Hindawi
Scientific Programming
Volume 2020, Article ID 6642586, 11 pages
https://doi.org/10.1155/2020/6642586

Research Article

A Robust Authentication Algorithm for Medical Images Based on Fractal Brownian Model and Visual Cryptography

Sun Tiankai ,[1,2] Wang Xingyuan ,[1,3] Jiang Daihong,[2] Lin Da,[2] Ding Bin,[2] and Li Dan[2]

[1] *Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China*
[2] *School of Information and Electrical Engineering, Xuzhou University of Technology, Xuzhou 221008, China*
[3] *School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China*

Correspondence should be addressed to Sun Tiankai; strongtiankai@163.com and Wang Xingyuan; 495620761@qq.com

Received 14 October 2020; Revised 11 November 2020; Accepted 18 November 2020; Published 4 December 2020

Academic Editor: Wenzheng Bao

In this paper, we aimed to discuss the security authentication requirements of medical images in the medical network, and a security authentication method is designed based on fractal and visual cryptography. Based on the discrete fractal Brownian random field model, the gray-level statistical information and spatial structure information of medical images is fully mined. The gray distribution of medical images is expressed in the form of fractal features. By using the spatial data mining methods, the data of fractal structure space is analyzed, and by using the stability of the energy structure, the authentication features are formed. Using the visual cryptography (VC), the robustness of the authentication method is further enhanced. Through the centralized test of common medical images and the comparison analysis with existing methods, it is further verified that the method is effective against common attacks such as JPEG compression, scaling, rotation operation, clipping, added noise, filtering, and blurring.

1. Introduction

The rapid development of 5G technology provides a strong technical guarantee for the popularization and application of medical networking. Under the current novel coronavirus pneumonia epidemic situation, the utilization rate of telemedicine and teleconsultation is increasing day by day. While digital medical images such as CT, MRI, US, and other diagnosis and treatment information are rapidly distributed and disseminated on the medical networking platform, the authentication of the integrity, authenticity, and validity of medical information has also become a hot issue that needs to be solved urgently. The rapid development of digital watermarking technology provides a solution for the authentication of medical information. However, the traditional watermarking technology often modifies the original carrier information to some extent. Any nonmedical changes of medical information may affect the diagnosis of doctors, which may lead to medical disputes. Therefore, without any modification to the original medical information, starting from the original data, analyzing and mining the inherent stable characteristics of the carrier information, and using the stable characteristics as the basis for security certification has become a feasible solution for medical information security certification.

In recent years, many scholars at home and abroad have done a lot of research to meet the needs of medical image security authentication [1–12]. Using perceptual hashing, DTCWT-DCT, and Hénon mapping, Jing et al. proposed a multiwatermarking method for medical image authentication, which is robust against common geometric attacks [1]. Tzuo et al. used the significant difference of cellular automata coefficient to realize the lossless authentication of medical images [2]. Hu and Zhu used the key to control the logistic chaotic map and used a certain strategy to search for the similar binary sequences as the watermark information to achieve authentication [3]. Kavitha and Sakthivel implemented a medical image copyright protection scheme in hybrid domain by using the mechanism of fast response code [4]. Arsalan et al. used compression function to reduce the embedding distortion and realized the reversibility of medical image authentication [5]. Fatahbeygi and

Akhlaghian combined support vector machine and visual cryptography to propose a high-security image authentication method [6]. Elham combined entropy analysis and discrete firefly algorithm to achieve image security authentication [7]. Hsieh and Huang proposed an authentication scheme based on DWT and visual cryptography. The scheme was based on the mean value and variance of the wavelet coefficients to achieve authentication [8]. Qingtang and Beijing made full use of the distribution characteristics of the DC coefficients of DCT transform to implement a copyright authentication scheme suitable for color images in the spatial domain [9].

On the basis of previous research, combined with fractal Brownian model and visual cryptography, an authentication scheme suitable for medical image is proposed. This method maps medical image information from gray-scale space to fractal dimension space and uses the stability of fractal data to form authentication features. The initial authentication features are scrambled and confused by visual cryptography, which further enhances the robustness of the method. There is no noise added in the authentication process. A series of experiments reveal that the method is robust against common attacks, such as JPEG compression, scaling, angle rotation, clipping, noise, filtering, blurring, and so on.

2. Related Technique

2.1. Fractional Brownian Random Field Model. The concept of fractal was first introduced by Hausdorff in 1919 and then developed by Mandelbrot in 1975. The basic characteristic of fractal is scale invariance. Mandelbrot thinks that fractal has three elements: form, chance, and dimension. Fractal dimension is a basic parameter to describe fractal quantitatively. It is an important feature of geometric object scale transformation. According to different definitions and calculation methods, the commonly used fractal dimensions include Hausdorff dimension, box dimension, information dimension, and fractal Brownian random field model [10].

The gray value of the image is processed in random walk mode, and the gray value at (x, y) is marked as $I\ (x, y)$. According to the model of fractal Brownian random field, the following results are obtained:

$$E\left(\left|I\left(x_2, y_2\right) - I\left(x_1, y_1\right)\right|\right) = K\left(\sqrt{\left(x_2 - x_1\right)^2 + \left(y_2 - y_1\right)^2}\right)^H. \tag{1}$$

Let $\Delta I_{\Delta r} = \left|I\left(x_2, y_2\right) - I\left(x_1, y_1\right)\right|, \Delta r = \sqrt{\left(x_2 - x_1\right)^2 + \left(y_2 - y_1\right)^2}$.

Formula (1) can be simplified as

$$E\left(\Delta I_{\Delta r}\right) = K \cdot \Delta r^H. \tag{2}$$

By taking the logarithm of both sides of (2), the following can be obtained:

$$\ln E\left(\Delta I_{\Delta r}\right) = H \cdot \ln\left(\Delta r\right) + C, \tag{3}$$

where C is a constant.

By using least squares method, the data points $(\ln E(\Delta I_{\Delta r}), \ln(\Delta r))$ are fitted. The slope of the straight line is the Hurst exponent H of the fractal Brownian model. For two-dimensional medical images, its fractal dimension D is equal to 3 minus H.

Through research on natural images, Pentland proved that the anisotropy of gray images conformed to the discrete fractional Brownian random field model. Pentland and other scholars first introduced the concept of fractal dimension into signal processing and pointed out that the shape and texture information of objects can be obtained by fractal analysis of images. Fractal information not only reflects the change of gray amplitude but also reflects the change of gray level at different scales. In the edge region of the image, the value of fractal characteristic parameters will undergo singular change. After experimental analysis, under a series of attack modes such as translation, rotation, affine transformation, and JPEG compression, the structure ordering of the edge area has good regularity and the change of fractal dimension value is not obvious, so it has strong robustness. In this paper, we make full use of the fine-grained stable relationship in the edge area to form a stable extremum structure in the fractal dimensional structure as copyright authentication information.

2.2. Visual Cryptography. In 1994, the visual cryptography was proposed by Naor and Shamir. It is actually a secret sharing scheme (n, k) [11]. This method provides a scheme of dividing a secret image into n subimages. Without any cryptographic calculations, the original secret image can be recovered through k subimages. Even an attacker with infinite computing power cannot obtain any information about the secret image when the number of subsecrets is less than a given value (k). Figure 1 shows the structure of a (2, 2) visual cryptography. Figure 2 shows an application example of (2, 2) visual cryptography.

3. The Authentication Scheme

This section presents the authentication scheme. The scheme consists of two phases: one is the ownership construction phase and the other is the ownership verification phase.

3.1. Ownership Construction Phase. The medical image is divided into blocks. Based on the fractal Brownian random field model, the fractal dimension of the subimage is calculated one by one. The original carrier information is mapped from the gray space to the fractal dimension space. The fractal dimension features of the subimages are formed. The fractal dimension features are connected together for analysis and normalization to form the stable feature which is regarded as the key point of copyright authentication. Figure 3 shows the ownership construction phase. The details of this phase are described as follows.

(i) Step 1: Divide the medical image into blocks to form 8×8 nonoverlapping cell units.

(ii) Step 2: Analyze and calculate each cell unit by using the fractal Brownian random model. The fractal

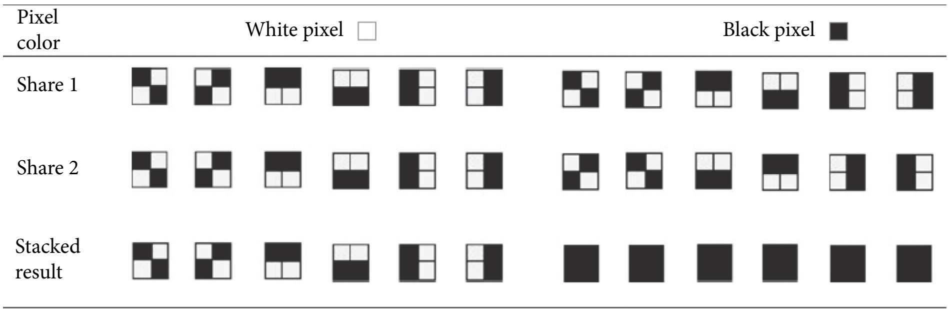


Figure 1: The structure of (2, 2) visual cryptography scheme.

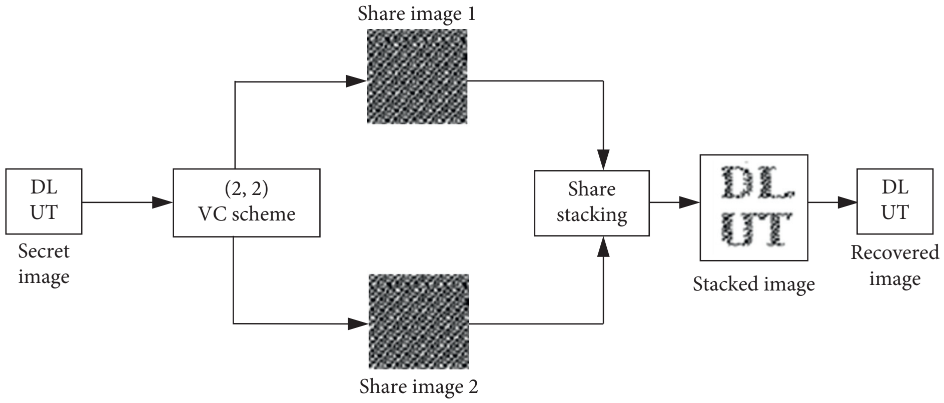


Figure 2: An application example of (2, 2) visual cryptography scheme.

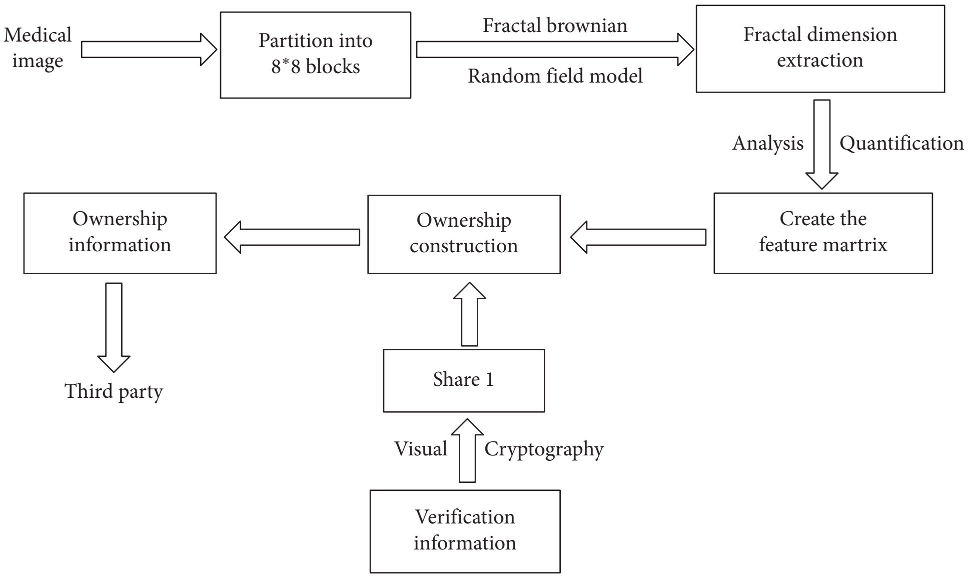


Figure 3: Ownership construction phase.

dimension value DB of each cell unit is obtained and the DB is stored in matrix D.

(iii) Step 3: Based on the matrix D, create a matrix FD with the same size as D; the initial value of FD is set to zero.

(iv) Step 4: Analyze the data of matrix D (i, j). 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 data in the matrix FD is the feature information extracted from the medical image.

(v) Step 5: Using the (2, 2) visual cryptography mechanism as shown in Figure 1 and the copyright information *im*, the sharing matrix *im_share1*, im_share2 are constructed. The master share matrix *im_share* is constructed by the following rule: *im_share* = OR (*im_share1*, *im_share2*).

(vi) Step 6: Perform the exclusive or operation on *im_share1* and FD, and the results are stored in *dw_copyright*. At the same time, *dw_copyright* and *im_share2* are stored in the third-party certification center for further authentication.

3.2. Ownership Verification Phase. Figure 4 shows the ownership verification phase. The details of this phase are described as follows.

(i) Step 1: Divide the suspected medical image into blocks to form 8 × 8 nonoverlapping cell units.

(ii) Step 2: Analyze and calculate each cell unit by using the fractal Brownian random model. The fractal dimension value DB of each cell unit is obtained, and the DB is stored in matrix D1.

(iii) Step 3: Based on the matrix D1, create a matrix FD1 with the same size as D1; the initial value of FD1 is set to zero.

(iv) Step 4: Analyze the data of matrix D1 (i, j). If the D1 (i, j) is greater than or equal to 2, then, FD1 (i, j) is equal to 1; otherwise, FD1 (i, j) is equal to 0. The data in the matrix FD1 is the feature information extracted from the suspected medical image.

(v) Step 5: Fetch *dw_copyright* from the third-party certification center. Perform the exclusive or operation on FD1 and *dw_copyright*; the results are stored in *im_share1_1*. That is to say, *im_share1_1* = (*dw_copyright*) XOR (FD1).

(vi) Step 6: Fetch *im_share2* from the third-party certification center. The shared image *im_share* is restored according to the sharing of *im_share1_1* and *im_share2* as the following rule: *im_share* = (*im_share1_1*) OR (*im_share2*).

(vii) Step 7: Divide the share image *im_share* into nonoverlapping 2 × 2 blocks. Calculate the sum of each small block (i); if the sum is less than or equal to 2, the *im1* (i) is equal to 0; otherwise, *im1* (i) is equal to 1. That is to say,

$$im1(i) = \begin{cases} 0, & \sum_{j=1}^{2}\sum_{k=1}^{2} \text{block}(i) < \ = 2, \\ 1, & \text{else}, \end{cases} \quad (4)$$

where *im1* is the recovered authentication information.

4. Experimental Results

In order to verify the robustness of the algorithm some experiments are carried out in this section. Figure 5 shows six 512 × 512 medical images named "abdomen," "heart," "lung," "breast," "adrenal," "head" and one 32 × 32 logo image. All the images have been tested using this algorithm.

In order to describe the effectiveness and robustness of the algorithm, the peak signal-to-noise ratio (PSNR) is used to measure the visual changes of the image after a series of attacks. The larger the PSNR value is, the less damage the image will have [3]. The normalized similarity (NC) value is used to measure the similarity between the extracted copyright information and original copyright information. The larger the NC value, the higher the similarity between the two. The PSNR and NC are defined by the following rules:

$$\text{PSNR} = 10\log_{10}\frac{255^2}{\text{MSE}}\ (\text{dB}),$$
$$\text{MSE} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(H_{ij} - H_{ij}'\right)^2, \quad (5)$$

where M and N are the size of the test image. H_{ij} and H_{ij}' are the original image and the attacked image.

$$\text{NC} = 1 - \frac{\sum_{b=1}^{B} w_b \oplus w_b'}{B}, \quad (6)$$

where w_b, w_b' are the original copyright information and recovered copyright information. B is the size of copyright information.

4.1. Correlation Test of the Carrier Images. The authentication information stored in the authentication center is closely related to the inherent characteristics of the carrier image, so the feature information of different carrier images should be independent of each other. The correlation data between the tested images is given in Table 1. From Table 1, it can be seen that the correlation data between different images are mostly concentrated around 0.6, which indicates that the feature information extracted from different images has significant differences.

4.2. Common Attack Test. Medical images are prone to geometric and nongeometric attacks in the process of network transmission. The robustness test is carried out after the common attacks such as JPEG compression (compression factor 50%), salt and pepper noise (0.001), Gaussian noise (0.001), image rotation (10°), scaling attack (reduced to 50%), sharpening, multiplicative noise (0.01), cropping attack (1/5), median filtering (7 × 7), contrast enhancement, and brightness enhancement. Figures 6–16 show the results obtained by performing the proposed scheme on the "abdomen" image.

From Figures 6–16, it can be seen that the algorithm shows strong robustness against both conventional geometric attacks and nongeometric attacks, and the NC value of the authentication image is mostly close to 1. For medical images, any visible changes will cause special attention. In the attack test given in Figures 6–16, there are many attacks that make the carrier image change significantly. For example, as shown in Figure 13, the carrier image is cut by 1/5 and its PSNR value is much lower than 30 dB. However, the obtained authentication image still performs well. The NC of

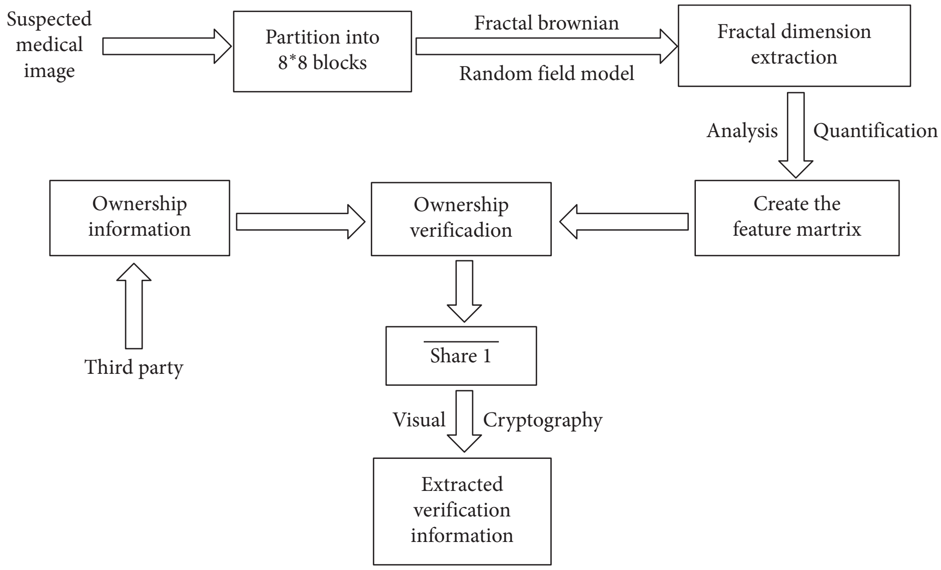


Figure 4: Ownership Verification phase flow.

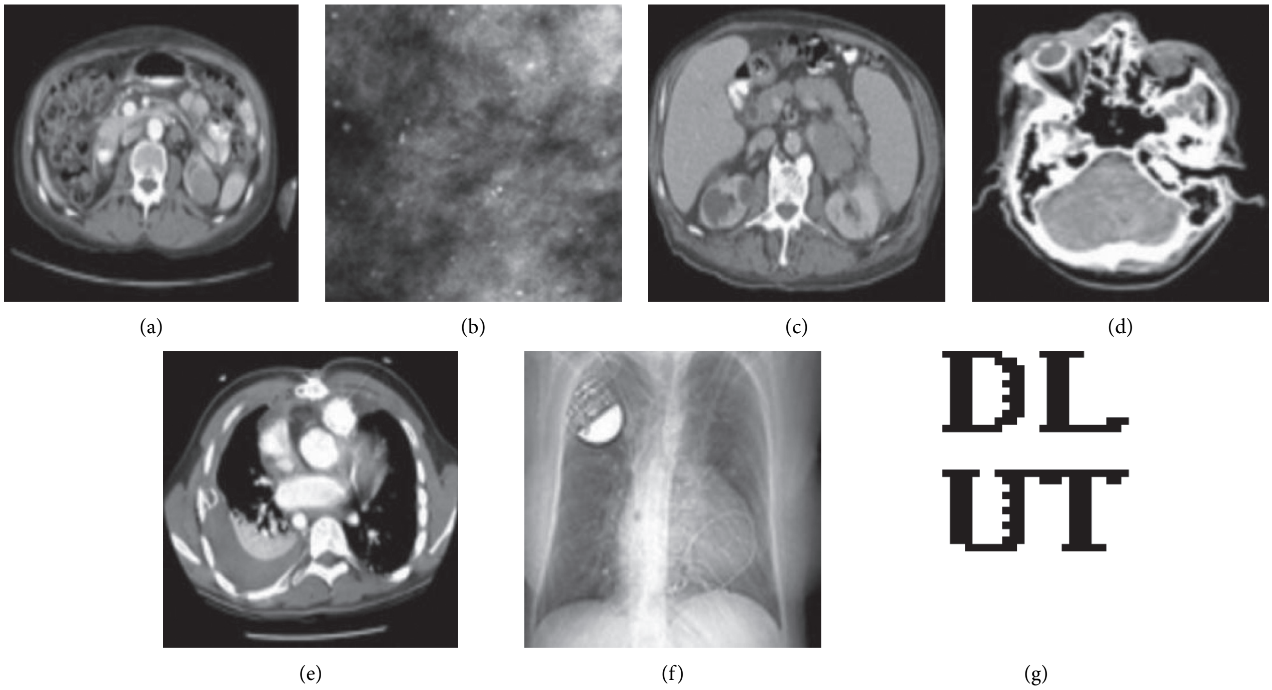


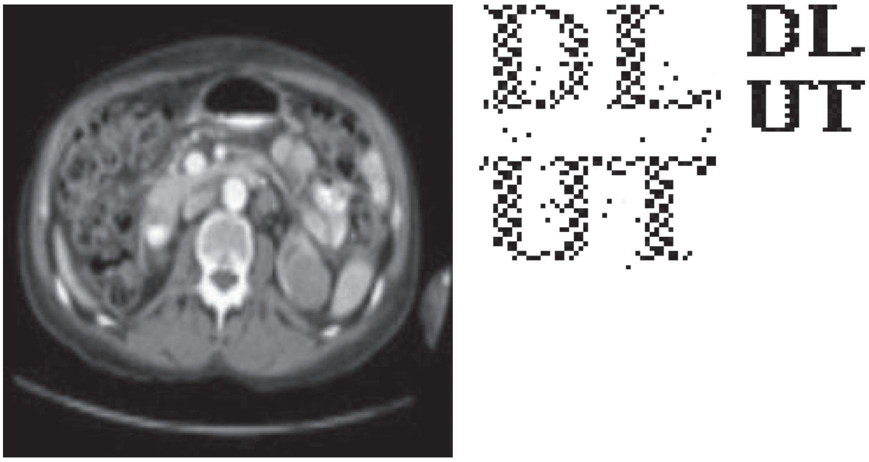
Figure 5: Tested images and logo image. (a) Abdomen. (b) Breast. (c) Adrenal. (d) Head. (e) Heart. (f) Lung. (g) Logo image.

the authentication image extracted from Figure 13(a) is equal to 0.9971.

Table 1: Correlation test between different carrier images.

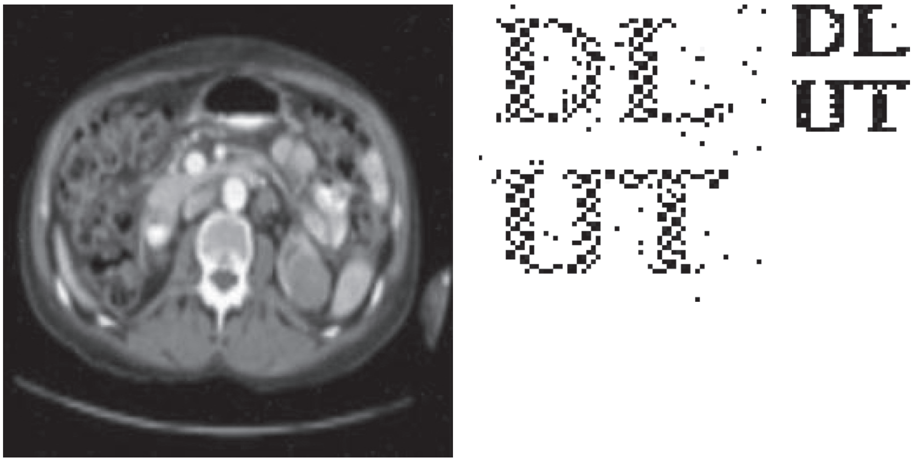
	Abdomen	Breast	Adrenal	Head	Heart	Lung
Abdomen	1	0.6047	0.6096	0.6365	0.6147	0.6169
Breast	0.6047	1	0.5513	0.5713	0.6077	0.5820
Adrenal	0.6096	0.5513	1	0.6011	0.5950	0.5698
Head	0.6365	0.5713	0.6011	1	0.6096	0.5864
Heart	0.6147	0.6077	0.5950	0.6096	1	0.6101
Lung	0.6169	0.5820	0.5698	0.5864	0.6101	1

4.3. Algorithm Comparison. Tables 2 and 3 show the performance comparison between this algorithm and other security authentication algorithms. From the comparison data, the algorithm shows strong robustness in resisting geometric attacks and conventional attacks.



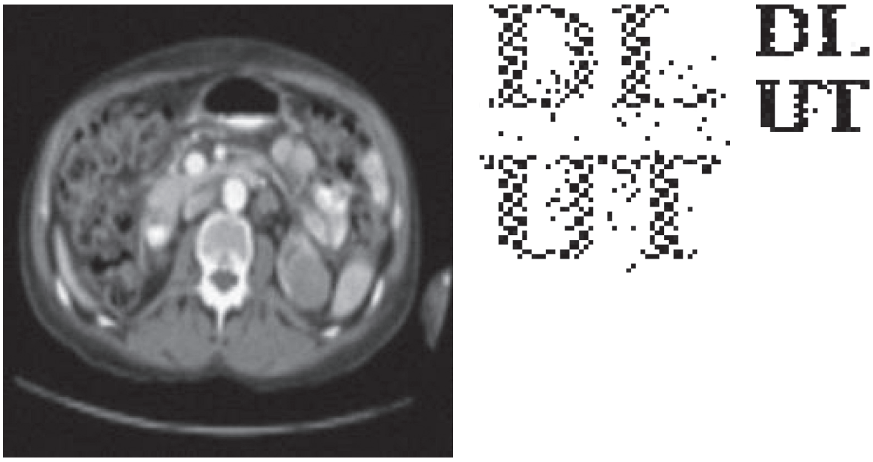
(a) (b) (c)

Figure 6: (a) Under JPEG attack (PSNR = 43.576). (b) Extracted share image from (a). (c) Recovered secrete image from (b) (NC = 0.9961).



(a) (b) (c)

Figure 7: (a) Under salt and pepper noise attack (PSNR = 38.3825). (b) Extracted share image from (a). (c) Recovered secrete image from (b) (NC = 0.9863).



(a) (b) (c)

Figure 8: (a) Under Gaussian noise attack (PSNR = 36.546). (b) Extracted share image from (a). (c) Recovered secrete image from (b) (NC = 0.9805).

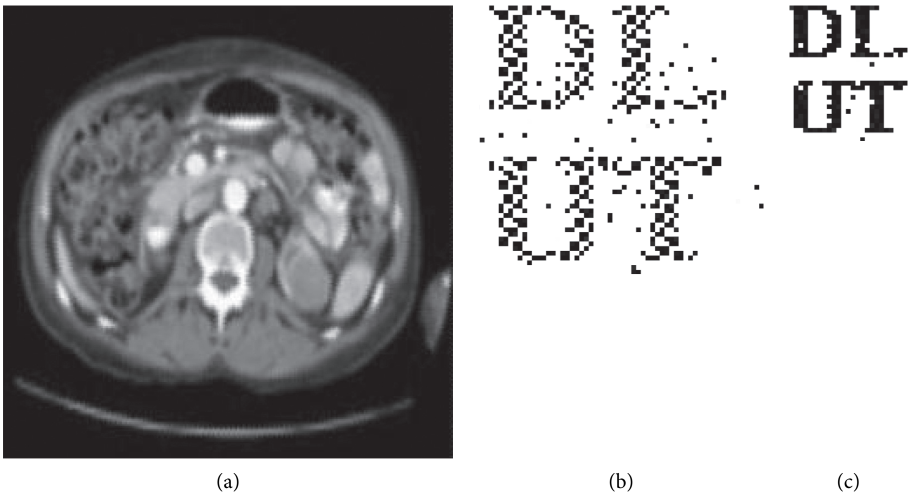


Figure 9: (a) Under rotation attack (PSNR = 32.28). (b) Extracted share image from (a). (c) Recovered secrete image from (b) (NC = 0.9854).

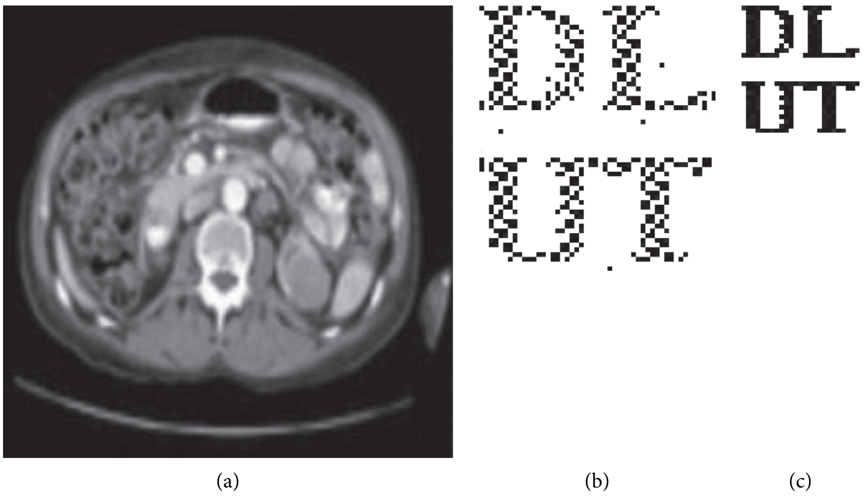


Figure 10: (a) Under scaling attack (PSNR = 43.6755). (b) Extracted share image from (a). (c) Recovered secrete image from (b) (NC = 0.998).

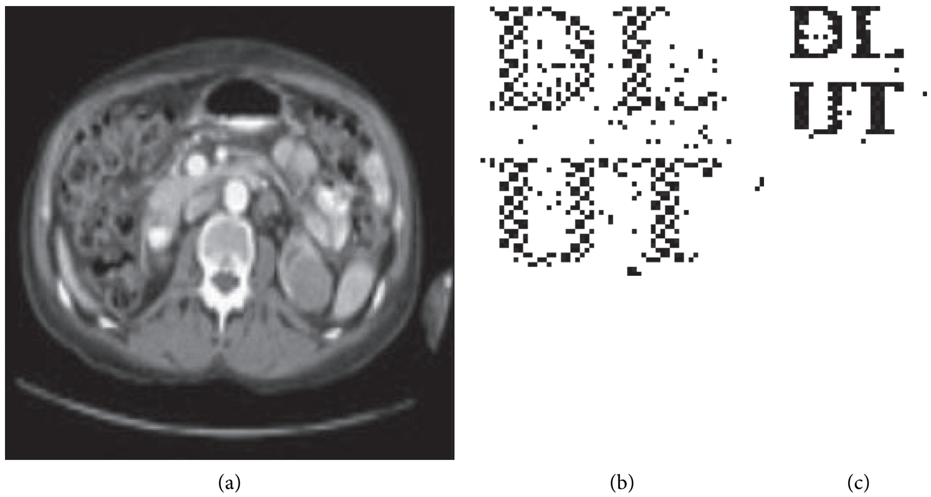


Figure 11: (a) Under sharpening attack (PSNR = 35.9346). (b) Extracted share image from (a). (c) Recovered secrete image from (b) (NC = 0.9707).

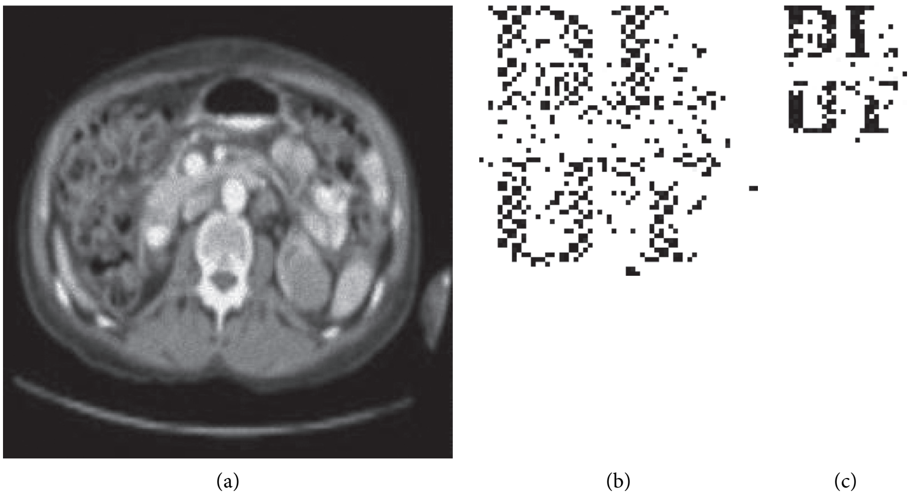


Figure 12: (a) Under multiplicative noise attack (PSNR = 29.1198). (b) Extracted share image from (a). (c) Recovered secrete image from (b) (NC = 0.9209).

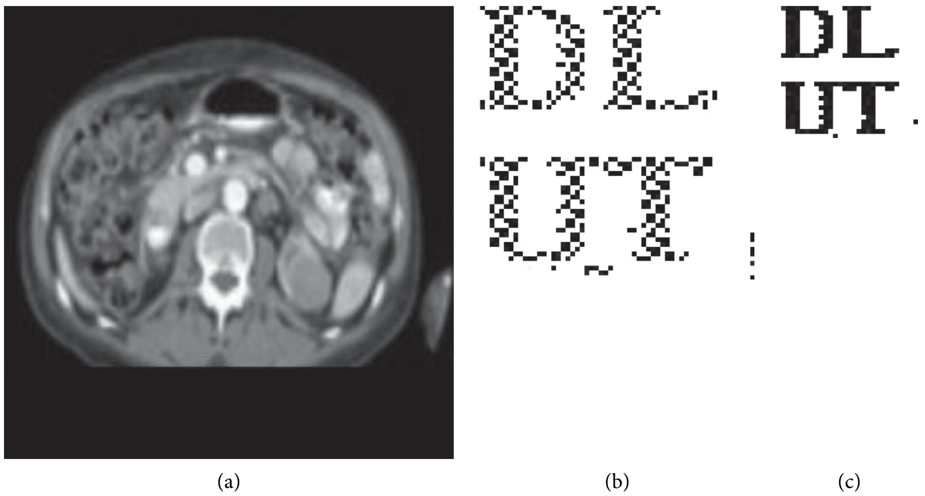


Figure 13: (a) Under cropping attack (PSNR = 24.066). (b) Extracted share image from (a). (c) Recovered secrete image from (b) (NC = 0.9971).

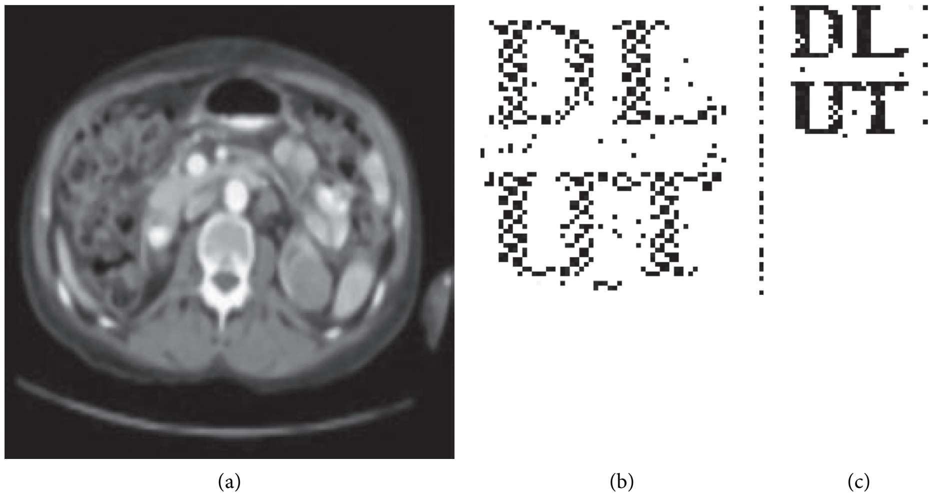
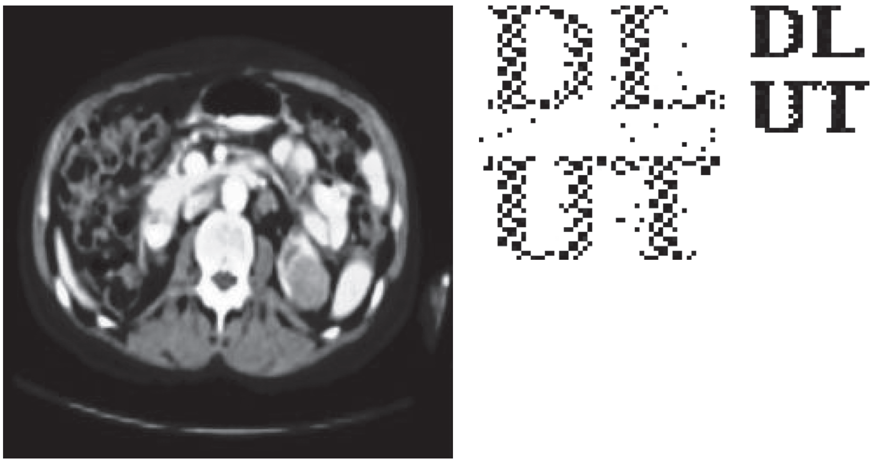
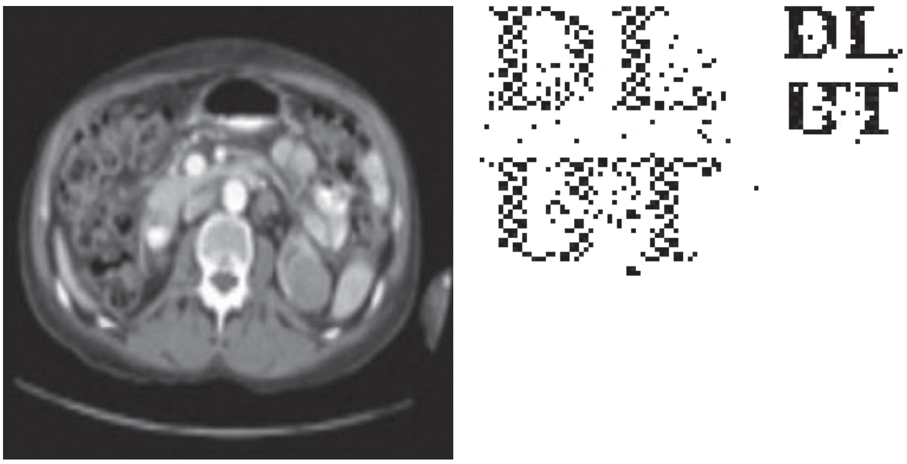


Figure 14: (a) Under median filtering attack (PSNR = 26.2929). (b) Extracted share image from (a). (c) Recovered secrete image from (b) (NC = 0.9766).



(a) (b) (c)

Figure 15: (a) Under contrast enhancement attack (PSNR = 8.997). (b) Extracted share image from (a). (c) Recovered secrete image from (b) (NC = 0.9951).



(a) (b) (c)

Figure 16: (a) Under brightness enhancement attack (PSNR = 34.1651). (b) Extracted share image from (a). (c) Recovered secrete image from (b) (NC = 0.9688).

Table 2: Performance comparison of different algorithms under various attacks [1].

Attacks	Hsieh and Huang's scheme [8]	Hsu and Hou's scheme [13]	Tiankai's scheme [17]	Proposed scheme
Sharpening	0.752	0.819	0.9561	0.9707
Median filtering	0.843	0.938	0.9775	0.9766
Resizing	0.733	0.887	0.9521	0.9980
Noise addition	0.723	0.761	0.9854	0.9863
JPEG	0.845	0.956	0.9912	0.9961

Table 3: Performance comparison of different algorithms under various attacks [2].

Attacks	Hu and Zhu's scheme [3]	Gao's scheme [15]	Xiang et al.'s scheme [16]	Tiankai's scheme [17]	Proposed scheme
Gaussian noise	0.9300	0.8594	0.9600	0.9854	0.9805
Median filtering 1	0.9900	0.9453	0.9800	0.9912	0.9980
Median filtering 2	0.9700	0.9063	0.9800	0.9775	0.9766
JPEG (70)	0.9700	1.0000	1.0000	0.9951	0.9951
JPEG (50)	0.9600	—	0.9900	0.9912	0.9961
JPEG (20)	0.9400	0.9570	0.9700	0.9824	0.9795
Cropping (10%)	0.9900	—	—	0.9756	0.9990
Cropping (20%)	0.9700	—	—	0.9463	0.9971
Rotating 1°	0.9300	0.8164	—	0.9102	0.9609
Rotating 2.5°	0.9700	—	—	0.9307	0.9844
Rotating 5°	0.9600	—	1.0000	0.9424	0.9912
Rotating 10°	0.9500	—	0.9500	0.9580	0.9854
Visibility	No	No	No	Yes	Yes

5. Conclusion

Based on the discrete fractal Brownian random field model, the medical image is transformed from gray space to fractal space without adding any noise. In the fractal space, the fractal dimension data is analyzed and mined to form stable features. Based on the stable features, the copyright information of the medical image is authenticated. The security of the method is further enhanced by using the visual cryptography scheme. In the extraction process, the knowledge of probability statistics is applied to further improve the accuracy of the authentication. The scheme has the following characteristics. (1) The fractal dimension reflects the inherent attribute of the image, which is the energy property rather than the visual property. The attribute still shows good intrinsic stability under the affine transformation modes, such as rotation, shearing, size adjustment, and compression transformation. A series of attack tests have proved the robustness of scheme. (2) The meaningful binary image is used as authentication information. This scheme differs from the traditional authentication algorithms simply judge the similarity of the threshold. (3) The security of the algorithm is further enhanced by visual cryptography obfuscation operation. Meanwhile, to improve the accuracy of information detection, the probability and statistics knowledge is applied. At the same time, the algorithm has a good universality, especially suitable for medical images and military images, and has a good theoretical significance and popularization value [18–31].

Data Availability

The tested images are available at http://peir.path.uab.edu/library.

Conflicts of Interest

The authors declare no conflicts of interest.

Authors' Contributions

Xingyuan Wang was responsible of the formal analysis. Bin Ding was responsible of the funding acquisition. Daihong Jiang and Dan Li were responsible of the investigation. Tiankai Sun was responsible of the methodology.

Acknowledgments

This research was supported 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, and 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.

References

[1] L. Jing, L. Jingbing, M. Jixin et al., "A robust multi-watermarking algorithm for medical images based on DTCWT-DCT and henon map," *Applied Sciences*, vol. 9, no. 4, p. 700, 2019.

[2] Y. Tzuo, C. Her, and C. Bin, "Lossless medical image watermarking method based on significant difference of cellular automata transform coefficient," *Signal Processing: Image Communication*, vol. 70, pp. 174–183, 2019.

[3] Y. Hu and S. Zhu, "Zero-watermark algorithm based on PCA and chaotic scrambling," *Journal of Zhejiang University (Engineering Science)*, vol. 42, no. 4, pp. 593–597, 2008.

[4] C. Kavitha and S. Sakthivel, "An effective mechanism for medical images authentication using quick response code," *Cluster Computing*, vol. 22, no. S2, pp. 4375–4382, 2018.

[5] M. Arsalan, A. S. Qureshi, A. Khan, and M. Rajarajan, "Protection of medical images and patient related information in healthcare: using an intelligent and reversible watermarking technique," *Applied Soft Computing*, vol. 51, pp. 168–179, 2017.

[6] A. Fatahbeygi and F. T. Akhlaghian, "A highly robust and secure image watermarking based on classification and visual cryptography," *Journal of Information Security and Applications*, vol. 45, pp. 71–78, 2019.

[7] M. Elham, "Selecting optimal blocks for image watermarking using entropy and distinct discrete firefly algorithm," *Soft Computing*, vol. 23, no. 19, pp. 9685–9699, 2019.

[8] S. Hsieh and B. Huang, "A copyright protection scheme for gray-level images based on image secret sharing and wavelet transformatio," in *Proceedings of the Third International Conference on Information Technology: New Generation*, pp. 661–666, Las Vegas, NV, USA, 2004.

[9] S. Qingtang and C. Beijing, "Robust color image watermarking technique in the spatial domain," *Soft Computing*, vol. 22, no. 1, pp. 91–106, 2018.

[10] Q. Guan and W. Zhang, "Image edge detection based on fractal dimension," *Computer Science*, vol. 42, pp. 296–298, 2015.

[11] M. Naor and A. Shamir, "Visual cryptography," *Advances in Cryptology—EUROCRYPT'94*, Springer, Berlin, Germany, pp. 1–12, 1995.

[12] B. Wenzheng, Y. Bin, B. Rong, and Y. Chen, "LipoFNT: lipoylation sites identification with flexible neural tree," *Complexity*, vol. 2019, Article ID 1603867, 9 pages, 2019.

[13] C. Hsu and Y. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods," *Optical Engineering*, vol. 44, pp. 1–10, 2005.

[14] C. Ankita, M. Dheerendra, and S. Mukhopadhyay, "An enhanced dynamic ID-based authentication scheme for telecare medical information systems," *Journal of King Saud University Computer and Information Sciences*, vol. 29, no. 1, pp. 54–62, 2017.

[15] S. Gao, "An adaptive image zero-watermarking algorithm in DT-CWT domain," *Journal of Sichuan University (Natural Science Edition)*, vol. 6, pp. 493–497, 2008.

[16] H. Xiang, H. Cao, W. Kai-ning, and W. Fang, "A zero-watermarking algorithm based on chaotic modulation," *Journal of Image and Graphics*, vol. 5, pp. 720–724, 2006.

[17] S. Tiankai, W. Xingyuan, and B. Rong, "A hybrid contourlet-singular value decomposition authentication scheme based on chaos and visual cryptography for medical images," *Journal of Computational and Theoretical Nanoscience*, vol. 13, pp. 1–11, 2016.

[18] N. Arsshad and M. Nikooghadam, "An efficient and secure authentication and key agreement scheme for session initiation protocol using EC," *Multimedia Tools and Applications*, vol. 75, no. 1, pp. 181–197, 2016.

[19] B. Wenzheng, H. De-Shuang, and C. Yue-Hui, "Malonylation sites identification tree," *Current Bioinformatics*, vol. 15, no. 1, pp. 59–67, 2020.

[20] B. Wenzheng, Y. Bin, L. Dan et al., "CMSENN: computational modification sites with ensemble neural network," *Chemometrics and Intelligent Laboratory Systems*, vol. 185, pp. 65–72, 2019.

[21] B. Wenzheng, Y. Bin, and H. De-Shuang, "Identification of protein malonylation sites by the key features into general PseAAC," *IEEE Access*, vol. 7, pp. 54073–54083, 2019.

[22] L. Yu, G. Xinxin, and Q. Xin, "A ROI-based reversible data hiding scheme in encrypted medical images," *Journal of Visual Communication and Image Representation*, vol. 39, pp. 51–57, 2016.

[23] B. Wenzheng, Y. Bin, L. Zhengwei, and Y. Zhou, "Lysine acetylation site identification with polynomial tree," *International Journal of Molecular Sciences*, vol. 20, no. 1, pp. 113–131, 2019.

[24] C. Shin-Yan, Y. Zhaoqin, and L. Junqiang, "Improvement of a privacy authentication scheme based on cloud fro medical environment," *Journal of Medical Systems*, vol. 40, no. 4, pp. 1–15, 2016.

[25] B. Wenzheng, Y. Chang-An, Z. Youhua et al., "Mutli-features prediction of protein translational modification sites," *IEEE-ACM Transactions on Computational Biology and Bioinformatics*, vol. 15, no. 5, pp. 1453–1460, 2018.

[26] B. Wenzheng, W. Dong, and C. Yuehui, "Classification of protein structure classes on flexible neutral tree," *IEEE-ACM Transactions on Computational Biology and Bioinformatics*, vol. 14, no. 5, pp. 1122–1133, 2017.

[27] B. Wenzheng, H. Zhenhua, and Y. Changan, "Pupylation sites prediction with ensemble classification model," *International Journal of Data Mining and Bioinformatics*, vol. 18, pp. 91–104, 2017.

[28] U. A. Muhammad, D. Abdelouahid, K. Saleem et al., "A survey of authentication schemes in telecare medicine information systems," *Journal of Medical Systems*, vol. 14, pp. 1–26, 2017.

[29] B. Wenzheng, C. Yuehui, and W. Dong, "Prediction of protein structure classes with flexible neural tree," *Bio-Medical Materials and Engineering*, vol. 24, no. 6, pp. 3797–3806, 2014.

[30] Z. Xiao, Z. Heng, and W. Chengyou, "A robust image watermarking technique based on DWT, APDCBT, and SVD," *Symmetry*, vol. 10, no. 3, pp. 1–14, 2018.

[31] S. Tiankai, B. Rong, and Z. Renwei, "Research on the dynamic sharing scheme of core medical information in the cloud," *Journal of Xuzhou Institute of Technology*, vol. 30, pp. 79–84, 2015.