entropy

MDPI

Article

Medical Image Authentication Method Based on the Wavelet Packet and Energy Entropy

Tiankai Sun [1,2], Xingyuan Wang [1,3,*], Kejun Zhang [2], Daihong Jiang [2], Da Lin [2], Xunguang Jv [2], Bin Ding [2] and Weidong Zhu [2]

[1] Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China; strongtiankai@163.com
[2] School of Information and Electrical Engineering, Xuzhou University of Technology, Xuzhou 221008, China; kej_zhang@163.com (K.Z.); daihong69@163.com (D.J.); lin_da76@163.com (D.L.); xg_jv66@163.com (X.J.); dingbin80@163.com (B.D.); wd_zhu69@163.com (W.Z.)
[3] School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China
* Correspondence: wangxy@dlut.edu.cn

Abstract: The transmission of digital medical information is affected by data compression, noise, scaling, labeling, and other factors. At the same time, medical data may be illegally copied and maliciously tampered with without authorization. Therefore, the copyright protection and integrity authentication of medical information are worthy of attention. In this paper, based on the wavelet packet and energy entropy, a new method of medical image authentication is designed. The proposed method uses the sliding window to measure the energy of the detail information. In the time–frequency data distribution, the local details of the data are mined. The complexity of energy is quantitatively described to highlight the valuable information. Based on the energy weight, the local energy entropy is constructed and normalized. The adjusted entropy value is used as the feature vector of the authentication information. A series of experiments show that the authentication method has good robustness against shearing attacks, median filtering, contrast enhancement, brightness enhancement, salt-and-pepper noise, Gaussian noise, multiplicative noise, image rotation, scaling attacks, sharpening, JPEG compression, and other attacks.

Keywords: wavelet packet decomposition; energy entropy; authentication; robustness

Citation: Sun, T.; Wang, X.; Zhang, K.; Jiang, D.; Lin, D.; Jv, X.; Ding, B.; Zhu, W. Medical Image Authentication Method Based on the Wavelet Packet and Energy Entropy. *Entropy* **2022**, *24*, 798. https://doi.org/10.3390/e24060798

Academic Editor: Amelia Carolina Sparavigna

Received: 27 April 2022
Accepted: 6 June 2022
Published: 8 June 2022

1. Introduction

With the widespread application of digital diagnosis technology, hospitals are producing a large amount of digital medical information every day. The digital medical information includes all kinds of medical images, electronic medical records (EPRs), electronic health records (EHRs), and diagnosis data. The rapid development of image analysis, signal processing, and 5G network technology have provided technical support for telemedicine, telemedicine consultation, and telemedicine teaching. Relying on efficient information processing methods, medical experts in different places can discuss diseases in real time. The application of new technology has further improved the diagnosis and treatment effect for patients.

In the public network environment, the dissemination of digital medical information not only provides convenience for patients but also brings new security risks. When increasing amounts of medical data are transmitted to medical centers, the confusion of the medical data of different patients may cause medical negligence. Therefore, the medical data of different patients require extra care in the storage and distribution processes. At the same time, during the process of network transmission, any minor changes in medical information may create new medical disputes. Therefore, the security authentication of medical information is particularly important. In recent years, experts and scholars have studied a variety of medical image authentication schemes [1,2]. Some researchers

have focused their efforts on detecting whether the medical images have been tampered. Others focused their efforts on identifying the tampered areas and repairing the tampered areas [3,4]. However, from the perspective of practical application, the authentication process of medical images should focus on whether the medical images have been tampered. The process should also focus on whether the authentication process impacts the medical diagnosis. In order to avoid distortion, some researchers divided the medical images into blocks; that is, the images were divided into regions of interest (ROIs) and regions of noninterest (RONIs). Different authentication methods are used for the ROI region and the RONI region. This kind of method is simple to implement, easy to operate, and easy to recover. The disadvantage of this scheme is that the method has poor fault tolerance and is easy for attackers to recover [1,5,6]. Some scholars have integrated different kinds of transformation domain operations such as DWT, DCT, DFT, quantization index modulation under dither modulation (QIM-DM), SVD, neural networks, and cryptography to authenticate medical images [7–9]. Several classical authentication schemes integrate various transform domain operations. For example, Anand integrated ECC encryption and digital watermarking technology to protect the security of medical information [3]. Singh used Hamming error correction code, a digital watermark, and cryptography to improve the security of authentication methods and reduce the bandwidth redundancy [8]. Thakur designed a double watermark model suitable for medical image security authentication by comprehensively using DWT, SVD, Hamming code, and chaotic encryption [9]. Jinhua designed a quantization-based image watermarking scheme by using the information entropy of the wavelet domain [10]. Hu et al. used a key to control the logistic chaotic map, and searched for the same binary sequence as the watermark information to realize authentication [11]. Based on DWT and visual cryptography, Hsieh and Huang proposed an authentication scheme, which is characterized by the mean and variance of the wavelet coefficients [12]. Aiming at the security protection of telemedicine applications, scholars such as Borra, Pirbhulal, and Farhan fully integrated FRT-SVD and cryptographic methods to realize the authentication of medical information [13–16]. Scholars such as Hsu and Hou have studied some security authentication methods by integrating cryptography and zero watermark. The implementation of such methods requires the integration of special transformation operations [17–20]. Compared with the spatial domain methods, the transformation domain methods have strong reversibility, high security, good visual quality, and resist attack. The disadvantages are that the calculation is complex and the implementation of the algorithm needs a specially designed scheme.

The effectiveness of all of the authentication schemes has been confirmed, and the different authentication methods each have their own advantages and disadvantages. Under the application background, the authentication model should ensure the uniqueness of data sources. The authentication model should also ensure the one-to-one correspondence between the data information and the relevant patients. A good authentication model should have good invisibility and robustness. Invisibility means that the authentication process cannot affect the quality of medical information. At the same time, the authentication process should not cause new medical disputes. Robustness means that the authentication model is still available under various geometric attacks and noise attacks. On the basis of previous work, we discussed the problem from the perspective of energy entropy. By using energy entropy, a suitable method for medical image authentication was designed. The innovations of this method are as follows:

(1) In the time–frequency data distribution, the energy of the detailed information is described. Then, the complexity weight of the energy is measured. Based on this, the local energy entropy is constructed.
(2) From the perspective of energy, the local details of the data are mined and then the local energy entropy is normalized. The processed entropy is used as the feature of the authentication information.

(3) The proposed authentication method combines the advantages of multiresolution analysis and the stability of local energy entropy. No noise is added in the authentication process. The integrity goal of the authentication is achieved.

A series of attack experiments verified that the proposed method is robust in image compression, channel noise, as well as against intentional and unintentional attacks.

2. Basic Theory

2.1. Basic Theory of Wavelet Packet Transform

The wavelet packet transform is an extension of the wavelet transform, and its theory and algorithm are based on the wavelet transform [21–23]. The wavelet transform adopts a tower-type signal decomposition mode; that is, the signal is continuously decomposed on the low-frequency channel. The wavelet transform only extracts the low-frequency components and ignores the middle- and high-frequency features that may reflect the important information in the signal. The wavelet packet transform can gather in all frequency ranges, which not only retains the multiresolution characteristics but also makes full use of the rich detail information.

In orthogonal wavelet decomposition, through multiresolution analysis, only the subspace V_j is decomposed into mutually orthogonal subspaces V_{j+1} and W_{j+1}, namely:

$$V_j = V_{j+1} \oplus W_{j+1} \tag{1}$$

Different from the wavelet transform, the wavelet packet transform also further decomposes W_j at any decomposition level. Assuming that the decomposition starts from V_0, let $W_0^0 = V_0$, $\psi_0^0(t) = \phi(t)$, where $\phi(t)$ is the scaling function, then $\{\psi_0^0(t-k)\}_{k\in Z}$ is the orthonormal basis of W_0^0. First, W_0^0 is decomposed into W_1^0 and W_1^1, and there are $W_1^0 \perp W_1^1$ and $W_0^0 = W_1^0 \oplus W_1^1$. The subspace W_j^n is decomposed into W_{j+1}^{2n} and W_{j+1}^{2n+1}, and there are $W_{j+1}^{2n} \perp W_{j+1}^{2n+1}$ and $W_j^n = W_{j+1}^{2n} \oplus W_{j+1}^{2n+1}$.Then, the orthonormal bases of subspaces W_j^n, W_{j+1}^{2n}, and W_{j+1}^{2n+1} are $\left\{\psi_j^n(t-2^j k)\right\}_{k\in Z}$, $\left\{\psi_{j+1}^{2n}(t-2^{j+1}k)\right\}_{k\in Z}$, and $\left\{\psi_{j+1}^{2n+1}(t-2^{j+1}k)\right\}_{k\in Z}$, respectively, and they satisfy the following two-scale equations:

$$\begin{cases} \psi_{j+1}^{2n}(t) = \sum\limits_{k\in z} h_k \psi_j^n(t-2^j k) \\ \psi_{j+1}^{2n+1}(t) = \sum\limits_{k\in z} g_k \psi_j^n(t-2^j k) \end{cases} \tag{2}$$

where h_k and g_k are a pair of conjugate mirror filters, and $g_k = (-1)^k h_{1-k}$.

Let $f(t) \in V_0$; according to the decomposition relationship of V_0, for any specified layer j, $V_0 = W_j^0 \oplus W_j^1 \oplus \cdots \oplus W_j^{2^j-1}$.

Using the known filter $\{h_k, g_k\}$ and the projection coefficient $d_{j,k}^n$ of f in subspace W_j^n at scale j, the projection coefficients $d_{j+1,k}^{2n}$, $d_{j+1,k}^{2n+1}$ of f in subspaces W_{j+1}^{2n} and W_{j+1}^{2n+1} at scale $j+1$ are calculated.

The decomposition and reconstruction algorithm of the wavelet packet are as follows:

Equation (3) gives the decomposition algorithm of the wavelet packet:

$$\begin{cases} d_{j+1,k}^{2n} = \sum\limits_l h_{l-2k} d_{j,l}^n \\ d_{j+1,k}^{2n+1} = \sum\limits_l g_{l-2k} d_{j,l}^n \end{cases}, k \in Z \tag{3}$$

Equation (4) gives the reconstruction algorithm of the wavelet packet:

$$d_{j,k}^n = \sum_m (h_{k-2m} d_{j+1,m}^{2n} + g_{k-2m} d_{j+1,m}^{2n+1}), k \in Z \tag{4}$$

2.2. Wavelet Packet Decomposition of Images

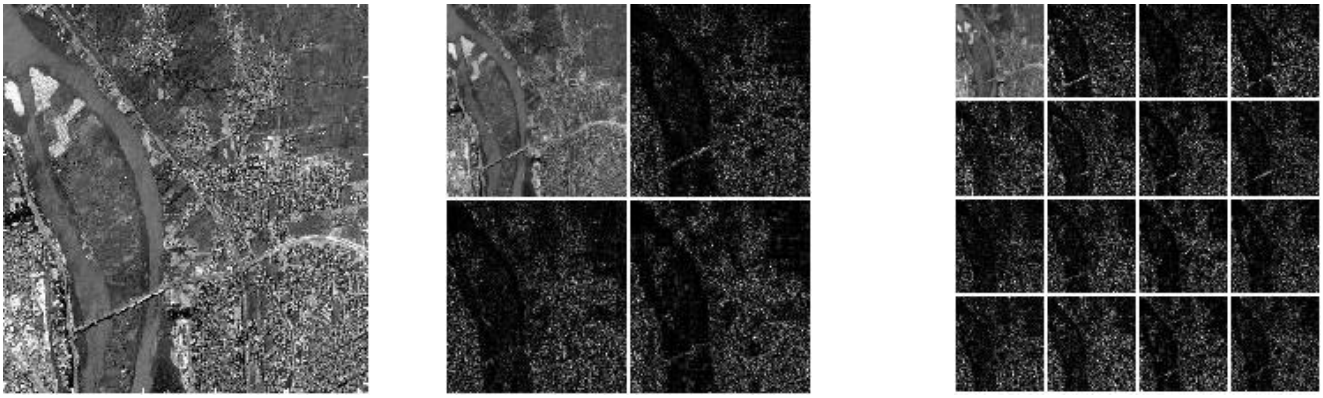
The wavelet decomposition of the image can be transformed into the wavelet decomposition of the one-dimensional signal (row and column). For the two-dimensional image f of $M \times N$, the following steps can be used for wavelet packet decomposition:

(1) Wavelet transform is performed on image f, then four subimages $f \otimes (H_r, H_c)$, $f \otimes (H_r, G_c)$, $f \otimes (G_r, H_c)$, and $f \otimes (G_r, G_c)$ are obtained.

Among them, $f \otimes (H_r, H_c)$ is a low-frequency image. $f \otimes (H_r, G_c)$, $f \otimes (G_r, H_c)$, and $f \otimes (G_r, G_c)$ are the vertical, horizontal, and diagonal subimages, respectively, which are high-frequency images.

(2) Continue the operation in step (1) for the four subgraphs and then obtain the four subgraphs of each subimage. The cycle is carried out until n-level wavelet packet decomposition subgraphs are obtained.

Figure 1 shows the subgraphs of the image decomposed by the first- and second-level wavelet packets.



(**a**) The original image. (**b**) The first-level decomposition. (**c**) The second-level decomposition.

Figure 1. An example of two-level wavelet packet decomposition. (**a**) represents the original image, (**b**) represents the 4 subimages of the first-level wavelet packet decomposition, and (**c**) represents the 16 subimages of the second-level wavelet packet decomposition.

2.3. Theory of Energy Entropy

Information entropy is a concept used to measure the amount of information in information theory [10]. It was proposed by Shannon in 1948 and is defined as follows:

Suppose that the information source X is a discrete random variable and the value of X is $X = \{x_1, x_2, \cdots, x_n\}$. If the probability of the occurrence of each message is $P = \{p_1, p_2, \cdots, p_n\}$ and $\sum_{i=1}^{n} p_i = 1$, then the information entropy of X can be expressed as Formula (5):

$$H(X) = -\sum_{i=1}^{n} p_i \log p_i \tag{5}$$

Suppose that a two-dimensional image f is decomposed by wavelet packet. The energy corresponding to the ith sub-image $f_{i,j}$ of the jth layer is denoted as $E_{i,j}$, then

$$E_{i,j} = \sum_{k=1}^{M'} \sum_{l=1}^{N'} \left| f_{i,j}(k,l) \right|^2, \; i = 0, 1, \cdots, 4^j - 1 \tag{6}$$

where M' and N' are the size of the subimage $f_{i,j}$, and $f_{i,j}(k,l)$ represents the gray value of the subimage $f_{i,j}(k,l)$ at (k,l). Then, the total energy of the jth layer is $E_j = \sum_{i=0}^{4^j-1} E_{i,j}$.

Let $P_{i,j} = \frac{E_{i,j}}{E_j} = \frac{E_{i,j}}{\sum_{i=0}^{4^j-1} E_{i,j}}$, then $\sum_{i=0}^{4^j-1} P_{i,j} = 1$. According to information entropy theory, the energy entropy of the ith subimage $f_{i,j}$ is defined as follows:

$$E_{WPEE} = -\sum_{i=0}^{4^j-1} P_{i,j} \log P_{i,j} \tag{7}$$

3. Authentication Scheme

3.1. Ownership Construction Phase

Multiresolution decomposition of medical images is carried out by the wavelet packet transform. In a time–frequency data distribution, a sliding window is used to measure the energy of the detailed information. Based on the energy weight, the local energy entropy is constructed. From the perspective of energy entropy, the local details of the data are mined. The local energy entropy is normalized and stored in a third-party certification center as authentication information. Figure 2 shows a schematic diagram of the copyright construction process. The detailed implementation process is shown below.

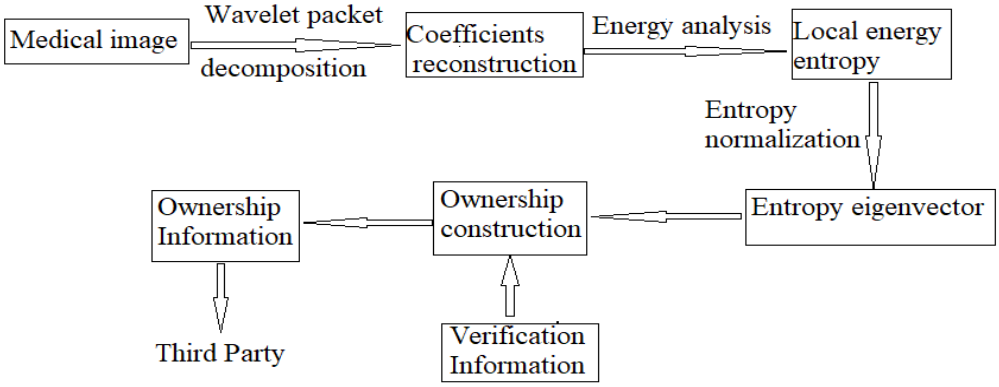


Figure 2. Flow chart of the copyright construction.

Step 1: Extraction of robust features.

When the robust areas of carrier information are fully used, the authentication method can better resist various attacks. The medical image R is multiscale-decomposed by the wavelet packet. After this operation, the low-frequency approximate wavelet coefficient f_{11} can be obtained. The low-frequency data f_{11} are decomposed into nonoverlapping blocks. The energy entropy of the segmented data can be calculated by Formulas (6) and (7) in Section 2.3.

$$[f_{11}, f_{12}, f_{21}, f_{22}] = \mathrm{DWT(R)}.$$

Step 2: Construct feature vector.

According to the energy entropy of each data block, the average energy entropy of the segmented data can be calculated. By using Equation (8), the relationship between the energy entropy of each segmented data and the mean energy entropy can be analyzed, and then the binary feature vector can be constructed.

$$F = \begin{cases} 0, \ if \ En_i >= En \\ 1, \ \text{else} \end{cases} \tag{8}$$

where $i = 1, 2, \cdots, n \times n$, En_i is the energy entropy of each block, and En is the mean energy entropy of all information blocks. The feature vector F is the original feature information extracted from the medical images by using wavelet packet energy entropy as the analysis tool.

Step 3: Form authentication information and store authentication results.

Perform the *XOR* operation between the copyright authentication information *IM* and the extracted feature vector *F*. The results are stored in a third-party center for authentication.

$$DW = XOR(IM, F) \tag{9}$$

where *IM* is the copyright logo data.

3.2. Ownership Verification Phase

Assuming that R' is the image to be authenticated after a series of attacks, Figure 3 shows the schematic diagram of the authentication process. The detailed authentication process is shown below.

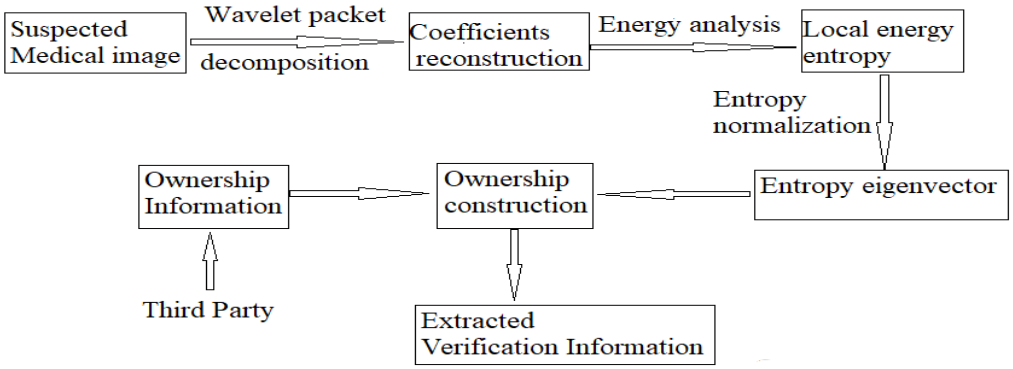


Figure 3. Flow chart of the ownership verification.

Step1: Extraction of robust features.

The suspected medical image R' is multiscale-decomposed by the wavelet packet. The low-frequency approximate wavelet coefficient $f_{11}{}'$ can be obtained. Then, the low-frequency data $f_{11}{}'$ are decomposed into nonoverlapping blocks. The energy entropy of the segmented data can be calculated by the Formulas (6) and (7) in Section 2.3.

$$[f_{11}{}', f_{12}{}', f_{21}{}', f_{22}{}'] = DWT(R').$$

Step 2: Construct feature vector.

According to the energy entropy of each data block, the average energy entropy of the segmented data is calculated. By using Equation (10), the relationship between the energy entropy of each segmented data and the mean energy entropy is analyzed. The binary feature vector F' can be constructed.

$$F' = \begin{cases} 0, \ if \ E'n_i >= E'n \\ 1, \ \text{else} \end{cases}, \tag{10}$$

where $i = 1, 2, \cdots, n \times n$, $E'n_i$ is the energy entropy of each block, and $E'n$ is the mean energy entropy of all the information blocks. The feature vector F' is the feature information extracted from the suspected images.

Step3: Complete verification.

Perform the XOR operation between the feature information F' and *DW*, which is stored in a third-party authentication center. The results are stored in matrix IM' and IM' is the recovered authentication information. The authentication is completed by judging the difference between *IM* and IM'.

$$IM' = XOR(DW, F') \tag{11}$$

where *IM* is the original logo data, and IM' is the recovered logo data.

4. Analysis of Experimental Results

In order to verify the feasibility of this method, six different types of medical images were selected as the test images from the medical image platform at https://peir.path.uab.edu/library/We, accessed the platform, (accessed on 10 August 2021). The six images were from different parts of the human body, which better verified the robustness of the proposed method. Figure 4 gives the test images and a 32×32 logo image. The proposed method was tested in the six images. Due to the space limitations, we provide the test results on breast images and presents the averaged results for all six test images.

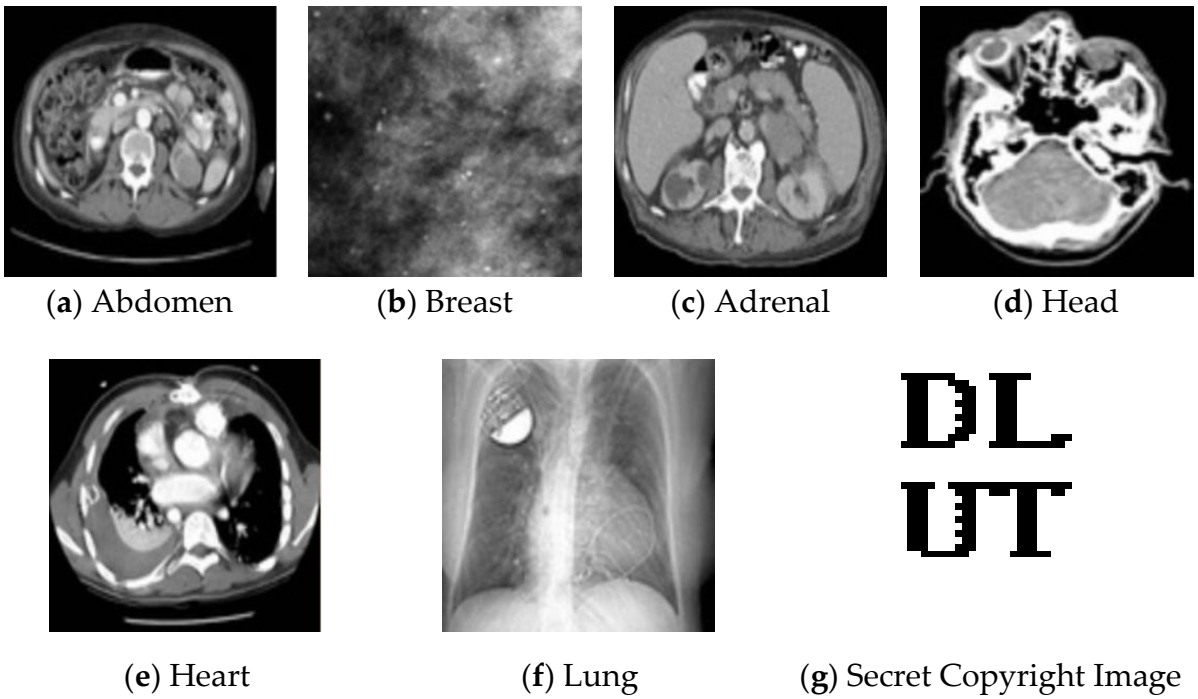


Figure 4. The test images and copyright logo.

The peak signal-to-noise ratio (*PSNR*) of the original image and the attacked image is used to quantitatively describe the impact of various attacks on the original carrier information. The greater the *PSNR* value, the higher the similarity of the two images. When the *PSNR* value is less than 30 dB, the human eye can perceive the difference between the original image and the attacked image. The evaluation index is more consistent with the visual perception characteristics of the human eyes. The robustness of the authentication method is evaluated by the normalized similarity value (*NC*). The *NC* value is between zero and one. The larger the *NC* value, the higher the similarity between them. The robustness of the authentication method can be verified when the *PSNR* is very low and the *NC* value is very high.

$$\begin{aligned} PSNR &= 10 \log_{10} \frac{255^2}{MSE}(dB), \\ MSE &= \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (H_{ij} - H'_{ij})^2, \end{aligned} \tag{12}$$

where M and N are the width and height of the tested image; H_{ij}, H'_{ij} are the pixel value of the carrier image before and after the attack, respectively.

$$NC = 1 - \frac{\sum_{b=1}^{B} w_b \oplus w'_b}{B} \tag{13}$$

where w_b, w'_b are the original authentication information and the extracted copyright information, respectively; B is the size of the copyright information.

4.1. Correlation Test between Different Features

The features used for authentication should have strong autocorrelation with the carrier. The authentication features extracted from different images should have strong independence. The authentication features extracted from different images should be independent of each other. In order to verify the autocorrelation between the features, Table 1 is used to show the correlation values of the different features. The correlation between different features is evaluated by the normalized similarity value (*NC*). The *NC* value is between zero and one. The larger the *NC* value, the higher the similarity between them. It can be seen from Table 1 that most of the data are close to 0.7 and some are close to 0.3. The results indicate that the features extracted from different images were different.

Table 1. Similarity test of different features.

	Abdomen (b) Breast (c) Chest (d) Head	**Breast**	**Adrenal**	**Head**	**Heart**	**Lung**
Abdomen	1	0.2793	0.7334	0.7490	0.6777	0.7188
Breast	0.2793	1	0.1533	0.2412	0.2891	0.0156
Adrenal	0.7334	0.1533	1	0.7578	0.7471	0.8467
Head	0.7490	0.2412	0.7578	1	0.6748	0.7432
Heart	0.6777	0.2891	0.7471	0.6748	1	0.7246
Lung	0.7188	0.0156	0.8467	0.7432	0.7246	1

4.2. Analysis of Experimental Results

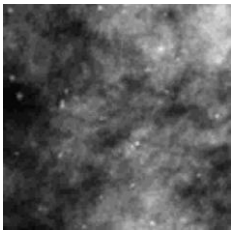
Due to the interference of network noise and human factors, medical information may change in the process of network transmission. In order to intuitively verify the effectiveness of the proposed method, we use Figures 5–15, which show the robustness results of a breast after a series of simulated attacks. The simulated attack types were image rotation (rotation 10 degrees), scaling attack (zoom to 200%), sharpening attack, JPEG compression attack (compression factor 10%), salt and pepper noise attack (parameter 0.001), Gaussian noise attack (Gaussian parameter 0.005), multiplicative noise attack (noise parameter 0.01), contrast enhancement attack, brightness enhancement attack, clipping attack (cutting out 1/5 of the original image), and median filtering attack (filtering parameter 5×5).

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

Figure 5. (**a**) JPEG compression attack PSNR = 34.4752; (**b**) recovered logo image from (**a**) (NC = 1).

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

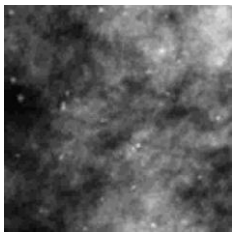
Figure 6. (**a**) Salt and pepper noise attack PSNR = 35.1107; (**b**) recovered logo image from (**a**) (NC = 0.9980).



(**a**)

(**b**)

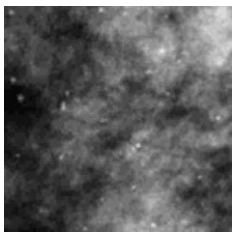
Figure 7. (**a**) Gaussian noise attack PSNR = 22.4612; (**b**) recovered logo image from (**a**) (NC = 0.9824).



(**a**)

(**b**)

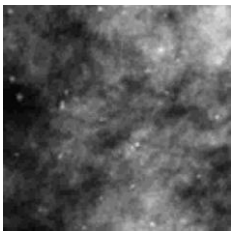
Figure 8. (**a**) Rotation attack PSNR = 34.7317; (**b**) recovered logo image from (**a**) (NC = 1).



(**a**)

(**b**)

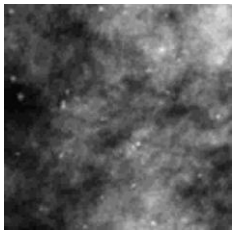
Figure 9. (**a**) Scaling attack PSNR = 56.0139; (**b**) recovered logo image from (**a**) (NC = 1).



(**a**)

(**b**)

Figure 10. (**a**) Sharpening attack PSNR = 30.6776; (**b**) recovered logo image from (**a**) (NC = 0.9990).



(**a**)

(**b**)

Figure 11. (**a**) Multiplicative noise attack PSNR = 28.4653; (**b**) recovered logo image from (**a**) (NC = 1).

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

Figure 12. (**a**) Clipping attack PSNR = 15.7723; (**b**) recovered logo image from (**a**) (NC = 0.9688).

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

Figure 13. (**a**) Median filtering attack PSNR = 43.9290; (**b**) recovered logo image from (**a**) (NC= 0.9990).

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

Figure 14. (**a**) Contrast enhancement attack PSNR = 21.5881; (**b**) recovered logo image from (**a**) (NC = 0.9766).

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

Figure 15. (**a**) Brightness enhancement attack PSNR = 28.2620; (**b**) recovered logo image from (**a**) (NC = 1).

Figures 5–15 show the robustness of the breast image after a series of simulated attacks. Table 2 presents the averaged results of the six test images.

Table 2. Averaged results of six test images.

Attack	Breast	Averaged Results of Six Test Images
JPEG (10)	1	0.9952
Salt-and-pepper noise (0.001)	0.9980	0.9749
Gaussian noise (0.005)	0.9824	0.9819
Rotation (10 degrees)	1.0000	0.9968
Scale scaling (200%)	1	0.9924
Sharpening	0.9990	0.9938
Multiplicative noise (0.01)	1	0.9918
Clipping (20%)	0.9688	0.9637
Median filtering 5×5	0.9990	0.9970
Contrast enhancement	0.9766	0.9852
Brightness enhancement	1	0.9853

Medical information is different from traditional data information. Even slight changes in medical information may cause medical disputes. From Figures 5–15, it can be seen that the proposed method has good robustness against conventional attacks, especially against JPEG compression (compression factor 10%), rotation attack (rotation 10 degrees), scaling attack (zoom in 200%), multiplicative noise (noise parameter 0.01), brightness enhancement, etc. The *NC* value of the authentication image was one. The *NC* values of the other attack tests were also close to one. Especially for the clipping attack, the visual change was obvious after the attack (*PSNR* = 15.7723 after the attack). The *NC* value of the authentication information extracted from the attacked image was still close to one (*NC* = 0.9688). After Gaussian noise, contrast enhancement, and brightness enhancement attacks, the visual change in the original medical image was also obvious (*PSNR* value was less than 30). The *NC* value of the authentication information extracted from the attacked image was also close to one. It can be seen that the proposed method has good robustness against both conventional geometric and nongeometric attacks.

4.3. Algorithm Comparison Test

Figures 5–15 and Table 2 verify the effectiveness of the method from both visual effects and numerical calculations. To further verify the robustness of the proposed method, Tables 3–5 and Figures 16 and 17 show the comparison results between this method and other authentication methods.

Table 3. Comparison tests (1).

Attacks	Hsieh and Huang's Scheme [12]	Hsu and Hou's Scheme [17]	Tiankai's Scheme [20]	Proposed Scheme
Sharpening	0.752	0.819	0.9561	0.9990
Median filtering	0.843	0.938	0.9775	0.9990
Resizing	0.733	0.887	0.9521	1
Noise addition	0.723	0.761	0.9854	0.9941
JPEG	0.845	0.956	0.9912	0.9990

Table 4. Comparison tests (2).

Attack	Ref. [11]	Ref. [18]	Ref. [19]	Ref. [20]	Proposed Scheme
Gaussian noise	0.9300	0.8594	0.9600	0.9854	0.9941
Median filtering 5×5	0.9900	0.9453	0.9800	0.9912	0.9990
Median filtering 7×7	0.9700	0.9063	0.9800	0.9775	0.9990
JPEG (70)	0.9700	1.0000	1.0000	0.9951	1

Table 4. *Cont.*

Attack	Ref. [11]	Ref. [18]	Ref. [19]	Ref. [20]	Proposed Scheme
JPEG (50)	0.9600	-	0.9900	0.9912	0.9990
JPEG (20)	0.9400	0.9570	0.9700	0.9824	1
Cropping (10%)	0.9900	-	-	0.9756	0.9463
Cropping (20%)	0.9700	-	-	0.9463	0.9688
Rotation attack (1 degree)	0.9300	0.8164	-	0.9102	0.9990
Rotation attack (2.5 degrees)	0.9700	-	-	0.9307	0.9746
Rotation attack (5 degrees)	0.9600	-	1.0000	0.9424	1
Rotation attack (10 degrees)	0.9500	-	0.9500	0.9580	1
Visibility	No	No	No	Yes	Yes

Table 5. Comparison test (3).

Attack	Noise Density	Ref. [3]	Ref. [8]	Ref. [9]	Proposed Scheme
Salt-and-pepper noise	0.0001	0.9995	0.9836	0.9975	1
Salt-and-pepper noise	0.0005	0.9977	0.9769	0.9630	0.9990
Salt-and-pepper noise	0.001	0.9949	0.9687	0.8761	0.9980
Gaussian noise	0.001	0.9917	0.9398	-	0.9941
Gaussian noise	0.005	0.9599	0.9315	-	0.9824
Rotation	1 degree	0.7806	0.9221	0.9308	0.9990
JPEG compression	QF = 10	0.9835	0.8952	0.8994	1
JPEG compression	QF = 50	0.9951	0.9510	0.9626	0.9990
JPEG compression	QF = 90	0.9994	0.9809	-	1
Speckle noise	0.001	0.9913	0.9800	0.9947	1
Speckle noise	0.005	0.9766	0.9014	-	1
Image scaling	2	0.9614	-	0.8242	1
Median filter	[11]	0.9760	0.9819	0.9973	1

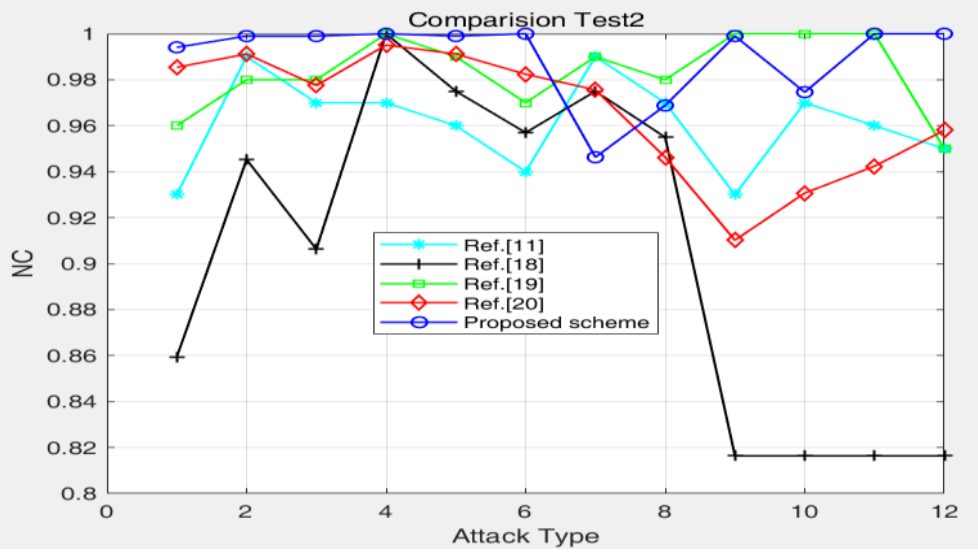


Figure 16. Comparisons of the robustness between different schemes: (1) attacks type 1–12 are Gaussian noise, median filtering 5 × 5, median filtering 7 × 7, JPEG (70%), JPEG (50%), JPEG (20%), cropping (10%), cropping (20%), rotation attack (1 degree), rotation attack (2.5 degree), rotation attack (5 degrees), and rotation attack (10 degrees), respectively.

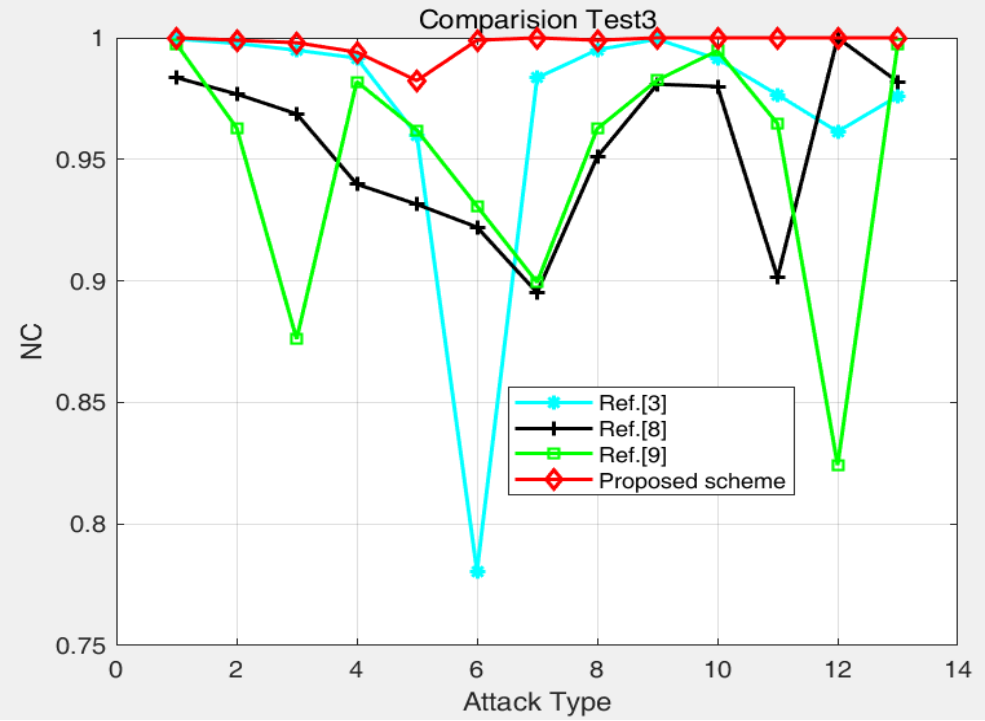


Figure 17. Comparisons of the robustness between different schemes: (2) attacks type 1–13 are salt and pepper noise (0.0001), salt and pepper noise (0.0005), salt and pepper noise (0.001), Gaussian noise (0.001), Gaussian noise (0.005), rotation (1 degree), JPEG (10%), JPEG (50%), JPEG (90%), speckle noise (0.001), speckle noise (0.005), image scaling (2×), and median filtering 1 × 1), respectively.

Table 4 and Figure 16 describe the comparison results with reference methods [11,18–20] under various attacks such as brightness, median filtering, scaling change, noise, rotation, JPEG compression, clipping, etc. The results show that the proposed method has good robustness under various attacks. From Figure 16, compared with the reference methods [11,18–20], the proposed method shows good robustness in resisting Gaussian noise, median filtering, JPEG compression, rotation attack, etc. The robustness of the proposed method against cropping attack is slightly weaker than that of the reference methods [11,18–20]. The proposed method can meet security authentication requirements.

In comparison with reference methods [3,8,9], the proposed method shows good robustness against salt-and-pepper noise, Gaussian noise, multiplicative noise, rotation attack, JPEG compression, scaling, median filtering, etc. From Table 5 and Figure 17, the *NC* value of seven attack tests is equal to 1 and the other NC values are also close to 1.

Through comparative analysis with previously reported methods [3,8,9,11,18–20], by mining and analyzing the local features of wavelet packet energy entropy, the formed authentication information shows good robustness in resisting Gaussian noise, median filtering, JPEG compression, rotation attack, and so on. Limited by the aggregation of energy, the robustness of the proposed method against cropping attack is slightly weaker.

5. Conclusions

Without adding any noise or making any change to the original medical image, based on the wavelet packet energy entropy, the complexity of the information energy was quantitatively described. From the perspective of local energy, the features of the data were fully mined, and the local energy entropy was constructed. By using the energy measurement the feature vector was formed. A series of attack tests showed that the authentication method has good rotation invariance and scale invariance. The results showed strong robustness against common geometric deformation and various kinds of

noise attacks. At the same time, this method has good universality and is especially useful for military images and medical images.

Author Contributions: Conceptualization, T.S. and X.W.; methodology, T.S.; software, T.S.; validation, K.Z. and D.J.; resources, W.Z.; data curation, B.D.; writing—original draft preparation, D.L.; writing—review and editing, X.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (no.: 61672124), the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund (no.: MMJJ20170203), Liaoning Province Science and Technology Innovation Leading Talents Program Project (no.: XLYC1802013), Key R&D Projects of Liaoning Province (no.: 2019020105-JH2/103), the Youth Foundation of Xuzhou Institute of Technology (No:XKY2017223), Xuzhou Science and Technology Plan Project (KC19197, KC17078, KC18011), Major Project of Natural Science Research of the Jiangsu Higher Education Institutions of China (18KJA520012), and Qinglan Project of Jiangsu Province under grant 2018.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: The medical images selected as the test images were taken from the medical image platform at https://peir.path.uab.edu/library/ (accessed on 10 August 2021).

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

References

1. Ashima, A.; Amitkumar, S. Watermarking techniques for medical data authentication: A survey. *Multimed. Tools Appl.* **2020**, *13*, 30165–30197.
2. Singh, A.K.; Patna, N. Data Hiding: Current Trends, Innovation and Potential challenges. *ACM Trans. Multimed. Comput. Commun. Appl.* **2020**, *16*, 1–16. [CrossRef]
3. Anand, A.; Singh, A.K. Joint Watermarking-Encryption-ECC for Patient Record Security in Wavelet Domain. *IEEE Multimed.* **2020**, *3*, 66–75. [CrossRef]
4. Singh, A.K.; Thakur, A. Joint Encryption and Compression-Based Watermarking Technique for Security of Digital Documents. *ACM Trans. Internet Technol.* **2021**, *1*, 1–20. [CrossRef]
5. Singh, A.K.; Chandan, K. Encryption-then-Compression based Copyright Protection Scheme for E-Governance. *IEEE IT Prof.* **2020**, *3*, 45–52. [CrossRef]
6. Daihong, J.; Sai, Z.; Lei, D.; Yueming, D. Multi-scale generative adversarial network for image super-resolution. *Soft Comput.* **2022**, *26*, 3631–3641. [CrossRef]
7. Solihah, G.; Shabir, A.; Parah, K. Reversible data hiding exploiting Huffman encoding with dual images for IoMT based healthcare. *Comput. Commun.* **2020**, *163*, 134–149.
8. Anand, A.; Singh, A.K. An improved DWT-SVD domain watermarking for medical information security. *Comput. Commun.* **2020**, *152*, 72–80. [CrossRef]
9. Thakur, S.; Singh, B.; Kumar, B. Improved DWT-SVD Based Medical Image Watermarking Through Hamming Code and Chaotic Encryption. *Commun. Signal Process.* **2020**, *587*, 897–905.
10. Jinhua, L.; Shan, W.; Xinye, X. A Logarithmic Quantization-Based Image Watermarking Using Information Entropy in the Wavelet Domain. *Entropy* **2018**, *945*.
11. Hu, Y.; Zhu, S. Zero-watermark algorithm based on PCA and chaotic scrambling. *J. Zhejiang Univ. Eng. Sci.* **2008**, *4*, 593–597.
12. Hsieh, S.; Huang, B. A copyright protection scheme for gray-level images based on image secret sharing and wavelet transformation. In Proceedings of the International Computer Symposium, Las Vegas, NV, USA, 16–18 June 2004; pp. 661–666.
13. Borra, S.; Thanki, R. A FRT-SVD based blind medical watermarking technique for telemedicine applications. *Int. J. Digit. Crime Forensics* **2019**, *11*, 13–33. [CrossRef]
14. Farhan, M.; Sanjeev, K. Generating Visually coherent encrypted images with reversible data hiding in wavelet domain by fusing chaos and pairing function. *Comput. Commun.* **2020**, *162*, 12–30.
15. Qin, C.; He, Z.; Yao, H. Visible watermark removal scheme based on reversible data hiding and image inpainting. *Signal Process. Image Commun.* **2018**, *60*, 160–172. [CrossRef]
16. Pirbhulal, S.; Samuel, O.W.; Wu, W. A joint resource-aware and medical data security framework for wearable healthcare systems. *Future Gener. Comput. Syst.* **2019**, *95*, 382–391. [CrossRef]
17. Hsu, C.; Hou, Y. Copyright protection scheme for digital images using visual cryptography and sampling methods. *Opt. Eng.* **2005**, *44*, 077003.
18. Gao, S. An adaptive image zero-watermarking algorithm in DT-CWT domain. *J. Sichuan Univ. Nat. Sci. Ed.* **2008**, *6*, 493–497.
19. Xiang, H.; Cao, H. A Zero-watermarking Algorithm Based on Chaotic Modulation. *J. Image Graph.* **2006**, *5*, 720–724.
20. Tiankai, S.; Xingyuan, W.; Rong, B. A Hybrid Contourlet-Singular Value Decomposition Authentication Scheme Based on Chaos and Visual Cryptography for Medical Images. *J. Comput. Theor. Nanosci.* **2016**, *13*, 8885–8895.

21. Andreas, P.; Andreas, U. Selective encryption of wavelet-packet encoded image data:efficiency and security. *Multimed. Syst.* **2003**, *9*, 279–287.
22. Arcangelo, C.; Alfredo, D.S.; Vincenzo, L.; Francesco, P. On the Protection of fMRI Images in Multi-Domain Environments. In Proceedings of the IEEE 29th International Conference on Advanced Information Networking and Applicatins, Gwangju, Korea, 24–27 March 2015; Volume 224, pp. 476–481.
23. Tiankai, S.; Xingyuan, W.; Da, L.; Daihong, J. Medical image security authentication method based on wavelet reconstruction and fractal dimension. *Int. J. Distrib. Sens. Netw.* **2021**, *4*, 1–9.