Medical image security authentication method based on wavelet reconstruction and fractal dimension

Tiankai Sun\textsuperscript{1,2}*, Xingyuan Wang\textsuperscript{1,3}, Da Lin\textsuperscript{2}, Rong Bao\textsuperscript{2}, Daihong Jiang\textsuperscript{2}, Bin Ding\textsuperscript{2} and Dan Li\textsuperscript{2}

Abstract
In this article, based on wavelet reconstruction and fractal dimension, a medical image authentication method is implemented. According to the local and global methods, the regularity of the mutation structure in the carrier information is analyzed through a measurement defined in the medical image transformation domain. To eliminate the redundancy of the reconstructed data, the fractal dimension is used to reduce the attributes of the reconstructed wavelet coefficients. According to the singularity of the fractal dimension of the block information, the key features are extracted and the fractal feature is constructed as the authentication feature of the images. The experimental results show that the authentication scheme has good robustness against attacks, such as JPEG compression, multiplicative noise, salt and pepper noise, Gaussian noise, image rotation, scaling attack, sharpening, clipping attack, median filtering, contrast enhancement, and brightness enhancement.

Keywords
Wavelet reconstruction, fractal dimension, singularity, robustness, security authentication

Date received: 21 November 2020; accepted: 12 April 2021

Handling Editor: Benny Lo

Introduction
The rapid development of 5G technology makes telemedicine and tele-consultation become a reality. The authentication of the authenticity, integrity, and validity of medical information in the process of telemedicine has become a hot issue in current research. Medical information is different from other digital information. Any small changes in digital medical information may cause medical disputes. Therefore, no noise is added during the authentication process, and only using the inherent properties and internal characteristics of digital medical information to complete copyright authentication has become a feasible scheme for medical information authentication. Aiming at the security authentication problem of the E-health application environment, many experts and scholars have proposed a series of schemes.\textsuperscript{1–5} Ashima Anand combined discrete wavelet transform (DWT) and singular value decomposition (SVD) technology and gave a feasible scheme for the security authentication of patient data by embedding multi-level watermark into medical carrier image.\textsuperscript{6} To realize the security authentication of medical information, Solihah Gull exploited the Huffman coding method to realize the reversible

\textsuperscript{1}Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian, China
\textsuperscript{2}School of Information and Electrical Engineering, Xuzhou University of Technology, Xuzhou, China
\textsuperscript{3}School of Information Science and Technology, Dalian Maritime University, Dalian, China

\textbf{Corresponding author:}
Xingyuan Wang, Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China.
Email: 495620761@qq.com; strongtiankai@163.com

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).
data hiding. Babu completed the authentication of medical images using multiple digital signatures.

On the basis of summarizing the previous work, combining multi-scale wavelet transform and fractal dimension theory, a medical image authentication method based on wavelet reconstruction and fractal dimension is proposed. The novelty along with the contributions of this article is as follows:

1. This scheme makes full use of the inherent stability of the reconstructed information in the wavelet transform domain. Based on the fractal dimension of the block information, the scheme analyzes and studies the difference of the coarse degree of the block information and the structural characteristics of the data. The stable relationship of the roughness difference is used to construct the fractal features.

2. The quantified fractal features are used as the authentication information of the medical images. The authentication method combines the scale invariance of the fractal dimension and the advantages of multi-resolution analysis of wavelet decomposition.

3. There is no noise added in the authentication process. Through all kinds of conventional attack tests, the practicability of this method is verified.

Related technique

Wavelet

As an important mathematical tool, wavelet is widely used in many aspects of digital image processing due to its frequency decomposition, multi-resolution analysis, and other characteristics. The wavelet transform adopts the systematic method of local dependence on the whole, makes full use of the signal separation function of wavelet, and performs multi-scale refinement analysis of the signal through translation and expansion. The definition of wavelet transform is given below.

Set the function $\psi(x) \in L^2(R)$, if the allowable conditions are met

$$C_\psi = \int_{-\infty}^{+\infty} \frac{\left| \mathcal{F}(\omega) \right|^2}{\omega} d\omega < +\infty$$  \hspace{1cm} (1)

where $\psi(x)$ is called a basic wavelet or a mother wavelet. Here, $\mathcal{F}(\omega) = \int_{-\infty}^{+\infty} \psi(x)e^{-j\omega x}dx$ is the Fourier transform of $\psi(x)$.

The mother wavelet function $\psi(x)$ is transformed into a wavelet sequence by scaling and translation

$$\psi_{a,b}(x) = \frac{1}{\sqrt{a}} \psi \left( \frac{x - b}{a} \right), \quad a \in R^+, b \in R$$  \hspace{1cm} (2)

here, $a$ is the stretching factor and $b$ is the translation factor.

With the change of the factors $a, b$, a set of wavelet basis functions $\{\psi_{a,b}(x)\}_{a \in R^+, b \in R}$ can be obtained.

For any function $f(x) \in L^2(R)$, based on the above wavelet basis functions, the projection decomposition of $f(x)$ can be carried out which is called continuous wavelet transform

$$WT_f(a,b) = \langle f(x), \psi_{a,b}(x) \rangle = \frac{1}{\sqrt{a}} \int_{R} f(x) \psi^* \left( \frac{x - b}{a} \right) dx$$  \hspace{1cm} (3)

here, $\psi^*$ is the conjugate function of the function $\psi$.

The factors $a$ and $b$ are discretized, respectively, $a = a_0^j, b = k_0^j b_0, j \in Z$.

The corresponding discrete wavelet function $\psi_{j,k}(x)$ is

$$\psi_{j,k}(x) = a_0^{-j/2} \psi \left( \frac{x - k b_0}{a_0} \right) = a_0^{-j/2} \psi \left( a_0^{-j} x - k b_0 \right)$$  \hspace{1cm} (4)

The discrete wavelet coefficients $C_{j,k}$ and their reconstruction formulas are

$$C_{j,k} = \langle f(x), \psi_{j,k}(x) \rangle = \int_{-\infty}^{+\infty} f(x) \psi^*(x) dx$$  \hspace{1cm} (5)

$$f(x) = C \sum_{j=-\infty}^{+\infty} \sum_{k=-\infty}^{+\infty} C_{j,k} \psi_{j,k}(x)$$  \hspace{1cm} (6)

Formula (5) is called discrete wavelet transform and $C$ is a constant independent of the signal.

Wavelet transform has good time-frequency localization, scale transformation, and directivity. Meanwhile, wavelet transform is especially suitable for analyzing digital images with rich details, poor spatial correlation, and low redundancy. In scale transformation, wavelet and fractal have a profound internal relationship.

Fractal

The concept of fractal was first introduced by Hausdorff in 1919 and then improved and developed by Mandelbrot in 1975. In fractal theory, fractal dimension can measure the singularity of signal and the ability of filling space which reflects the effectiveness of the space occupied by complex shapes. Fractal dimension is a measure of the irregularity of complex shapes and it can quantitatively describe the fractal characteristics of the structural region in a nonlinear system. Fractal dimension is a morphological characteristic parameter with constant signal scale which reflects the similarity of signals. It is an important structural feature of fractal signals. Using fractal dimension, we can quantitatively describe the...
relationship between data points and surrounding points, accurately describe the spatial characteristics of the signal, and observe the essential content of the signal from another angle. In this article, the stability of fractal dimension under different attack modes is tested. According to the working mode of E-health, the robustness of fractal dimension is deeply analyzed and studied. In this scheme, the fractal dimension is measured using the fractal Brownian random field model.10

The authentication scheme

The authentication process is presented in this section. This section included two parts, one is the ownership construction and the other is the ownership verification.

Ownership construction phase

The low-frequency detail region of medical image is obtained by discrete wavelet transform, and the low-frequency approximate data are reconstructed by coefficient. The stable feature regions are found in the reconstructed data and then the fractal dimension of each block is analyzed and calculated. Analyze and normalize the fractal dimension to construct a feature matrix which is stored in the third-party certification center as authentication information. Figure 1 shows the process of copyright construction, and the detailed authentication process is as follows.

Step 1. Discrete wavelet transform is used to decompose the original medical image in multiple scales then the low-frequency approximate wavelet coefficients are obtained.

Step 2. Reconstructing low-frequency wavelet coefficients, using structural elements to divide the data into large blocks first and then the large blocks are divided into small blocks. Each small block is used as a node to form the low-frequency reconstruction data volume.

Step 3. Analyze the reconstructed data, and attribute reduction is carried out based on 8×8 sub-blocks with more non-zero coefficients to construct the stable feature regions.

Step 4. Measure and characterize the data of the feature area by the fractal dimension, the boundary points are defined based on the self-similar characteristics of the data and the change trend of the characteristics under the influence of noise. The difference of fractal dimension between nodes is calculated. The singular values with different fractal dimensions are classified into fractal features. The fractal features are stored into matrix D. Then, the fractal features are mapped into matrix FD according to the rule that if the $D(i, j)$ is greater than or equal to 2, then $FD(i, j)$ is equal to 1; otherwise, $FD(i, j)$ is equal to 0. The matrix FD is the original feature information extracted from the original medical images.

Step 5. The exclusive or operation (XOR) is performed between the copyright authentication information and the extracted original feature information. The results are stored in the third-party certification center for authentication and recovery.

Ownership verification phase

Figure 2 gives a schematic diagram of the copyright authentication process. The detailed implementation process is as follows:

Step 1. The suspected medical image is decomposed into multiple scales by discrete wavelet transform method then the low-frequency approximate wavelet coefficients are obtained.
Step 2. Reconstructing low-frequency wavelet coefficients, using structural elements to divide the data into large blocks first and then the large blocks are divided into small blocks. Each small block is used as a node to form the low-frequency reconstruction data volume.

Step 3. Analyze the reconstructed data, and attribute reduction is carried out based on 8 × 8 sub-blocks with more non-zero coefficients to construct the stable feature regions.

Step 4. Measure and characterize the data of the feature area by the fractal dimension, the boundary points are defined based on the self-similar characteristics of the data and the change trend of the characteristics under the influence of noise. The difference of fractal dimension between nodes is calculated. The singular values with different fractal dimensions are classified into fractal features. The fractal features are stored into matrix $D_1$. Then the fractal features are mapped into matrix $FD_1$ according to the rule that if $D_1(i, j)$ is greater than or equal to 2, then $FD_1(i, j)$ is equal to 1; otherwise, $FD_1(i, j)$ is equal to 0. The matrix $FD_1$ is the original feature information extracted from the suspected medical images.

Step 5. Perform the XOR operation between the feature information extracted from the suspected image and the data stored in the third-party authentication center. The result is the recovered authentication information.

Analysis of experimental results

To compare the scheme of this article with the research work of other authors, six pairs of medical images are selected as the test objects. The size of the tested image is 512 × 512. The tested images all come from the public network platform https://peir.path.uab.edu/library/.

The scheme of this article has been tested on all six types of medical images. Due to space limitations, only the test results of Adrenal images are given. Figure 3 shows the test examples of six kinds of medical images and also shows a secret copyright image. The size of the secret copyright image is 32 × 32.

To quantitatively characterize the robustness and effectiveness of the authentication method, the peak signal-to-noise ratio (PSNR) is used to measure the similarity difference between the original image and the attack image. The greater the PSNR value, the higher the similarity between the two images. When the PSNR value is greater than 30 dB, it is difficult for human eyes to perceive the difference between the original image and the attacked image. The normalized similarity value (NC) is used to calculate the difference between the original authentication feature and the extracted copyright feature. The NC value is between 0 and 1. The larger the NC value, the higher the similarity between the two. The theoretical value of NC value is 1

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

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (H_{ij} - H'_{ij})^2$$

(7)

$M$ and $N$ are the width and height of the test image, and $H_{ij}, H'_{ij}$ are the pixel values of the carrier image before and after the attack

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

(8)

$w_b, w'_b$ are the original authentication information and the extracted copyright information. $B$ is the size of the copyright information.
Correlation test of the carrier images

However, the features extracted from the images can express and describe the essential attributes of the carrier. Meanwhile, the authentication features extracted from different images should be independent of each other and not related to each other. To verify the independence of the proposed method, the authentication features of six test images are solved, respectively, and the correlation of the feature data is calculated and analyzed. Table 1 shows the correlation test results. It can be seen from Table 1 that the correlation coefficients of the features of different test images are mostly around 0.5 which shows that there are significant differences between the features extracted for different images.

**Experimental results and analysis**

In the process of tele-medicine and tele-consultation, the transmitted medical images will be affected by a series of noises. Figures 4–14 show the robustness experiments of medical image Adrenal under the common attack modes. The attack types include image rotation (10°), scaling attack (reducing to 50%), sharpening, JPEG compression (compression factor 50%), salt and pepper noise (0.001), Gaussian noise (0.001), multiplicative noise (0.01), contrast enhancement,
brightness enhancement, clipping attack (1/5), median filtering (7 × 7), and so on.

Medical information is different from other types of carrier information. Any subtle changes in medical images may cause special attention. From the simulation tests given in Figures 4–14, it can be seen that there are a variety of simulated attack methods that have caused major changes to the medical image. As shown in Figure 11, the test image is cut by 1/5 which causes a huge visual change. Its PSNR value is 17.9704, which is much lower than 30 dB. However, the authentication result obtained from the clipping image still performs well. The NC of the authentication result extracted from Figure 11(a) is equal to 1. In other attack tests, the extracted NC values are mostly around 0.99, which further verifies the effectiveness of this method in
resisting conventional geometric attacks and non-geometric attacks.

**Algorithm comparison tests**

For different attack modes, Tables 2 and 3 show the comparison results between this method and other authentication methods. From the comparison results, it can be found that the method proposed in this article shows better robustness against common attack modes, such as noise, rotation, and cropping.

### Table 2. Comparison tests (1).

| Attacks         | Hsieh and Huang's scheme \(^{11}\) | Hsu and Hou's scheme \(^{12}\) | The Tiankai's et al. scheme \(^{13}\) | Proposed scheme |
|-----------------|--------------------------------------|---------------------------------|----------------------------------------|-----------------|
| Sharpening      | 0.752                                | 0.819                           | 0.9561                                 | 0.9834          |
| Median filtering| 0.843                                | 0.938                           | 0.9775                                 | 0.9961          |
| Resizing        | 0.733                                | 0.887                           | 0.9521                                 | 0.9971          |
| Noise addition  | 0.723                                | 0.761                           | 0.9854                                 | 0.9883          |
| JPEG            | 0.845                                | 0.956                           | 0.9912                                 | 0.9941          |

### Table 3. Comparison tests (2).

| Attacks                  | Hu and Zhu \(^{14}\) | Gao \(^{15}\) | Xiang and Cao \(^{16}\) | Tiankai et al. \(^{13}\) | Proposed scheme |
|--------------------------|----------------------|--------------|------------------------|-------------------------|------------------|
| Gaussian noise           | 0.9300               | 0.8594       | 0.9600                 | 0.9854                  | 0.9893           |
| 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                  | 0.9971           |
| JPEG (70)                | 0.9700               | 1.0000       | 1.0000                 | 0.9951                  | 0.9980           |
| JPEG (50)                | 0.9600               | –            | 0.9900                 | 0.9912                  | 0.9941           |
| JPEG (20)                | 0.9400               | 0.9570       | 0.9700                 | 0.9824                  | 0.9951           |
| Cropping (10%)           | 0.9900               | –            | –                      | 0.9756                  | I                |
| Cropping (20%)           | 0.9700               | –            | –                      | 0.9463                  | I                |
| Rotation attack (1°)     | 0.9300               | 0.8164       | –                      | 0.9102                  | 0.9932           |
| Rotation attack (2.5°)   | 0.9700               | –            | –                      | 0.9307                  | 0.9941           |
| Rotation attack (5°)     | 0.9600               | –            | –                      | 0.9424                  | 0.9980           |
| Rotation attack (10°)    | 0.9500               | –            | 0.9500                 | 0.9580                  | 0.9971           |
| Visibility               | NO                   | NO           | NO                     | YES                     | YES              |

**Figure 11.** (a) Cropping attack PSNR = 17.9704. (b) Recovered secret copyright image from (a) (NC = 1, SSIM = 0.9928).

**Figure 12.** (a) Median filtering attack PSNR = 39.0042. (b) Recovered secret copyright image from (a) (NC = 0.9961, SSIM = 0.9929).

**Conclusion**

By measuring and analyzing the fractal dimension of medical image in wavelet reconstruction domain, the security authentication scheme of medical image is realized. The scheme does not add any noise. This method fully combines the multi-scale decomposition of wavelet transform and fractal singularity recognition. The inherent regularity of the hierarchical structure of the data is fully analyzed and mined. This method not only measures the anti-noise property of carrier features but
also shows the stability of fractal features of carrier information under multi-scale and multi-resolution changes. A series of tests show that the authentication method is scale-invariant, rotation-invariant, and is robust to geometric deformation and noise of medical images. At the same time, the algorithm has good universality and can be extended to military images with higher security authentication level. The authentication method has good theoretical significance and popularization value.

Declaration of conflicting interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was supported by the National Natural Science Foundation of China (Grant no. 61672124), the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund (Grant no. MMJJ20170203), Liaoning Province Science and Technology Innovation Leading Talents Program Project (Grant no. XLYC1802013), Key R&D Projects of Liaoning Province (Grant no. 2019020105-JH2/103), the Youth Foundation of Xuzhou Institute of Technology (Grant 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.

ORCID iD
Tiankai Sun https://orcid.org/0000-0003-0417-8044

References
1. Ashima A and Amitkumar S. Watermarking techniques for medical data authentication: a survey. Multimed Tool Appl 2020; 13: 1–33.
2. Singh AK; NIT Patna. Data hiding: current trends, innovation and potential challenges. ACM Trans Multimed Comput Commun Appl 2020; 16: 1–16.
3. Anand A and Singh AK. Joint watermarking-encryption-ECC for patient record security in wavelet domain. IEEE Multimed 2020; 27: 66–75.
4. Singh AK, Thakur S, Jolfaei A, et al. Joint encryption and compression-based watermarking technique for security of digital documents. ACM Trans Intern Tech 2021; 11: 18.
5. Singh AK and Kumar C. Encryption-then-compression based copyright protection scheme for E-governance. IEEE IT Prof 2020; 22: 45–52.
6. Ashima A and AmitKumar S. An improved DWT-SVD domain watermarking for medical information security. Comput Commun 2020; 15: 272–280.
7. Solihah G, Parah SA and Muhammad K. Reversible data hiding exploiting Huffman encoding with dual images for IoMT based healthcare. Comput Commun 2020; 163: 134–149.
8. Babu S and Kapinaiah V. Medical image authentication using quartic digital signature algorithm. Int J Intel Inform Syst 2019; 7(4): 38–41.
9. Singh AK, Kumar B and Dave M. Multiple watermarking on medical images using selective discrete wavelet transform coefficients. J Med Imag Health Inform 2015; 5(3): 607–614.
10. Guan Q and Zhang W. Image edge detection based on fractal dimension. Comput Sci 2015; 42: 296–298.
11. Hsieh S and Huang B. A copyright protection scheme for gray-level images based on image secret sharing and wavelet transformation. In: Proceedings of the 3rd international conference on information technology: new generation (ITNG’06), Las Vegas, NV, vol. 4, 2006, pp.661–666. IEEE, https://ieeexplore.ieee.org/xpl/conhome/10728/proceeding
12. Hsu C and Hou Y. Copyright protection scheme for digital images using visual cryptography and sampling methods. Opt Eng 2005; 44: 077003.
13. Tiankai S, Xingyuan W and Rong B. A hybrid contourlet-singular value decomposition authentication scheme based on chaos and visual cryptography for

Figure 13. (a) Contrast enhancement attack PSNR = 32.5055. (b) Recovered secret copyright image from (a) (NC = 0.9785, SSIM = 0.9927).

Figure 14. (a) Brightness enhancement attack PSNR = 27.2279. (b) Recovered secret copyright image from (a) (NC = 0.9541, SSIM = 0.9931).
medical images. *J Comput Theoretical Nanosci* 2016; 13: 8885–8895.

14. Hu Y and Zhu S. Zero-watermark algorithm based on PCA and chaotic scrambling. *J Zhejiang Univ* 2008; 4: 593–597.

15. Gao S. An adaptive image zero-watermarking algorithm in DT-CWT domain. *J Sichuan Univ* 2008; 6: 493–497.

16. Xiang H and Cao H. A zero-watermarking algorithm based on chaotic modulation. *J Image Graph* 2006; 5: 720–724.