ChinaRxiv

AI translation · View original & related papers at
chinarxiv.org/items/chinaxiv-201812.00090

Postprint: Medical Image Frequency-Domain Encryption Algorithm Based on 2D Sine-Logistic Chaotic Map

Authors: Deng Xiaohong, Liang Diqing, Liu Huiwen

Date: 2018-12-13T00:00:00+00:00

Abstract

To address the deficiencies in encryption efficiency and security of existing medical image encryption algorithms, a wavelet-domain encryption algorithm for medical images based on the 2D sine Logistic chaotic map is proposed. The algorithm first employs integer wavelet transform to convert the medical image from the spatial domain to the frequency domain, thoroughly breaking the correlation between pixels. Secondly, it utilizes the 2D sine Logistic chaotic map to generate chaotic sequences, selecting the low-frequency coefficients LL3 from the three-level wavelet decomposition for diffusion and scrambling encryption to improve encryption efficiency. Additionally, diffusion encryption is performed on the medium-high frequency coefficients HL2 and LH2 from the second-level wavelet decomposition to resolve the prominent contour problem present in encrypted images. Finally, the encrypted wavelet coefficients undergo inverse wavelet transform to obtain the encrypted image. Experimental simulation results demonstrate that the algorithm possesses high security and encryption efficiency. Compared with existing spatial-domain methods, the encryption time is approximately 1/40; and compared with existing frequency-domain methods, it achieves better concealment of the encrypted image while maintaining encryption efficiency.

Full Text

Preamble

Medical Image Encryption Algorithm in Frequency Domain Based on 2D Sine Logistic Chaotic Mapping

Deng Xiaohong[1], Liang Diqing[2], Liu Huiwen[1] [1]College of Applied Science, Jiangxi University of Science & Technology, Ganzhou Jiangxi 341000, China

[2]Informatization Construction & Management Dept., Changsha University of Science & Technology, Changsha 410114, China

Abstract: To address the limitations of existing medical image encryption algorithms in terms of efficiency and security, this paper proposes a novel wavelet-domain encryption algorithm for medical images based on a 2D sine Logistic chaotic map. The algorithm first employs integer wavelet transform to convert medical images from the spatial domain to the frequency domain, effectively breaking the correlation between pixels. Second, it utilizes the 2D sine Logistic chaotic map to generate chaotic sequences, selecting the low-frequency coefficients LL from three-level wavelet decomposition for diffusion and scrambling encryption to improve encryption efficiency. Additionally, the medium-high frequency coefficients HL and LH from two-level wavelet decomposition undergo diffusion encryption to resolve the prominent contour problem present in encrypted images. Finally, the encrypted wavelet coefficients are reconstructed through inverse wavelet transform to obtain the encrypted image. Experimental simulation results demonstrate that the proposed algorithm achieves high security and encryption efficiency. Compared with existing spatial-domain methods, the encryption time is approximately 1/40; compared with existing frequency-domain methods, it provides better imperceptibility of encrypted images while maintaining encryption efficiency.

Keywords: chaotic mapping; medical image; data encryption; integer wavelet transform; imperceptibility

0 Introduction

With the continuous development of "Internet + Healthcare,"online transmission of medical images has become increasingly common. Digital medical images play a crucial role in clinical diagnosis, but as they contain important patient privacy information, their security has attracted widespread attention from researchers [1~3]. Among various security protection methods, encryption remains an effective approach for active data protection. Compared with natural images, medical images exhibit characteristics such as large data volume, typical regional features, high pixel correlation, and non-uniform histogram distribution. Consequently, some encryption methods suitable for natural images are not applicable to medical images. For instance, traditional AES and 3DES algorithms cannot meet the real-time encryption requirements for large-volume medical images. Chaotic maps possess pseudo-randomness, ergodicity, and sensitivity to initial conditions, and chaotic sequences generated from them exhibit desirable cryptographic key properties. Chaotic cryptography has gradually emerged as a new research direction in cryptography, and medical image encryption using chaotic maps has been proven to offer high security and efficiency [4~6].

Currently, chaos-based medical image encryption algorithms can be divided into two categories: spatial-domain and frequency-domain methods. The for-

mer encrypts medical image pixels using chaotic sequences, with typical approaches found in references [7~9]. Reference [7] designed a scrambling and substitution-diffusion architecture based on chaotic maps for medical image encryption, which encrypts all pixels through XOR operations before changing their positions. While this algorithm demonstrates high encryption performance, its efficiency is limited due to the large data volume of medical images. To address the efficiency issues of spatial-domain algorithms, Moumen et al. [8] proposed encrypting only selected pixels using graph coloring theory. Pareek et al. [9] suggested encrypting only the region of interest (foreground region) based on the regional characteristics of medical images. However, these methods require feature extraction, pattern matching, and other prior knowledge, reducing algorithm operability. For instance, region segmentation is needed for ROI extraction, and irregular region characteristics require representation [10].

Frequency-domain encryption methods first transform medical images from the spatial domain to the frequency domain, then encrypt selected frequency coefficients before inverse transformation to obtain the encrypted image, with typical approaches in references [11~13]. Reference [11] proposed an encryption method based on cosine transform and chaotic mapping, which offers high efficiency. However, since cosine transform involves floating-point operations, ensuring reversibility of medical image encryption/decryption without specialized floating-point hardware is impractical. To solve this problem, Wu et al. [12] and Liang et al. [13] both proposed encryption methods based on integer wavelet transform and hyper-chaotic mapping. Integer wavelet transform avoids floating-point issues in coefficient operations, while hyper-chaotic mapping enhances algorithm security. These algorithms only encrypt low-frequency coefficients after wavelet decomposition, significantly improving encryption efficiency, but hyper-chaotic sequence generation becomes a bottleneck in time efficiency. Since no explicit correspondence exists between frequency-domain coefficients and spatial-domain pixels, changes in frequency-domain coefficients often affect numerous spatial-domain pixel values, making frequency-domain coefficient selection advantageous for security and more efficient than spatial-domain algorithms.

In summary, spatial-domain encryption algorithms offer higher encryption performance but lower efficiency compared to frequency-domain methods. Frequency-domain methods only encrypt partial coefficients, requiring more complex chaotic maps to enhance security, yet hyper-chaotic system design challenges encryption efficiency. Experimental analysis of reference [13] reveals that encrypting only low-frequency coefficients causes severe contour visibility in encrypted images when medical images contain distinct boundaries, compromising algorithm security. To address these issues, this paper proposes a medical image frequency-domain encryption algorithm based on 2D sine Logistic chaotic mapping. The employed 2D sine Logistic chaotic map has been proven to exhibit hyper-chaotic behavior while being composed of simple low-dimensional chaotic systems with a simpler structure. Additionally, simple diffusion encryption is applied to medium-high frequency subbands after

wavelet decomposition to break edge and texture information, resolving the contour problem in encrypted images.

1.1 Integer Wavelet Transform

To ensure reversibility of image encryption/decryption, the LeGall 5/3 integer wavelet transform based on the lifting scheme is adopted. This transform maps integers to integers and guarantees lossless information during forward and inverse wavelet transforms, serving as the reversible wavelet transform specified in the JPEG2000 compression standard [13]. For a one-dimensional signal where values are integers, the forward wavelet transform can be performed using Equation (1). The low-frequency and high-frequency coefficients obtained from one-level decomposition can be further decomposed using Equation (1) for higher-level analysis, where represents the low-frequency coefficients from three-level wavelet decomposition. For two-dimensional image matrices, wavelet decomposition can be applied separately to row and column vectors, and the inverse wavelet transform using Equation (2) reconstructs the original image from the coefficient matrix.

where j represents the decomposition level. Figure 1 [Figure 1: see original paper] illustrates the frequency-domain coefficient subbands after three-level wavelet decomposition and a medical image decomposition example. Each wavelet decomposition level yields four frequency subbands: LL, HL, LH, and HH. The LL subband contains low-frequency coefficients, concentrating most of the original image' s energy as an approximation of the original image. The HL and LH subbands represent medium-high frequency coefficients in vertical and horizontal directions, respectively, containing texture and edge information that primarily constitute image contours.

1.2 2D Sine Logistic Chaotic Mapping

One-dimensional chaotic systems feature simpler structures but inferior security performance. For example, the Logistic chaotic system has proven security vulnerabilities [14]. High-dimensional chaotic systems offer more complex structures and better chaotic performance but are computationally expensive. Hua et al. [15] combined two one-dimensional chaotic systems—Logistic and Sine maps —to propose the 2D sine Logistic chaotic map, demonstrating advantages in both security and implementation efficiency compared to other high-dimensional chaotic systems. The 2D sine Logistic chaotic map can be expressed as:

where and . When and , the 2D sine Logistic chaotic map exhibits hyper-chaotic behavior.

1.3 Problem Statement

Reference [15] first generates chaotic sequences using the 2D sine Logistic chaotic map, then designs pixel position scrambling and diffusion algorithms that oper-

ate directly on all image pixels. Table 1 presents the test results of the method from reference [15] on the natural image Lena with different image sizes. The results show that the encrypted image entropy approaches the ideal value of 8, indicating good encryption performance. However, encryption time increases significantly with image size. Although better experimental environments may yield improved results, the algorithm is unsuitable for large-volume medical images due to both the large amount of data requiring encryption in the spatial domain and the excessive complexity of the designed diffusion and scrambling algorithms.

Figure 2 [Figure 2: see original paper] shows the encryption results of the cover image CT using the method from reference [13]. This method only encrypts low-frequency coefficients from three-level wavelet decomposition, resulting in visible contours in the encrypted image. Experimental analysis demonstrates that reference [13] achieves good encryption effects for medical images without distinct contours, but when medical images exhibit high contrast between foreground and background regions (black-and-white distinction), obvious contours appear in encrypted images. The presence of original image contours severely compromises encryption algorithm security, as attackers can break the encryption through chosen-plaintext attacks.

2.1 Algorithm Model

The proposed algorithm model is illustrated in Figure 3 [Figure 3: see original paper]. The algorithm first performs three-level forward wavelet transform on the original medical image to obtain its coefficient matrix, selecting the low-frequency coefficients LL from three-level decomposition and the medium-high frequency coefficients LH and HL from two-level decomposition as encryption targets while keeping other coefficients unchanged. Given chaotic initial values and parameters, the algorithm generates chaotic sequences 1 and 2 using the 2D sine Logistic chaotic map. The coefficient LL undergoes diffusion encryption using sequence 1, followed by scrambling using sequence 2. The coefficients LH and HL undergo diffusion encryption using sequence 1. Finally, the encrypted coefficient matrix is reconstructed through inverse wavelet transform along with unchanged coefficients to obtain the encrypted medical image. The decryption process is the inverse of encryption: the encrypted medical image is processed similarly, with coefficient LL first undergoing inverse scrambling followed by inverse diffusion, while other steps remain unchanged to achieve decryption. The algorithm constructs a secure image transmission model in public network environments, where image senders and receivers negotiate keys transmitted through public-key cryptography. Due to the large key space and strong initial value sensitivity of chaotic encryption systems, attackers cannot recover correct image information from ciphertext alone without the key.

The innovation of this paper lies in applying the 2D sine Logistic chaotic map to wavelet-domain encryption of medical images, designing novel chaotic diffusion and scrambling methods to improve encryption efficiency, and simultaneously

selecting LH and HL coefficients for scrambling encryption to effectively resolve the contour problem arising from encrypting only low-frequency coefficients.

2.2 Diffusion and Scrambling Algorithm Based on 2D Sine Logistic

1) Diffusion Mechanism

Let and be chaotic sequences generated by the 2D sine Logistic chaotic map, where is used for coefficient diffusion and for position scrambling of diffused coefficients. Let be the coefficient set after integer wavelet decomposition of the original medical image. Equation (4) generates chaotic keys, and Equation (5) employs a forward feedback mechanism for coefficient diffusion.

where represents the key, is the number of elements in , mod is the modulo function, round is the rounding function, and denotes XOR operation. is the encrypted coefficient set, and len is the length of the coefficient set.

2) Scrambling Mechanism

The diffused coefficients are scrambled using Equation (6) to change coefficient positions.

where represents the result of ascending sorting of sequence , location stores the original positions of sorted elements, sort is the ascending sort function, and represents the result after position scrambling.

The diffusion and scrambling algorithm based on 2D sine Logistic is presented as Algorithm 1.

Algorithm 1: Diffusion and Scrambling Encryption of Input Coefficients Based on Generated Chaotic Sequences

Input: Chaotic sequence set , coefficient set coe
Output: Encrypted coefficient set

1. Initialize = coe; // Original coefficient set
2. for i = 1:len do // len is set length
3. `(i) = mod(round((i) × 10 ), 256);`
4. end for
5. for i = 1:len do
6. `Use Equation 5 for encryption; // Diffusion encryption`

7. end for
8. [sort_seq2, loc] = sort(seq2); // Ascending sort of seq2
9. for i = 1:len do
10. `(loc(i)); // Position scrambling`
11. end for
12. output

Building upon Algorithm 1, the proposed medical image frequency-domain encryption algorithm is presented as Algorithm 2.

Algorithm 2: Generating Encrypted Medical Image from Given Chaotic Parameters and Original Medical Image

Input: Chaotic initial values x , y , control parameters and , original medical image I
Output: Encrypted medical image EI

1. EI = I; // Initialize as original medical image
2. [dim1, dim2] = size(I); // Get medical image dimensions
3. Level = 3; // Set wavelet decomposition level
4. decompose53(I, dim1, level); // Forward wavelet transform
5. N = dim1 / (2^level);
6. cof_LL = s33(1:N, 1:N); // s33 is low-frequency coefficients from three-level decomposition
7. cof_HL = s22(1:N×2, N×2+1:2×N×2); // s22 is low-frequency coefficients from two-level decomposition
8. cof_LH = d22(1:N×2, 1:2×N); // d22 is high-frequency coefficients from two-level decomposition

9. [seq1, seq2] = D2_SLMM(, x , y , 4×N×N); // D2_SLMM generates chaotic sequences using Equation (3)

10. for each cof_LL do

11. `Call Algorithm 1 to obtain e_cof_LL;`

12. end for

13. for each cof_HL and cof_LH do

14. `Call scrambling method in Algorithm 1 to obtain e_cof_HL and e_cof_LH;`

15. end for

16. s33(1:N, 1:N) = e_cof_LL;

17. s22(1:N×2, N×2+1:2×N×2) = e_cof_HL;

18. d22(1:N×2, 1:2×N) = e_cof_LH;

19. EI = recompose53(I' , dim1, level); // Inverse wavelet transform

20. output EI;

3 Experimental Results and Analysis

The six medical images selected for experiments are from Xiangya Medical College of Central South University, including four images of size 512×512 (x-ray, US, CT, MRI) and two images of size 1024×1024 (CT_foot and MRI_cervices). The experimental environment: MATLAB 7.0, Intel(R) CoreTM i5-6500 3.20 GHz CPU, 8 GB RAM, 64-bit Windows 7 Ultimate OS. The initial values for the 2D sine Logistic chaotic map are set as x = 0.9380, y = 0.7006, with control parameters , .

3.1.1 Encryption Results

Figure 4 [Figure 4: see original paper] shows the encryption results of cover medical images using the proposed algorithm. In Figure 4, (a)(c)(e)(g)(i)(k) represent original medical images, and (b)(d)(f)(h)(j)(l) are their corresponding encrypted images. The encrypted images exhibit random noise distribution characteristics with good encryption effects. When encrypted images remain

untampered and decryption keys match encryption keys, the original medical images can be recovered losslessly. Comparing results between Figure 2(b) and Figure 4(d) clearly demonstrates that the proposed algorithm effectively resolves the contour problem in encrypted images. By analyzing wavelet decomposition characteristics, the algorithm selects medium-high frequency subbands from two-level decomposition (representing image texture and edge information) for encryption. This ensures that encrypted coefficients undergo iterative reconstruction during inverse wavelet transform, thoroughly masking image edge information. Experiments also tested encrypting medium-high frequency subbands from three-level decomposition, but the effect was less significant than using two-level coefficients. While encrypting medium-high frequency coefficients from one-level decomposition could better resolve contour issues, encryption time increased substantially.

3.1.2 Performance Analysis

1) Key Security Analysis

Key security is primarily measured by key space and key sensitivity. Key space size determines the difficulty of brute-force attacks, while key sensitivity ensures that adversaries cannot recover original information using keys close to the actual key. The designed key length is 128 bits (chaotic initial values and control parameters occupy 4 bytes each, totaling $4 \times 32 = 128$ bits), resulting in a key space of 2^{12} , making brute-force attacks computationally infeasible. Experimental tests modified the initial value x of the 2D sine Logistic chaotic map to 0.9381 while keeping other parameters unchanged. Using this modified key for image decryption yielded the test results shown in Figure 5 [Figure 5: see original paper]. In Figure 5, (a) is the original medical image, (b) is the image encrypted with the default key, (c) is the image encrypted with the modified key, and (d) shows the difference between images (b) and (c). The results demonstrate that slight key changes cause significant differences in encryption outcomes, and decryption with the modified key cannot recover the original medical image.

2) Statistical Attack Resistance Analysis

Encrypted image entropy and adjacent pixel correlation are effective quantitative measures for evaluating statistical attack resistance. Image entropy represents statistical characteristics of gray-level distribution. For encrypted images resembling random noise, the gray-level distribution should approach uniformity with an expected value of 8. The entropy and pixel correlation formulas are:

where N is the number of gray levels, is the probability of pixel value . In Equation (8), E denotes expectation, X and Y are data sequences, and are means, and and are standard deviations. High correlation between sequences X and Y yields corr values approaching 1, while low correlation approaches 0.

The calculated entropy of the six encrypted images is approximately 7.8, close

to the ideal value of 8. Table 2 presents the pixel correlation of cover image CT_foot before and after encryption. The results show that encrypted images exhibit very low pixel correlation. In summary, the proposed encryption algorithm effectively resists statistical attacks.

3) Differential Attack Resistance Analysis

Differential attacks analyze how specific differences in plaintext propagate through encryption to attack cryptographic algorithms. The sensitivity of encrypted images to plaintext is a common measure for evaluating differential attack resistance, typically calculated using the Number of Pixels Change Rate (NPCR) in Equation (9).

where I and I are ciphertexts corresponding to two medical images differing by only one pixel value, M × N is image size, and C and C are the two medical images. Figure 6 [Figure 6: see original paper] presents NPCR test results. Sixty groups of medical images were tested (each cover image had 10 different pixels modified to form groups). Each group was numbered and randomly selected for encryption, with NPCR values calculated for each group. The results show pixel change rates fluctuating around the ideal value of 0.996 [13], indicating strong differential attack resistance.

4) Encryption/Decryption Efficiency Analysis

Table 3 lists the encryption and decryption times for six cover images, with data averaged over 10 encryption/decryption operations. For 512×512 medical images, encryption/decryption times are approximately 1.1 seconds, while for 1024×1024 images, times are around 5 seconds, demonstrating good encryption/decryption efficiency.

3.2 Comparison Results and Analysis

The proposed algorithm primarily builds upon references [13, 15], with experimental results compared against these methods in terms of encrypted image entropy, encryption time, and contour visibility. Table 4 presents the comparison results. Compared with reference [15], although the encrypted image entropy is slightly lower, the proposed algorithm shows significant advantages in encryption time. For an M×N image, reference [15] requires encrypting M×N pixels, while the proposed algorithm only encrypts M×N(1/2 + 1/2³) M×N/8 coefficients. Compared with reference [13], the proposed algorithm' s encrypted image entropy is closer to the ideal value of 8 due to encrypting more coefficients, yet encryption time remains similar because reference [13]' s hyper-chaotic sequence generation is more complex than 2D sine Logistic. Beyond entropy, the proposed algorithm' s greatest advantage is solving the contour problem in encrypted images.

4 Conclusion

The demand for secure medical image transmission in network environments continues to grow, with chaos-based medical image encryption methods receiving extensive attention from researchers. Building upon analysis of existing methods and fully considering medical image characteristics, this paper proposes a medical image frequency-domain encryption algorithm based on 2D sine Logistic chaotic mapping. The algorithm designs novel chaotic diffusion and scrambling methods, encrypting low-frequency coefficients from three-level wavelet decomposition to enhance security and efficiency. To address contour problems in encrypted images, medium-high frequency coefficients from two-level wavelet decomposition representing edge and texture information are selected for chaotic diffusion. Experimental results demonstrate that the proposed algorithm offers advantages in encryption security and efficiency, making it suitable for real-time encryption of large-volume medical images.

References

[1] Cao Weijia J, Zhou Yicong, Chen C L P, et al. Medical image encryption using edge maps [J]. Signal Processing, 2017, 132(3): 134-144. [2] Shabir A P, Frahana A, Javaid A S, et al. Hiding clinical information in medical images: a new high capacity and reversible data hiding technique [J]. Journal of Biomedical Informatics, 2017, 66(2): 214-230. [3] Kumar C V, Natarajan V, Poonguzhali P. Secured patient information transmission using reversible watermarking and DNA encryption for medical images [J]. Applied Mathematical Sciences, 2015, 9(48): 98-116. [4] Ravivhandran D, Praveenkumar P, Balaguru Rayappan J B, et al. Chaos based crossover and mutation for securing DICOM image [J]. Computers in Biology and Medicine, 2016, 72(5): 170-184. [5] Singh L D, Singh K M. Medical image encryption based on improved ElGamal encryption technique [J]. Optik, 2017, 147(10): 88-102. [6] Hua Zhongyun, Yi Shuang, Zhou Yicong. Medical image encryption using high-speed scrambling and pixel adaptive diffusion [J]. Signal Processing, 2018, 144(3): 134-144. [7] Kanso A, Ghebleh M. An efficient and robust image encryption scheme for medical applications [J]. Communications in Nonlinear Science and Numerical Simulations, 2015, 24(1): 98-116. [8] Moumen A, Bouye M, Sissaoui H. New secure partial encryption method for medical images using graph coloring problem [J]. Nonlinear Dynamics, 2015, 82(3): 1475-1482. [9] Pareek N K, Patidar V. Medical image protecting using genetic algorithm operations [J]. Soft Computing, 2016, 20(2): 763-772. [10] Deng Xiaohong, Chen Zhigang, Liang Diqing, et al. Region-based lossless data hiding with high capacity for medical images [J]. Journal of Communications, 2015, 36(1): 187-196. [11] Lima J B, Madeiro F, Sales F J R. Encryption of medical images based on the cosine number transform [J]. Signal Processing: Image Communication, 2015, 35(1): 1-8. [12] Wu Xiangjun, Wang Dawei, Kurths J, et al. A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system [J]. Information Sciences, 2016, 349-350(C): 137-153. [13] Liang Diqing, Chen Zhigang, Deng Xiaohong. Encryption method

of medical image based on wavelet transform and hyper-chaotic mapping [J]. Journal of Tianjin University: Science and Technology, 2016, 49(12): 1255-1261. [14] Chen Zhigang, Liang Diqing, Deng Xiaohong, et al. Performance analysis and improvement of logistic chaotic mapping [J]. Journal of Electronics & Information Technology, 2016, 38(6): 1547-1551. [15] Hua Zhongyun, Zhou Yicong, Pun C M, et al. 2D sine Logistic modulation map for image encryption [J]. Information Sciences, 2015, 297(C): 80-94.

Note: Figure translations are in progress. See original paper for figures.

Source: ChinaXiv —Machine translation. Verify with original.