn; Tel.: +86-189-1380-8063

Received: 14 August 2018; Accepted: 5 September 2018; Published: 7 September 2018

Abstract: High resolution remote sensing (HRRS) images are widely used in many sensitive fields, and their security should be protected thoroughly. Integrity authentication is one of their major security problems, while the traditional techniques cannot fully meet the requirements. In this paper, a perceptual hashing based forensics scheme is proposed for the integrity authentication of a HRRS image. The proposed scheme firstly partitions the HRRS image into grids and adaptively pretreats the grid cells according to the entropy. Secondly, the multi-scale edge features of the grid cells are extracted by the edge chains based on the adaptive strategy. Thirdly, principal component analysis (PCA) is applied on the extracted edge feature to get robust feature, which is then normalized and encrypted with secret key set by the user to receive the perceptual hash sequence. The integrity authentication procedure is achieved via the comparison between the recomputed perceptual hash sequence and the original one. Experimental results have shown that the proposed scheme has good robustness to normal content-preserving manipulations, has good sensitivity to detect local subtle and illegal tampering of the HRRS image, and has the ability to locate the tampering area.

Keywords: perceptual hashing; forensics of tampering; high-resolution remote sensing image; image security; integrity authentication

1. Introduction

With the development of remote sensing technology, high resolution remote sensing (HRRS) image is of great help for various fields. The increasing spatial resolution provides new opportunities for advancing remote sensing image analysis and understanding, making it possible to develop novel approaches that were not possible before, especially for defense and military applications. However, it has resulted in a significant challenge: how to ensure the security of HRRS image, particularly the data integrity authentication. Loopholes in data management systems, threats from human factors, and the openness of computer networks make HRRS images vulnerable to various unintentional or intentional tampering attacks during transmission, storage, and use. As a HRRS image has the characteristics of high accuracy and security, if its integrity was affected, its value would be greatly

reduced. In other words, the forensics scheme for the integrity authentication of a HRRS image has important practical significance.

Traditional forensics techniques for data authentication mainly include cryptographic hash functions, digital signatures, and fragile watermarks. Hash functions (e.g., MD5, SHA-1) and digital signatures (e.g., DSA, ECDSA) are very sensitive to bit-level changes in the data, which means as long as the data undergoes an one-bit change, it is considered that the data has been the subject of tamper. This sensitivity is necessary for the authentication of text data, but it is not suitable for image data, including a HRRS image. If data compression or a format conversion operation is performed on HRRS images, the available content they contained does not change, which means the hash function and digital signature technology cannot properly authenticate the HRRS image. The fragile watermark embeds the authentication information in the data, and the embedded information can be extracted to authenticate the integrity of the data. However, the fragile watermark will modify the original data, and the modification would be not permitted for many of the HRRS images. Moreover, the fragile watermarking mainly uses the nature of the watermark itself, and does not emphasize the embedded content, which means it focuses on the change of the data carrier. In summary, traditional forensics techniques such as cryptographic Hash functions, digital signatures, and fragile watermarks cannot fully solve the problem of integrity authentication for a HRRS image. Perceptual hashing, also known as the perceptual hash algorithm, provides a new feasible solution for the forensics of HRRS image.

Perceptual hashing originates from digital watermarking technology, and the earliest perceptual hashing is used to generate the embedded information of watermark. Perceptual hashing is a class of one way mappings from multimedia presentations to a perceptual hash sequence in terms of their perceptual content [1]. A perceptual hash algorithm maps an input image into a compactible feature vector called perceptual hash sequence, which is a short summary of an image's perceptual content and could be applied to content identification, retrieval, authentication, etc. The significant difference between perceptual hashing and cryptographic hash function is that the perceptual hash sequence will not be changed by operations that do not change the data content, such as format conversion or compression. According to different multimedia objects, a perceptual hash algorithm can be classified into an image perceptual hash algorithm, audio perceptual hash algorithm, video perceptual hash algorithm, and so on.

There have been many scholars and institutions that have developed image perceptual hash algorithms [2–26], there are relatively few research results for remote sensing images, and especially few for the forensics of a HRRS image. Although there are many similarities between HRRS images and ordinary images in terms of format and storage, HRRS images have specific characteristics of spatial data. Perceptual hash algorithm for ordinary images cannot satisfy the forensics requirements of integrity authentication for HRRS images.

The HRRS image not only has high-precision, measurable, and high-security properties, but also has distinct multi-scale features. With the continuous improvement of spatial resolution, high-resolution images contain increasingly more information, and feature extraction methods on a single scale that can no longer reflect the valid content of the image. Aiming at high requirements of measuring accuracy and the scale characteristics of the HRRS image, this paper proposes a perceptual hash algorithm based on multiscale robust edge feature for the forensics of integrity authentication for the HRRS image.

The rest of the paper is organized as follows: Section 2 gives an overview of perceptual hashing and discusses the related work. Section 3 describes our proposed scheme in details. Section 4 presents our experimental results and analysis. Conclusions are finally made in Section 5.

2. Related Works

2.1. Overview of Perceptual Hash Algorithm

As HRRS image and common image share the same physical existence form, we refer to the related research of the image perceptual hash algorithm. Image perceptual hash algorithms provide reliable image recognition, image authentication, image retrieval, and other applications. Different applications often have different requirements for perceptual hash algorithms. For image authentication, an ideal image perceptual hash algorithm should satisfy the following requirements:

(1) Robustness: The robustness is the most striking difference between the perceptual hash algorithm and the cryptographic hash function. The cryptographic hash function implements the authentication of the image at the binary level, while the perceptual hash algorithm considers whether the available content of the image has been changed.
(2) Sensitivity to tampering: The perceptual hash algorithm has to be sensitive to malicious tampering operations, which means the visually distinct images should have significantly different hash sequences.
(3) Security: The effective content of the image content cannot be obtained from the perceptual hash sequence, that is, the calculation of image hashing depends on a secret key.
(4) Compactness: When the above characteristics are satisfied, the perceptual hash sequence generated by the algorithm should be as compact as possible. A short perceptual hash sequence is convenient for storage, transfer, and use.
(5) Tamper localization: In some applications, the perceptual hash algorithm should also be able to locate where the image was tampered with.

Perceptual hash algorithms generally include the following steps: image preprocessing, feature extraction, quantization, and hash generation, in which the extraction of features is the key step. According to the different methods of perceptual feature extraction, the perceptual hash algorithm can be roughly divided into the following categories: image statistical information based algorithms, rough representation of image based algorithms, transform domain coefficients based algorithms, feature point based algorithms, matrix decomposition based algorithms, as well as other algorithms:

1. Image statistical information based algorithms generally utilize statistical features such as histogram mean and variance of image blocks. Xiang et al. [2] propose a robust perceptual hash algorithm by using the invariance of the image histogram shape to geometric deformations. The robustness of the algorithm is achieved by using the histogram shape invariance. Xu et al. [3] propose a robust image hash scheme using a multi-resolution histogram for image copy detection, which is invariant to rigid motions and robust to noise. Tang et al. [4] propose a perceptual hash algorithm based on statistical features for color images, which extracts local color features by calculating the block mean and variance. Fang et al. [5] use image statistical information based perceptual hashing for person re-identification, which generates the perceptual hash vector by calculating the average gray value of all pixels. These kinds of algorithms have the advantages of simple principle and good robustness, but the attacker can modify the image content while keeping the image statistical information unchanged, and the security is insufficient. Moreover, there is a certain deficiency in the compactness of the algorithms.
2. Rough representation of image based algorithms mostly make use of the coarse features of the image to be perceptual of the valid content. Swaminathan et al. [6] propose an image perceptual hash algorithm based on Fourier transform features and controlled randomization, which is resilient to content-preserving modifications, such as moderate geometric and filtering distortions. Saad et al. [7] propose a content-based image authentication scheme, which exploits the scalability of a structural digital signature to achieve a good trade off between security and image transfer for networked image applications. Ahmed et al. [8] propose a hash-based image authentication

scheme that uses a secret key to randomly modulate image pixels to create a transformed feature space. This type of method has robust to subtle image modifications, but is more vulnerable to local malicious tampering.

3. Transform domain coefficients based algorithms mainly take the invariant relationship between the coefficients of the image after discrete cosine transform (DCT) or discrete wavelet transform (DWT) as the perceptual feature. Lin et al. [9] present a method for image authentication based on the invariance of the relationships between DCT coefficients at the same position in separate blocks of an image. Lu et al. [10] present an image authentication scheme by making use of the interscale relationship of wavelet coefficients. Zhang et al. [11] propose an authentication signature method for image based on Hotelling's T-square Statistic (HTS) via a Principal Component Analysis (PCA) of block DCT coefficients. Wang et al. [12] present a perceptual hashing for image copy-move forgery detection scheme, which generates the perceptual hash feature based on the DCT coefficient of the fixed-size image blocks. Yang et al. [13] propose an image hash algorithm based on wave atom transform (WAT) using distributed source coding, providing a better performance than existing WAT. This type of approach is relatively insufficient for the geometric transformation of images.
4. Feature point based algorithms. Monga et al. [14] propose an image hashing paradigm based on an iterative feature detector to extract significant geometry preserving feature points. Liu et al. [15] propose an image hash algorithm based on the SIFT operator, which is robust to geometric attacks. In this algorithm, the image digest is constructed through filtering and compressing the SIFT feature vector, which is followed by the quantization based on the centroid of feature vector. Wang et al. [16] propose an image forensic approach for content authenticity analysis. In the proposed method, adaptive Harris corner detection algorithm is used to extract image feature points, then the statistics of the feature point neighborhood are used to construct a forensic signature. Zhao et al. [17] propose a second-order image hash approach based on SIFT for image retrieval. Feature point based algorithms have relatively good robustness, while there are ubiquitous deficiencies in computational complexity. Moreover, those methods cannot prove the uniqueness of image content, that is, images with the same feature point may not have the same content, which makes the security of the perceptual hash algorithm insufficient.
5. Matrix decomposition based algorithms. Kozat et al. [18] propose an image hash algorithm based on singular value decomposition. Sun et al. [19] present a perceptual hash method based on non-negative matrix factorizations (NMF) and principal component analysis (PCA), in which NMF is used to capture the local features of the image. Xiang et al. [20] improve the NMF based perceptual hash algorithm by constraining blocking range and adopting appropriate block size, which provides a satisfactory robustness to image rotation. Tang et al. [21] designed an image hashing based on nonnegative matrix factorization (NMF) and ring partition, which has good discriminative capability. In general, matrix decomposition based perceptual hash algorithms are more sensitive to geometric attacks.
6. Other algorithms. Chen et al. [22] developed an image hash algorithm based on invariants of radial Tchebichef moments. It generates an image hash sequence by adaptive quantization of the invariants of radial Tchebichef moments. Qin et al. [23] designed a hybrid feature extraction based perceptual hashing scheme for color images, in which image normalization, Gaussian low-pass filtering, SVD and Canny operator are applied on the image to improve the robustness of the scheme. Chen et al. [24] propose a novel compressive sensing based perceptual hash algorithm for visual tracking, which constructs a perceptual feature by means of intensity histogram and DCT based on illumination and contour profile. Cui et al. [25] proposed a 3D images hash algorithm by selecting suitable Dual-tree complex wavelet transform coefficients. Yang et al. [26] proposed a perceptual image hashing algorithm by combining latent low-rank representation and rotation invariant uniform local binary patterns.

However, only a few researches on the perceptual hashing for remote sensing image have been carried out, especially for a HRRS image. In the existing research, an adaptive grid partitioning based perceptual hash algorithm is proposed in [27] for the authentication of remote sensing (RS) images, which is essentially the extension of the image perceptual hash algorithm. An edge-feature based perceptual hash algorithm is proposed in [28] to meet the requirements of authentication accuracy partly, while it is not specifically for the HRRS image and it extracts the edge features of different regions of the image at a fixed scale, which makes the sensitivity insufficient for HRRS image forensics. In [29], a perceptual hash algorithm for multi-spectral (MS) remote sensing image authentication is proposed, while its research priority is how to classify the bands of the MS images into several clusters and it takes the traditional DWT based feature extraction approach.

In fact, there are quite differences between the characteristics of MS images and HRRS images. A MS image is characterized by a lower spatial resolution than the HRRS image, but a higher spectral resolution. What is more, each band is taken at a specific wavelength and has explicit physical meaning. In contrast, the HRRS image usually has only one to three wave bands, and its outstanding characteristic is that it has higher spatial resolution and scale features. In this paper, we extend the research to HRRS image based on [28,29]. The design of the perceptual hash algorithms for HRRS image forensics should also be based on the data characteristics and application environment of the HRRS image.

2.2. High Resolution Remote Sensing Image

The HRRS image is essentially the energy distribution map of the electromagnetic radiation characteristics of the ground object obtained by the remote sensor. HRRS images can provide more and more detailed ground features, including not only large-scale features such as water bodies and farm fields, but also small-scale features such as automobiles and traffic signs. It not only contains rich spectral information, but also contains the shape structure and texture information of a large number of objects. Compared with the traditional low or moderate resolution remote sensing image, the meter and sub-meter resolution HRRS images contain multiple scene classes, sufficient diversities, and variations.

HRRS images have high requirements for measurement accuracy. After geometric correction and radiation correction, each pixel of the HRRS image has its own coordinates, which can be measured and positioned according to the scale and coordinates. It requires the forensics scheme of integrity authentication to detect subtle changes in the local image. On the other hand, edge features play an important role in the recognition, understanding and analysis of the HRRS images. The edge information is closely related to the object segmentation, and it is the carrier of objects such as roads and rivers.

However, there are relatively few edge features based perceptual hash algorithms. It is mainly due to the relative lack of robustness to content-preserving operations compared with other image features, such as statistics of image, and rough representation of images. For example, edge features do not preserve better robustness to image rotation operation. While the edge features can meet the requirements of measurement accuracy of HRRS image. For geometrically corrected HRRS image, rotation will change the available content of the image and is considered to be an illegal operation. If the local edge feature of HRRS image changes greatly, it often means that the available content on the image has been tampered with, which also loses its application value. Compared with traditional color, statistical information, and other features based perceptual hash algorithms, edge feature based perceptual hash algorithm can perform integrity verification on HRRS images with higher precision.

The traditional methods of edge extraction mainly include Prewitt, Sobel, Roberts, Kirsch, Canny, Log, etc. However, these methods use the gradient magnitudes as information, which make them difficult to distinguish the faint edge pixels from the noise, and the extracted edge features are not suited to directly generate the of hash sequences. Edge drawing [30] uses more direction information than Canny on its novel edge linking process.

Edge drawing first spots sparse points along rows and columns called anchors, and then joins these anchors via a smart, heuristic edge tracing procedure. It produces a set of edge segments,

which are chains of edge pixels. Edge drawing is fast and uses more direction information than Canny on its novel edge linking process. Instead of the traditional gradient-based methods; e.g., Canny, we adopt edge drawing to extract edge features of the HRRS image.

2.3. Multi-Scale Edge Feature Extraction for HRRS

Remote sensing images have a hierarchical structure and multi-scale characteristics, and the objects they contain can only become meaningful entities at specific scales and show different characteristics at different scales. For a HRRS image, the improvement in spatial resolution increases the internal spectral variability (intraclass variability) of each landcover class and decreases the spectral variability between different classes (interclass variability) [31]. The edge features of HRRS images on a single scale can no longer reflect whether the features change, while multiscale methods intend to use varying-scale versions of the same image and lead to a reduction of the ambiguity inherent to single-scale methods [32]. Therefore, our algorithm construct perceptual hash sequence based on multi-scale edge features to achieve the integrity authentication of HRRS.

In general, the methods of multi-scale edge feature extraction simulate a hierarchical image understanding to process the information at different stages, which are inspired by the human interpretation considering different amounts of information at different parts of the scene [33]. Often multi-scale processing is based on a pyramidal approach: different context sizes and different resolutions are fed as parallel inputs to one or multiple classifiers. In this process, the key concept is the scale that is interpreted in many different ways. In this paper, we assume that the scale of an edge detector is related to the scope of the search for intensity changes [34].

Many multiscale methods have been successfully applied to the detection of edges. For instance, Shih et al. [35] proposed a two-stage edge extraction approach with multiscale edge tracker that refines the results as well as reduces the noised influence. Xiang et al. [36] proposed a multiscale edge detector based on gabor filters for SAR imagery. Antunes et al. [37] introduced a multiscale directional edge detector for cardiac multi-detector CT segmentation. In this paper, we adopt the edge drawing based method to detect edge chains at the each scale, which are more robust against noise.

3. Proposed Scheme

This paper proposes a multi-scale edge features based perceptual hash algorithm for the forensics of integrity authentication. Firstly, the HRRS image is divided into grids, and the feature extraction scale of the grid cells is determined based on the adaptive strategy. Secondly, the multi-scale edge features of the grid elements are extracted by the edge chains, and the edge feature matrix is then constructed. Thirdly, principal component analysis (PCA) is applied on the edge feature matrix, and the normalized principal component is selected as the perceptual feature of the grid cell. Finally, the perceptual features of all grid cells are connected inseries and encrypted with secret key set by user to get the perceptual hash sequence of the HRRS image. The flow chart of the scheme is shown in Figure 1.

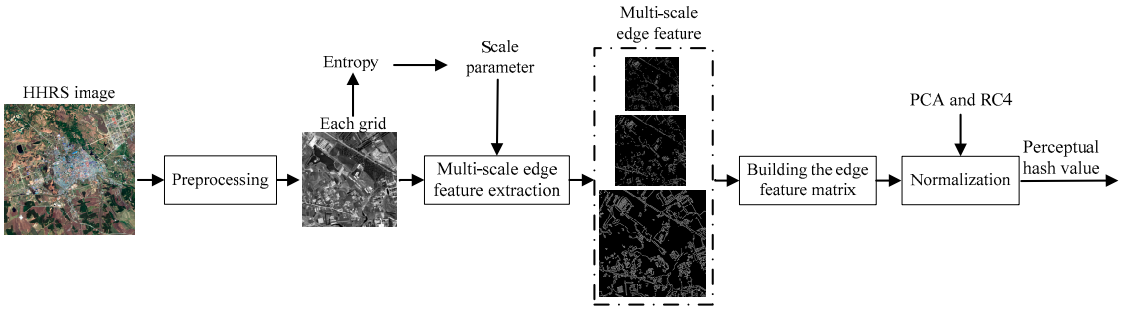


Figure 1. Framework of the proposed scheme.

3.1. HRRS Image Preprocessing

Taking the data's massive characteristics of HRRS images into account, the amount of information in different regions of the same image may not be the same. For instance, the edge information is often more abundant in regions with complex textures. Therefore, the proposed scheme performs distinctive feature extraction on different regions of the image: It divides the HRRS image into grids and extracts different levels of edge information according to the information entropy of the grid units, which not only enables more accurate forensics of tampering for information-rich regions, but also reduces the overall computational complexity of the algorithm and enhances the robustness of the algorithm.

Taking into account the characteristics of multi-bands of remote sensing images, bands of the HRRS image are fused based on the weighted fusion method. Let the original image and the fused image be denoted as R and F respectively:

$$F(x,y) = \sum_{k=1}^{N} \alpha_k R^k(x,y) \tag{1}$$

where R^k denotes the different bands of the original image; N denotes the number of bands of R; $R^k(x,y)$ and $F(x,y)$ denote the pixel values of the band R^k and the fused image F coordinates (x,y), respectively; α_k denotes Pixel weighted weights ($\sum_{k=1}^{N} \alpha_k = 1$), which should be based on the correlation of the band content. In order to make the fusion result more in line with the human eye's visual characteristics, the weighting coefficients are 0.30, 0.59, and 0.11, respectively. For single-band images, band fusion operations are not required.

The fused image F is then partitioned into $W \times H$ grid cells, and each grid cell is denoted as G_{ij} in which $i = 1, 2, \ldots, W$, $j = 1, 2, \ldots, H$. By analyzing the algorithm flow, it can be concluded that the grid cell should be larger than 256×256 pixels and smaller than 512×512 pixels. The size of the grid cells is then unified, that is, the grid resolution is unified to $m \times m$ pixels by bilinear interpolation.

Our work aims at designing such a scheme with good balance between cost and performance. The major computation in the scheme are as follows: grid partition, band fusion, extraction of multi-scale edge features for each grid cell, and the feature encryption. However, encryption is conducted only one time for each HRRS image, grid partition, and band fusion are lightweight. Therefore, the bottleneck of computation lies in the extraction of multi-scale edge features for each grid cell. To reduce the computational complexity and taking tampering sensitivity into consideration, the scheme adaptively determines the number of scales of edge feature extraction and the size of a unified grid cell. What is more, as the tamper location ability is based on the resolution of the grid division, the higher the resolution of the grid partition, the more fine-grained the authentication granularity would be, and the granularity of the differentiating extracted edge features would also be finer, while the computational cost would be raised. The choice of the grid partition resolution thus presents a trade-off between the cost and the ability of tampering location.

In this paper, a two-level adaptive process is taken to describe the algorithm. As information entropy can reflect the amount of average information in the image, information entropy is adopted to measure the amount of the image grid cell. For a grid cell Q_{ij} of size $M \times N$ pixels, the entropy is as follows:

$$E(Q_{ij}) = -\sum_{n=0}^{255} p_n \ln p_n \tag{2}$$

where p_n represents the probability of occurrence of a pixel with a gray value n in the grid cell Q_{ij}.

As shown in Formula (3) and (4), after setting the threshold T of the information entropy, the number of scales of the edge feature extraction is adaptively determined and each grid cell Q_{ij} is subjected to differentiated preprocessing according to the value of the information entropy.

$$L_{ij} = \begin{cases} L_1, E(Q_{ij}) \geq T \\ L_2, E(Q_{ij}) < T \end{cases} \tag{3}$$

$$m_{ij} = \begin{cases} m_1, E(Q_{ij}) \geq T \\ m_2, E(Q_{ij}) < T \end{cases} \tag{4}$$

If information entropy of the grid cell Q_{ij}, that is $E(Q_{ij})$, is greater than or equal to threshold T, the highest level L_{ij} is recommended as L_1 for the region (grid cell) that contains a relatively rich amount of information, and the size of the grid cell is changed to $m_1 \times m_1$ by interpolation algorithm. If $E(Q_{ij})$ is less than or equal to T, L_{ij} is recommended as L_2 ($L_1 > L_2$), for the relatively smooth region, and the size of the grid cell is changed to $m_2 \times m_2$ ($m_1 > m_2$). In the experiment, m_1 and m_2 is set to 128 and 64 respectively, and L_1 and L_2 is set to 3 and 2 respectively.

3.2. Multi-Scale Edge Feature Extraction

Multi-scale edge feature of the grid cell Q_{ij} will be extracted after the preprocessing stage, which is built upon pyramids and edge drawing to detect edge chains at each scale. Instead of testing individual pixels within the edge areas for being edge, we first spot a subset of pixels (called the anchors) and then connect these anchors to get the edge. The multi-scale edge feature process can be summarized as follows:

Step 1. Build a L_{ij}-layer image pyramid P for each grid cell Q_{ij}.

To suppress the noise, a 3×3 Gaussian filter with the standard deviation $\sigma = 1$ is applied on the preprocessed grid cell Q_{ij} with a size of $m_{ij} \times m_{ij}$. Then, the size of the grid cell Q_{ij} is reduced by half with the increment of the level of scales, which means that the size of the image at the level l is $m_{ij}/2l \times m_{ij}/2l$, $l \in \{1, 2, \ldots, L_{ij}\}$. The resized images are the lth layer of the image pyramid, which is denoted as P^l in this paper.

Step 2. Detect the edge chains.

For each image $P^l \in P$, the edge chains on it are detected by the edge drawing method introduced in [14]. The process is as follows:

(1) Computation of the gradient magnitude and edge direction maps. Canny operator is firstly performed on P^l to get an edge map E^l. Then, the edge pixels on E^l are recorded in a set P^l and roughly sorted in the descending order according to the gradient magnitudes G, which can be obtained by the formula $G = \sqrt{G_x^2 + G_y^2}$ where G_x and G_y are the horizontal and vertical gradients of the edge pixel.
(2) The foremost unprocessed edge pixel in P^l is selected as the initial seed pixel pseed, whose 8-neighbors are then searched. If there exists an 8-neighbor and unprocessed edge pixel, we consider it as the next seed pixel and add it into the current edge chain.
(3) The seed growing of the current edge chain is conducted iteratively until all the pixels in the chain is processed, and then we begin with another edge chain from the rest of P^l. The set of edge chains on P^l is denoted as C^l.

Step 3. Get the fused edge feature.

To fuse the edge features, it has to get the corresponding edge pixels on the original grid cell Q_{ij} of the pixels in edge chains C^l. The process is as follows:

(1) Traversing the grid cell Q_{ij} to detect the candidate edge pixel. For each pixel $Q_{ij}(x_0,y_0)$ of the grid cell, if there is a corresponding scaled pixel $P^l(x_l,y_l) = (x_0/2^l, y_0/2^l)$ on any layer of the image pyramid is an edge pixel, we consider $Q_{ij}(x_0,y_0)$ to be a candidate edge pixel. For all these candidate edge pixels, a mask image with the same size of Q_{ij} is created.

(2) Processing non-maximum suppression [38] on the pixel of the mask image to get real edge pixels, in which the gradient orientation of each pixel is defined as that of the corresponding pixels on the original grid cell Q_{ij}. The real edge pixels are the anchors.

(3) Connecting the anchors to get the fused edge feature. We simply go from one anchor to the next by proceeding over the cordillera peak of the gradient map mountain, which is guided by the gradient magnitude and edge direction maps.

The obtained edge image of the grid cell Q_{ij} is denoted as E_{ij}. Then we serialize E_{ij} to construct the edge feature matrix denoted by ME_{ij}. The serialization process is as follows: scanning from left to right and top to bottom. If the pixel is an edge point, the corresponding matrix element $ME_{ij}(x,y)$ is recorded as 1, otherwise it is recorded as 0.

3.3. The Generation of Perceptual Hash Sequence

It can be seen that ME_{ij} is a 0–1 matrix reflecting the edge features of the grid cells. To eliminate the conflict between robustness and tamper sensitivity, we perform principal component analysis (PCA) on ME_{ij} for noise reduction and data compaction. PCA is a common transform that is often used in numerical analysis of matrices [39–41]. It reduces the large dimensionality of image data in order to reduce the dimensionality of independent feature space.

In this paper, PCA is used to reduce the dimensionality and remove the redundant inter-spectral information to obtain the principal components of the edge feature. By performing PCA on the edge feature matrix ME_{ij}, the linear correlation of the matrix element can be removed. This means that the noise can be effectively removed and the extracted feature achieves data compression. The principal components of the edge feature matrix are then standardized in order to obtain the fixed-length string. The standardized string is the perceptual hash sequence of the grid, denoted as PH_{ij}. All of the grid's perceptual hash sequences are put together and encrypted by using a cryptographic encryption algorithm that takes RC4 as an example to enhance the security with secret *key* set by user. The encrypted sequence is the perceptual hash sequence of the original HRRS, denoted as PH:

$$PH = Encrypt_{RC4}(PH_{0,0}||PH_{0,1}||\ldots||PH_{W,H}, key) \tag{5}$$

where *key* is to guarantee the security of the algorithm.

3.4. Forensics of Tampering for HRRS Image

The forensics process of integrity is performed via the comparison between the reconstructed perceptual hash sequence and the original one: the higher the perceptual hash sequences' difference, the greater the corresponding images' difference. Although the hamming distance is frequently used to evaluate the difference between two sequences, it is not suitable for this purpose, because the length of the hash sequence may vary along with the change of algorithm parameters. We adopt the followed "Normalized Hamming Distance" [27] to evaluate the difference between two hash sequences:

$$Dis = \left(\sum_{i=1}^{L} |h1(i) - h2(i)| \right) / L \tag{6}$$

where h_1 and h_2 are perceptual hash sequences with L length. It is observed that the normalized hamming distance Dis is a float between 0 and 1. If the Dis of two perceptual hash sequences of the same area is lower than the threshold T_h, it means that the corresponding area is content-preserving; otherwise, it means that the content of the corresponding area has been tampered with.

The forensics of tampering process for a HRRS image can be described as follows: the same step is used to generate the perceptual hash sequence PH of the HRRS to be authenticated, and the received perceptual hash sequence of the original HRRS is denoted as PH'; set the threshold T_h of Dis, and calculate the Dis between the perceptual hash sequences PH_{ij} and corresponding one according to Formula (6) to verify whether the content of each grid unit has been tampered. If the image has been tampered with, the tampered area can be located to a specific geographic area. The granularity of the tampering positioning depends on the granularity of the grid division.

4. Experiments and Discussions

In this section, several experiments are conducted to evaluate the performance of the proposed scheme with our collected datasets. All experiments were implemented on a computer with a 2.40 GHz Intel i7 processor and 4.00 GB memory running Windows 10 operating system. The test software was developed using Microsoft Visual Studio 2013 in C++ and reading HRRS image based on GDAL library function.

4.1. Experiments Setting

The test image set contains 12 three-band HRRS images in Tiff format acquired by GeoEye-1, GaoFen-2, Pleiades-1, and WorldView-2 satellites, respectively, as show in Figure 2. From Figure 2a–l, the sizes of these HRRS images are 2455 × 1650 pixels, 1785 × 2400 pixels, 2495 × 2380 pixels, 6500 × 4500 pixels, 3000 × 3000 pixels, 3000 × 3000 pixels, 3000 × 3000 pixels, 5000 × 5000 pixels, 4200 × 5000 pixels, 4200 × 5000 pixels, 4200 × 5000 pixels, and 4200 × 5000 pixels, respectively. Our proposed method was compared with a traditional cryptographic authentication algorithm, classical perceptual hash algorithm for image, and perceptual hash algorithm for remote sensing image proposed in [28].

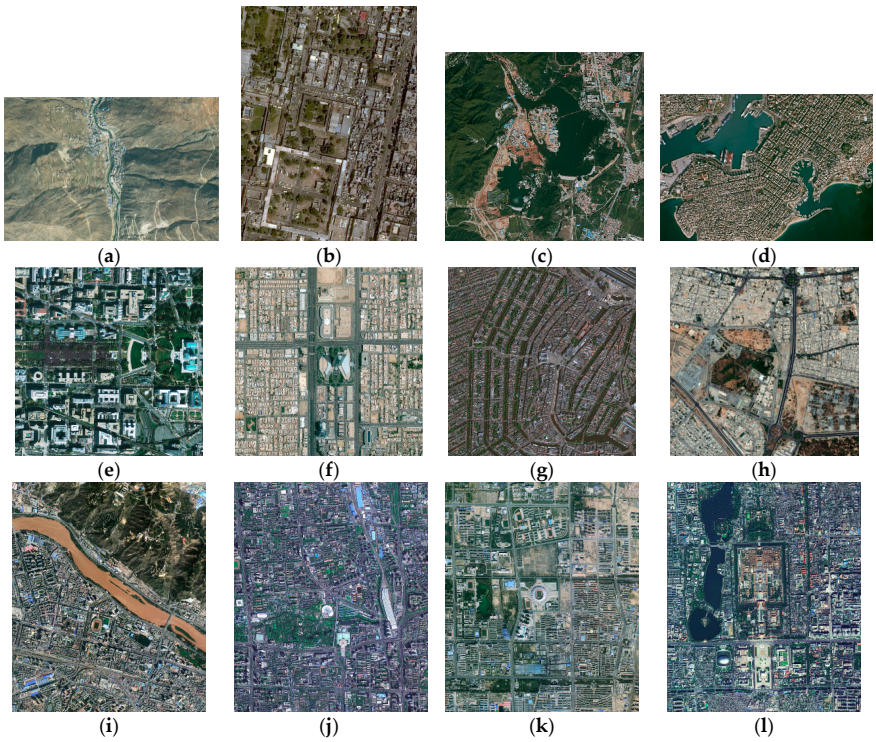


Figure 2. The high resolution remote sensing (HRRS) images used in the experiment; (**a**) image A (1786 × 2041 pixels); (**b**) image B (2455 × 1450 pixels); (**c**) image C (2495 × 2381 pixels); (**d**) image D (6500 × 4500 pixels); (**e**) image E (3000 × 3000 pixels); (**f**) image F (3000 × 3000 pixels); (**g**) image G (3000 × 3000 pixels); (**h**) image H (5000 × 5000 pixels); (**i**) image I (4200 × 5000 pixels); (**j**) image J (4200 × 5000 pixels); (**k**) image K (4200 × 5000 pixels); (**l**) image L (4200 × 5000 pixels).

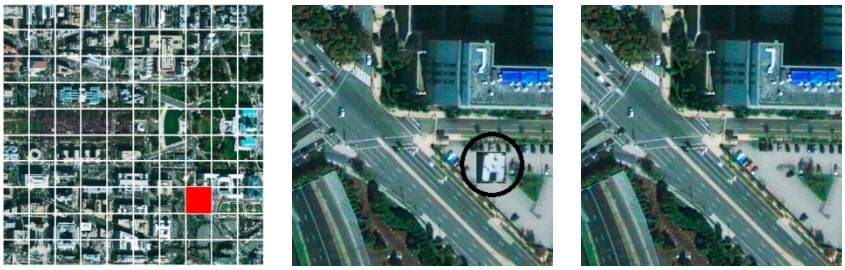
As mentioned in Section 3.1, the size of the grid cell should be larger than 256 × 256 pixels and smaller than 512 × 512 pixels. The granularity of grid partitioning is set to 6 × 4, 4 × 6, 6 × 6, 24 × 16, 10 × 10, 10 × 10, 10 × 10, 16 × 16, 12 × 16, 12 × 16, 12 × 16, 12 × 16. Thus, the total number of grid cells equivalent to the individual image used in a conventional image perceptual hash algorithm is about 1812, which is important for the robustness of the algorithm.

In the proposed scheme, the information entropy threshold T is set to the average of the information entropy of the grid cell in the same HRRS image. For the algorithm proposed in [28], the size of the pre-processed grid cell is set to 128 × 128 pixels to ensure the fairness of the test.

4.2. Sensitivity to Tampering Experiments and Analysis

As this scheme aims to achieve the forensics of integrity authentication for HRRS image, it must be able to detect the subtle malicious tampering, which means that the tampered and original images should have significantly different perceptual hash sequences. If the HRRS image has been tampered, the edge features of the corresponding grid cell and the regenerated perceptual hash sequence would be changed, and the malicious tampering can be detected. What is more, this algorithm has a certain ability of tamper localization.

Figure 3 shows an example of tamper location, wherein Figure 3a shows the result of tamper location, and Figure 3b,c respectively show the tampered grid cell and the original one.



(**a**) (**b**) (**c**)

Figure 3. An example of tamper location: (**a**) The result of tamper location; (**b**) The tampered grid cell; (**c**) The original grid cell.

Obviously, the tampering location granularity depends on the granularity of the grid partition. In theory, the finer the granularity of the grid division, the more accurate the tampering location granularity and the higher the accuracy of authentication. However, it will consume more computing time and storage space if the grid partitioning is too granular. The granularity of grid partitioning depends on the specific HRRS image and actual certification requirements.

To compare the performance of sensitivity to tampering with other perceptual hash algorithms, we take several kinds of tampering operations, including removing, appending, and changing the object. Taking into account the characteristics of data magnanimity of HRRS images, this algorithm extracts the features from each grid cell, while the image perceptual hash algorithm mostly extracts the global features of images to generate hash sequences. To ensure the fairness of the test, we chose the image grid unit instead of the entire image for testing, as shown in Figures 4–7.

The more popular image perceptual hash algorithm mainly includes the method based on DCT (discrete cosine transformation) [9,11,12,24], the method based on wavelet transform [10,13], and the method based on SVD (singular value decomposition) [18]. We compare the above algorithm with this proposed algorithm, and the comparison results are shown in Table 1. Without affecting the robustness of the algorithm, the threshold of the normalized hamming distance of the method based on wavelet transform is set to 0.01, the threshold of the method based on DCT is set to 0.01, the threshold of the method based on SVD is set to 0.002, and the threshold of the algorithm is set to 0.10.

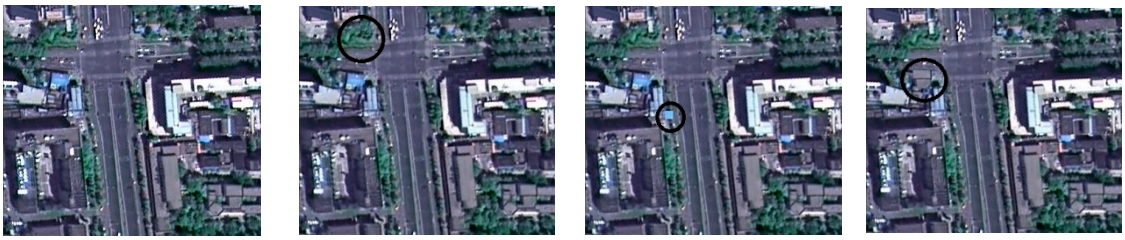
It can be observed from Table 1 that this proposed algorithm can detect subtle tampering of the HRRS image with higher precision, which meets the high-accuracy forensics requirements of HRRS images.

(**a**) (**b**) (**c**) (**d**)

Figure 4. Tampering Test 1: (**a**) The original grid cell; (**b**) Removing the object; (**c**) Appending the object; (**d**) Changing the object.

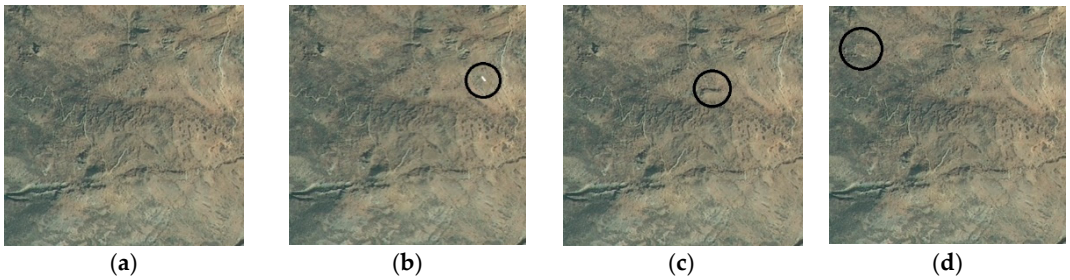
(**a**) (**b**) (**c**) (**d**)

Figure 5. Tampering Test 2: (**a**) The original grid cell; (**b**) Removing the object; (**c**) Appending the object; (**d**) Changing the object.



(**a**) (**b**) (**c**) (**d**)

Figure 6. Tampering Test 3: (**a**) The original grid cell; (**b**) Removing the object; (**c**) Appending the object; (**d**) Changing the object.



(**a**) (**b**) (**c**) (**d**)

Figure 7. Tampering Test 4: (**a**) The original grid cell; (**b**) Local subtle tampering instance 1; (**c**) Local subtle tampering instance 2; (**d**) Local subtle tampering instance 3.

Table 1. The comparison of tamper detection.

	Algorithm Based on DCT	Algorithm Based on Wavelet Transform	Algorithm Based on SVD	Algorithm in Paper [28]	Our Scheme
Figure 4b	Undetected	Undetected	Detected	Detected	Detected
Figure 4c	Detected	Detected	Detected	Detected	Detected
Figure 4d	Detected	Detected	Detected	Detected	Detected
Figure 5b	Detected	Detected	Detected	Detected	Detected
Figure 5c	Undetected	Detected	Undetected	Detected	Detected
Figure 5d	Detected	Detected	Detected	Detected	Detected
Figure 6b	Undetected	Undetected	Undetected	Detected	Detected
Figure 6c	Undetected	Undetected	Undetected	Undetected	Detected
Figure 6d	Undetected	Undetected	Undetected	Detected	Detected
Figure 7b	Undetected	Undetected	Undetected	Undetected	Detected
Figure 7c	Undetected	Undetected	Undetected	Detected	Detected
Figure 7d	Undetected	Undetected	Undetected	Undetected	Detected

4.3. Robust Experiments and Analysis

Robustness is the most significant difference between perceptual hashing and cryptographic hashing. In this study, if the HRRS images have undergone content-preserving manipulations, the normalized Hamming distance between the perceptual hash sequences of the original image and the processed one should be under the pre-determined threshold T.

As format conversion and digital watermark embedding are typical operations that do not change the image content, we adopt format conversion and watermark embedding as examples to test the robustness. The format conversion operation converts the original TIFF format image into BMP format, and the watermark embedding algorithm takes the least significant bit (LSB) as an example. The threshold T_h of the normalized Hamming distance Dis is set to 0 (that is, the perceptual hash sequence is required to be identical to indicate that the grid has not been tampered). In this paper, the robustness of the algorithm is described by the percentage of grid cells whose perceptual hash sequence has not changed. As shown in Table 2, the perceptual hash sequence of all grid cells of the test image has not changed, which means the proposed algorithm is robust to format conversion and LSB watermark embedding.

Table 2. The results of the robustness test (T_h is set to 0).

Manipulation	Format Conversion (TIFF to BMP)	Lossless Compression (PNG Compressing)	Digital Watermarking (LSB)
Image A (6 × 4 partition)	100%	100%	100%
Image B (4 × 6 partition)	100%	100%	100%
Image C (6 × 6 partition)	100%	100%	100%
Image D (24 × 16 partition)	100%	100%	100%
Image E (10 × 10 partition)	100%	100%	100%
Image F (10 × 10 partition)	100%	100%	100%
Image G (10 × 10 partition)	100%	100%	100%
Image H (16 × 16 partition)	100%	100%	100%
Image I (12 × 16 partition)	100%	100%	100%
Image J (12 × 16 partition)	100%	100%	100%
Image K (12 × 16 partition)	100%	100%	100%
Image L (12 × 16 partition)	100%	100%	100%

In contrast, cryptographic authentication methods cannot achieve better certification, since they treat the above manipulation as illegal operations and their hash value would be changed dramatically after content-preserving manipulations.

Next, the robustness of JPEG compression and brightness adjustment operation are tested. The threshold T_h is set to 0.20. The proportion of grid cells that the Dis is greater than T_h are shown in Table 3.

Table 3. The results of the robustness test (T_h is set to 0.20).

Manipulation	JPEG Compression (98%)	JPEG Compression (90%)	Brightness Adjustment (5% Reduction)
Image A (6 × 4 partition)	91.7%	86.1%	83.3%
Image B (4 × 6 partition)	91.7%	84.4%	81.3%
Image C (6 × 6 partition)	88.9%	86.1%	80.6%
Image D (24 × 16 partition)	91.1%	83.9%	79.4%
Image E (10 × 10 partition)	92.0%	86.0%	83.0%
Image F (10 × 10 partition)	93.0%	82.0%	81.0%
Image G (10 × 10 partition)	92.0%	80.0%	84.0%
Image H (16 × 16 partition)	91.0%	85.9%	81.6%
Image I (12 × 16 partition)	89.6%	85.9%	80.7%
Image J (12 × 16 partition)	93.8%	86.5%	82.3%
Image K (12 × 16 partition)	89.6%	85.9%	81.8%
Image L (12 × 16 partition)	91.2%	83.9%	80.7%

The robustness of the algorithm can be adjusted by changing the algorithm parameters such as T_h. However, if the robustness is excessively emphasized, the sensitivity may be directly affected and some tampering of the HRRS image may be impossible identified, which affects the authentication accuracy of the HRRS image.

Since the authentication object of this algorithm is the corrected (geometric correction and radiation correction) HRRS image, the rotation robustness is out of our consideration.

4.4. Computational Efficiency Experiments and Analysis

The computational efficiency of the proposed algorithm is tested and compared with the algorithm in [28] and traditional DWT-based algorithm with the same software and hardware platforms. The results are shown in Table 4.

Table 4. The comparison of the computational efficiency (in seconds).

	DWT-Based Algorithm	Algorithm in [28]	Our Scheme
Image A (6 × 4 partition)	0.85	1.56	4.56
Image C (6 × 6 partition)	1.33	2.25	6.71
Image D (24 × 16 partition)	18.34	31.56	73.34
Image G (10 × 10 partition)	3.78	6.09	17.38
Image L (12 × 16 partition)	7.05	12.36	33.12

As can be seen from Table 4, although our scheme has high sensitivity to subtle tamperings compared with traditional DWT-based algorithm and the algorithm in [28], the computational efficiency is inferior to the existing research, and how to improve the computational efficiency of this scheme is one of our future work goals. As mentioned in Section 3.1, the bottleneck of computation lies in the extraction of multi-scale edge features for each grid cell. The key to improving the computing performance is how to efficiently extract multi-scale features.

What is more, the computational complexity of the scheme has a great relationship with the granularity of grid partition and the information entropy threshold T. The finer the grid partition, the finer the granularity of the tampering location; however, the computational complexity will be greater. The smaller the information entropy threshold T, the greater the computational complexity, while tampering sensitivity is reduced.

4.5. Analysis of Algorithm Safety

The security of the perceptual hash algorithm mainly refers to the unidirectionality, that is, no valid information of the image content can be obtained from the perceptual hash sequences without the key. The security of this algorithm relies on the security of the cryptographic encryption algorithm,

and we adopt the RC4 algorithm as an example in this paper. As the security of the RC4 algorithm has been widely recognized, our algorithm has enough security.

5. Conclusions

For special characters, a high resolution remote sensing image has higher requirements in data security. In this paper, we have proposed a perceptual hashing based forensics scheme for the integrity authentication of a high resolution remote sensing image. Different from traditional forensics methods, this algorithm focuses on the content integrity of HRRS, instead of the carrier of the content. The proposed scheme extracts multi-scale edge features of the HRRS images to generate the perceptual hash sequences, in which the adaptive preprocessing is a balance between efficiency and authentication accuracy, and PCA decomposition is to reduce the contradiction between the robustness and tamper sensitivity of the algorithm. The length of the perceptual hash sequence generated by the algorithm changes elastically with the requirements authentication accuracy and the size of the image. The experiments show that the algorithm can resist content-preserving operations while detecting the subtle tamper of the HRRS image, achieving high authentication accuracy for the HRRS image.

In future work, we plan to improve the computational efficiency of this scheme and to improve the robustness against lossy compression while maintaining the ability to detect subtle tampering.

Author Contributions: K.D. conceived the idea and worked together with F.M. to design the scheme; Y.L. and N.X. assisted with the study design; W.C. helped to analyze the experimental data. All authors reviewed the manuscript.

Funding: This study is patricianly supported by the grants from: (a) the National Natural Science Foundation of China (Grant Nos. 41801303, 41601396); (b) the Jiangsu Province Science and Technology Support Program (Grant No. BK20170116); (c) the Scientific Research Hatch Fund of Jinling Institute of Technology (Grant Nos. jit-fhxm-201604, jit-b-201520); and (d) the State Key Laboratory of Resource and Environment Information System Open Funding Program.

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

References

1. Niu, X.M.; Jiao, Y.H. An Overview of Perceptual Hashing. *Acta Electron. Sin.* **2008**, *36*, 1405–1411.
2. Xiang, S.; Kim, H.J.; Huang, J. Histogram-based image hashing scheme robust against geometric deformations. In Proceedings of the 9th Workshop on Multimedia & Security, Dallas, TX, USA, 20–21 September 2007; pp. 121–128.
3. Xu, Z.; Ling, H.; Zou, F.; Li, P. Robust image copy detection using multi-resolution histogram. In Proceedings of the International Conference on Multimedia Information Retrieval, Philadelphia, PA, USA, 29–31 March 2010; pp. 129–136.
4. Tang, Z.J.; Zhang, X.Q.; Dai, X.; Yang, J.Z.; Wu, T.X. Robust image hash function using local color features. *AEU Int. J. Electron. Commun.* **2013**, *67*, 717–722. [CrossRef]
5. Fang, W.; HU, H.M.; Hu, Z.; Liao, S.C.; Li, B. Perceptual hash-based feature description for person re-identification. *Neurocomputing* **2018**, *272*, 520–531. [CrossRef]
6. Swaminathan, A.; Mao, Y.; Wu, M. Robust and secure image hashing. *IEEE Trans. Inf. Forensics Secur.* **2006**, *1*, 215–230. [CrossRef]
7. Saad, S.M. Design of a robust and secure digital signature scheme for image authentication over wireless channels. *IET Inf. Secur.* **2009**, *3*, 1–8. [CrossRef]
8. Ahmed, F.; Siyal, M.Y.; Abbas, V.U. A secure and robust hash-based scheme for image authentication. *Signal Process.* **2010**, *90*, 1456–1470. [CrossRef]
9. Lin, C.Y.; Chang, S.F. A robust image authentication method distinguishing JPEG compression from malicious manipulation. *EEE Trans. Circuits Syst. Video Technol.* **2001**, *11*, 153–168.
10. Lu, C.S.; Liao, H.Y.M. Structural digital signature for image authentication: An incidental distortion resistant scheme. *IEEE Trans. Multimed.* **2003**, *5*, 161–173.
11. Zhang, Y.D.; Tang, S.; Li, J.T. Secure and Incidental Distortion Tolerant Digital Signature for Image Authentication. *J. Comput. Sci. Technol.* **2007**, *22*, 618–625. [CrossRef]

12. Wang, H.; Wang, H.X. Perceptual Hashing-Based Image Copy-Move Forgery Detection. *Secur. Commun. Netw.* **2018**, *2018*, 1–11. [CrossRef]
13. Yang, Y.; Zhou, J.; Duan, F.; Liu, F.; Cheng, L.M. Wave atom transform based image hashing using distributed source coding. *J. Inf. Secur. Appl.* **2016**, *31*, 75–82. [CrossRef]
14. Monga, V.; Evans, B.L. Perceptual image hashing via feature points: Evaluation and tradeoffs. *IEEE Trans. Image Process.* **2006**, *15*, 3452–3465. [CrossRef] [PubMed]
15. Liu, Z.Q.; Li, Q.; Liu, J.R.; Peng, X.Y. SIFT based image hashing algorithm. *Chin. J. Sci. Instrum.* **2011**, *32*, 2024–2028.
16. Wang, X.F.; Xue, J.R.; Zheng, Z.Q.; Liu, Z.L.; Li, N. Image forensic signature for content authenticity analysis. *J. Vis. Commun. Image Represent.* **2012**, *23*, 782–797. [CrossRef]
17. Zhao, X.H.; Li, Z.R.; Yi, J.K. SIFT Feature-Based Second-Order Image Hash Retrieval Approach. *J. Softw.* **2018**, *13*, 103–116. [CrossRef]
18. Kozat, S.S.; Venkatesan, R.; Mihcak, M.K. Robust perceptual image hashing via matrix invariants. In Proceedings of the 2004 International Conference on Image Processing (ICIP), Singapore, 24–27 October 2004; pp. 3443–3446.
19. Sun, R.; Gao, J. Image Hashing method via combination of NMF and PCA. *J. Electron. Meas. Instrum.* **2009**, *23*, 52–57. [CrossRef]
20. Xiang, S.J.; Yang, J.Q. NMF-Based Image Hashing Algorithm Using Restricted Random Blocking. *J. Electron. Inf. Technol.* **2011**, *33*, 337–341. [CrossRef]
21. Tang, Z.J.; Zhang, X.Q.; Zhang, S.C. Perceptual Image Hashing Based on Ring Partition and NMF. *IEEE Trans. Knowl. Data Eng.* **2014**, *26*, 711–724. [CrossRef]
22. Chen, Y.C.; Yu, W.Y.; Feng, J.C. Robust image hashing using invariants of Tchebichef moments. *Opt. Int. J. Light Electron Opt.* **2014**, *125*, 5582–5587. [CrossRef]
23. Qin, C.; Sun, M.; Chang, C.C. Perceptual Hashing for Color Images Based on Hybrid Extraction of Structural Features. *Signal Process.* **2017**, *142*, 194–205. [CrossRef]
24. Chen, L.; Li, Z.; Yang, J.F. Compressive perceptual hashing tracking. *Neurocomputing* **2017**, *239*, 69–80. [CrossRef]
25. Cui, C.; Mao, H.; Niu, X.; Zhang, L.X.; Hayat, T.; Alsaedi, A. A novel hashing algorithm for Depth-image-based-rendering 3D images. *Neurocomputing* **2016**, *191*, 1–11. [CrossRef]
26. Yang, H.; Yin, J.; Jiang, M. Perceptual Image Hashing Using Latent Low-Rank Representation and Uniform LBP. *Appl. Sci.* **2018**, *8*, 317. [CrossRef]
27. Ding, K.M.; Zhu, C.Q.; Lu, F.Q. An adaptive grid partition based perceptual hash algorithm for remote sensing image authentication. *Wuhan Daxue Xuebao* **2015**, *40*, 716–720.
28. Ding, K.M.; Zhu, C.Q. Perceptual hash algorithm for integrity authentication of remote sensing image. *J. Southeast Univ.* **2014**, *44*, 723–727.
29. Ding, K.M.; Chen, S.P.; Meng, F. A Novel Perceptual Hash Algorithm for Multispectral Image Authentication. *Algorithms* **2018**, *11*, 6. [CrossRef]
30. Cihan, T.; Cuneyt, A. Edge Drawing: A combined real-time edge and segment detector. *J. Vis. Commun. Image R.* **2012**, *23*, 862–872.
31. Bruzzone, L.; Carlin, L. A Multilevel Context-Based System for Classification of Very High Spatial Resolution Images. *IEEE Trans. Geosci. Remote Sens.* **2006**, *44*, 2587–2600. [CrossRef]
32. Lopez-Molina, C.; Baets, B.D.; Bustince, H.; Sanz, J.; Barrenechea, E. Multiscale edge detection based on Gaussian smoothing and edge tracking. *Knowl. Based Syst.* **2013**, *44*, 101–111. [CrossRef]
33. Witkin, A.P. Scale-space Filtering. *Read. Comput. Vis.* **1987**, *42*, 329–332.
34. Coleman, S.A.; Scotney, B.W.; Suganthan, S. Multi-scale edge detection on range and intensity images. *Pattern Recognit.* **2011**, *44*, 821–838. [CrossRef]
35. Shih, M.Y.; Tseng, D.C. A wavelet-based multiresolution edge detection and tracking. *Image Vis. Comput.* **2005**, *23*, 441–451. [CrossRef]
36. Xiang, Y.; Wang, F.; Wan, L.; You, H. An Advanced Multiscale Edge Detector Based on Gabor Filters for SAR Imagery. *IEEE Geosci. Remote Sens. Lett.* **2017**, *14*, 1522–1526. [CrossRef]
37. Antunes, S.; Esposito, A.; Palmisano, A.; Colantoni, C.; Cerutti, S.; Rizzo, G. Cardiac Multi-detector CT Segmentation Based on Multiscale Directional Edge Detector and 3D Level Set. *Ann. Biomed. Eng.* **2016**, *44*, 1487–1501. [CrossRef] [PubMed]

38. Jin, G.; Wan, X. An improved method for SIFT-based copy–move forgery detection using non-maximum value suppression and optimized J-Linkage. *Signal Process. Image Commun.* **2017**, *57*, 113–125. [CrossRef]
39. Chen, Z.; Jiang, J.; Jiang, X.; Fang, X.; Cai, Z. Spectral-Spatial Feature Extraction of Hyperspectral Images Based on Propagation Filter. *Sensors* **2018**, *18*, 6. [CrossRef] [PubMed]
40. Xu, C.; Gao, S.; Li, M. A novel PCA-based microstructure descriptor for heterogeneous material design. *Comput. Mater. Sci.* **2017**, *130*, 39–49. [CrossRef]
41. Báscones, D.; González, C.; Mozos, D. Hyperspectral Image Compression Using Vector Quantization, PCA and JPEG2000. *Remote Sens.* **2018**, *10*, 6. [CrossRef]