mathematics

MDPI

Article

Double Security Level Protection Based on Chaotic Maps and SVD for Medical Images

Conghuan Ye [1,2,*], Shenglong Tan[1,2], Jun Wang [1,2], Li Shi [1,2], Qiankun Zuo [1,2] and Bing Xiong [3,*]

[1] School of Information Engineering, Hubei University of Economics, Wuhan 430205, China; tsl@hbue.edu.cn (S.T.); wjstky@hbue.edu.cn (J.W.); sl@hbue.edu.cn (L.S.); qk.zuo@hbue.edu.cn (Q.Z.)
[2] Hubei Internet Finance Information Engineering Technology Research Center, Hubei University of Economics, Wuhan 430205, China
[3] School of Computer and Communication Engineering, Changsha University of Science & Technology, Changsha 410114, China
* Correspondence: p2pgrid@hbue.edu.cn (C.Y.); xiongbing@csust.edu.cn (B.X.)

Abstract: The widespread distribution of medical images in smart healthcare systems will cause privacy concerns. The unauthorized sharing of decrypted medical images remains uncontrollable, though image encryption can discourage privacy disclosure. This research proposes a double-level security scheme for medical images to overcome this problem. The proposed joint encryption and watermarking scheme is based on singular-value decomposition (SVD) and chaotic maps. First, three different random sequences are used to encrypt the LL subband in the discrete wavelet transform (DWT) domain; then, HL and LH sub-bands are embedded with watermark information; in the end, we obtain the watermarked and encrypted image with the inverse DWT (IDWT) transform. In this study, SVD is used for watermarking and encryption in the DWT domain. The main originality is that decryption and watermark extraction can be performed separately. Experimental results demonstrate the superiority of the proposed method in key spaces (10^{225}), PSNR (76.2543), and UACI (0.3329). In this implementation, the following key achievements are attained. First, our scheme can meet requests of different security levels. Second, encryption and watermarking can be performed separately. Third, the watermark can be detected in the encrypted domain. Thus, experiment results and security analysis demonstrate the effectiveness of the proposed scheme.

Keywords: smart healthcare system; medical image security; joint encryption and watermarking; chaotic neural network; privacy protection

MSC: 68P25; 94A60

check for updates

Academic Editor: Junzo Watada

Received: 16 December 2024
Revised: 30 December 2024
Accepted: 6 January 2025
Published: 8 January 2025

Citation: Ye, C.; Tan, S.; Wang, J.; Shi, L.; Zuo, Q.; Xiong, B. Double Security Level Protection Based on Chaotic Maps and SVD for Medical Images. *Mathematics* **2025**, *13*, 182. https://doi.org/10.3390/math13020182

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The smart healthcare system is a component of the Internet of Medical Things (IoMT). It is hidden inside everyday medical objects that surround us and help us. The IoMT is becoming the dominant technology in homes, cell phones, medical instruments, and consumer medical electronics. The smart healthcare system is often used in medical care and increasingly helps to improve the quality of diagnostic tools available to physicians and treatment available to patients. The smart healthcare system has played key roles in telediagnosis, telesurgery, etc. At the same time, they often need to provide their services within strict deadlines to patients and the surrounding world.

Sharing medical images will be essential to smart healthcare systems. There are certain advantages to sharing. Medical image sharing in smart healthcare systems is inevitable due

to the popularity of IoMT; however, this does not imply that medical image sharing will be welcomed, and most individuals find the move to smart healthcare systems difficult. Data on images are created and sent. There are serious security and privacy issues with image communication in smart healthcare systems. Smart healthcare technologies that transmit medical images present new privacy protection challenges.

In smart healthcare systems, medical gadgets are always essential. Medical equipment present unique concerns, including the ability to extract confidential information and alter recorded medical images [1]. Due to the sensitive personal data involved, privacy issues will prevent smart healthcare systems from being widely used. The usage of smart healthcare systems may be restricted due to privacy concerns over the dissemination of medical images. Thus, patient privacy and security protection must be maintained [2]. To reach the next level of smart healthcare systems capabilities with minimal security and privacy compromises, methods, architectures, protocols, and verification techniques are required [3].

The number of IoMT devices that could be used to access or input medical images has been growing quickly [4]. The ability to quickly and easily communicate medical images concurrently in smart health systems has brought the practice into the public eye [5]. Sharing medical images has increased the need for smart health systems. In their clinical practice, doctors have already observed these advantages when they employed smart health systems to improve medical image dissemination in a private and secure manner [6]. However, until patients are certain that their medical images are secure and private, medical image interchange can never realize its full potential. In smart healthcare systems, the transmission of diagnostic reports and medical images across hospitals presents additional issues for the protection of identifiable medical image data. Cryptographic mechanisms are commonly used for medical image protection.

Encryption is a very common way to achieve medical image protection [7]. Full encryption of medical images was the first approach to medical image security. Most image encryption schemes were conducted in the spatial domain with full encryption methods [8–11]. In addition, the paper [12] presented an image encryption algorithm with a novel two-dimensional cross-hyperchaotic Sine-modulation-Logistic map (2D-CHSLM). Kocak et al. proposed an encryption scheme based on a logistic exponential map [13] and a color image encryption algorithm using a 2D hyperchaotic map [14]. A medical image encryption scheme was proposed in [15]. Feng et al. researched a multi-image encryption scheme [16], a pixel fusion strategy for image encryption [17], and a multichannel image encryption scheme based on hyperchaotic maps [18]. Wang et al. proposed a color image encryption scheme [19]. The research [20] encrypted face images based on DNA diffusion. A three-dimensional chaotic map for ship image encryption was proposed in [21].

All these image encryption schemes based on chaotic maps encrypt all content in the spatial domain. All of them involve full encryption. Recently, diverse cryptanalysis studies for advancing full encryption techniques in the spatial domain were proposed, such as image encryption cryptanalysis in [22], cryptanalyzing an image cipher using multiple chaos and DNA operations [23], and cryptanalyzing an image encryption algorithm with filtering and diffusion [24].

Both of the above image encryption algorithms are based on chaotic maps. Due to the application value of chaotic systems in image encryption, various chaotic systems [25,26] have been constructed recently. High-order polynomial chaotic maps were constructed for generating pseudorandom numbers in [27]. Random sequences produced with chaotic maps have been mainly used to confuse and diffuse. A new chaotic map based on a discrete second-order memristor was designed in [28]. In addition, Wu et al. designed a circularly shifting chaotic map generation method [29]. He et al. designed discrete dual-memristor

chaotic maps for speech encryption in [30]. The two-dimensional coupled complex chaotic map was designed in [31]. Li et al. [32] constructed conditional symmetry in a chaotic map. A method for constructing high-dimensional chaotic maps was proposed in [33]. Bao et al. designed multicavity chaotic maps [34]. Wang et al. introduced a novel 2D Log-Logistic-Sine chaotic map in [35]. A 5D hyperchaotic mapping was constructed by combining a discrete memristor and discrete meminductor [36]. Yu et al. constructed a 5D fractional-order memristive hyperchaotic system (FOMHS) in [37]. A novel fractional-order hyperchaotic system was proposed in [38]. A Multiscroll Memristive Neural Network for image encryption was presented in [39–41]. A Multiscroll Hopfield Neural Network for video encryption was introduced in [42].

In order to achieve encryption efficacy, the chaotic neural network can use some very simple rules with low-computation complexity to encrypt medical images. The low computational complexity of chaotic neural networks can meet the fast medical request.

With the increasing complexity of chaotic systems, image encryption based on chaotic systems is becoming more and more secure. However, the existing full encryption technology in the spatial domain not only has high time complexity, but it also has no scalability. Full encryption is not suitable for applications that require various security levels, and it consumes a lot of resources in cloud storage and secure communications. On the contrary, selective encryption, which is possible for the most important wavelet coefficients encryption in the transform domain, can improve the encryption efficiency. In fact, both selective and full encryption schemes only concern communication/store security of the medical image. However, once the image is decrypted, there is no way to protect it. Decrypted images can be used maliciously. Image encryption only deters unauthorized access. Watermarking can control application and store of the plain medical image. Therefore, the decrypted images need to be constantly monitored to prevent illegal misuse. Actually, the decrypted images should be protected forever. As a copyright verification technology, digital watermarking can continuously monitor the use of images. Digital watermarking can prevent the illegal misuse of plaintext images.

Along with encryption, digital watermarking can protect the decrypted image in [43]. However, the existing image encryption and watermarking methods cannot ensure the medical security of the whole life cycle. Furthermore, existing joint encryption and watermarking schemes cannot meet real-time secure requests. Watermark detection cannot be performed in the encrypted domain; therefore, privacy will still be disclosed. In addition, current privacy protection methods have to face challenges on watermark embedding in the encrypted images and fast personalized secure medical service. For remote healthcare applications, medical image security at any time and fast sharing are becoming increasingly urgent. Compared to full encryption, selective encryption in the transform domain is scalable, and the encrypted content can be processed further.

To overcome the shortcomings of existing image security schemes and to meet the double security level request in smart healthcare systems, a joint selective encryption and watermarking (JEW) scheme is proposed. As a nonsymmetrical decomposition, SVD can be used for digital watermarking to trace decrypted medical images. Most important of all, it is also possible for the diffusion of image encryption for a higher level of security. DWT can help to lower the time complexity of the JEW algorithm. In the meantime, scrambling along with SVD diffusion can increase the security level.

The proposed scheme can provide a JEW scheme for balancing different security requirements and algorithm efficiency. The proposed scheme uses a chaotic neural network for permutation, as well as SVD and bitxor computing for diffusion. The proposed scheme can overcome the shortcomings of existing image security schemes and implement scalable operations on encrypted images. The main highlights are the following:

(1) The JEW scheme offers a technology of two-layer security for medical images. The watermark can be embedded/extracted in the encrypted domain to ensure privacy and security.
(2) The JEW scheme can provide fast requirements for content secure sharing in smart healthcare systems.
(3) A controllable security level based on selective encryption can be designed for smart healthcare systems.

The other chapters of the work are as follows. Section 2 introduces the basic theory used in the work. Section 3 primarily describes the proposed secure idea and the detailed process. Section 4 shows simulation results and security evaluation. Section 5 concludes the work.

2. Basic Theory of the Proposed Scheme

2.1. The DWT

The DWT, which has received considerable attention, is a signal-processing application, including image watermarking. The main idea of DWT is multiresolution, which involves the hierarchical decomposition of a signal. Through the DWT, the medical image decomposition in frequency channels can be implemented with a multistage repeat transformation. A medical image can be decomposed as LL, HL, LH, and HH sub-band at level 1 in the DWT domain, where LL stands for the coarse-level coefficients, which include most information of the original medical image. On the other hand, LH, HL, and HH have the detail coefficients. All of them can further be decomposed to the next level of similar four sub-bands. Because human eyes are sensitive to the coarse-level part, watermark information is usually embedded into the detail coefficients of the HL, LH, and HH sub-bands to obtain better visual quality. In this paper, the watermark image has been embedded into the HL and LH sub-bands.

For a medical image A, Equation (1) shows its DWT transform process:

$$\begin{aligned} G_{LL}(N) &=< A \bullet LL_N > \\ G_{LH}(N) &=< A \bullet LH_n >, i = 1, \ldots, N \\ G_{HL}(N) &=< A \bullet HL_n >, i = 1, \ldots, N \\ G_{HH}(N) &=< A \bullet HH_n >, i = 1, \ldots, N \end{aligned} \tag{1}$$

where A is a medical image, and LL_i, LH_i, HL_i, and HH_i are sub-bands.

2.2. Singular-Value Decomposition

For a matrix, SVD is an important matrix decomposition with non-negative scalar entries [44]. Usually, a medical image is also a matrix. A given medical image A with size $M \times N$ can be divided with SVD. SVD can be shown as follows:

$$A = USV^T \tag{2}$$

Then, $A = USV^T$, where matrices U and V have orthonormal columns, and they are orthogonal matrices. U is also called the left singular vectors of image A, whereas V is its right singular vectors. Both of them are known as the left and right singular vectors of A. On the other hand, U and V satisfy

$$I_M = UU^T = U^TU \tag{3}$$

$$I_N = VV^T = V^TV \tag{4}$$

S is a real non-negative diagonal matrix. All the main diagonal elements in S arranged in descending order are not zero. All these nonzero elements are called singular values. S is a diagonal matrix with size $M \times N$ it is also called a singular-value matrix. Because traditional SVD-based watermarking schemes only hide a watermark into the coefficients of the diagonal matrix S, those schemes suffer from false-positive problems [45].

In order to avoid the false-positive problem, the proposed watermarking method divides the watermark image into two parts: $W = W_1 + W_2$, where W_k denotes half of the watermark image. The principal component of them is embedded into the HL and LH sub-bands of the cover image respectively.

$$W_k = U_{W_k} S_{W_k} V_{W_k}^T, \qquad k = 1, 2. \tag{5}$$

$$WP_k = U_{W_k} S_{W_k}, \qquad k = 1, 2. \tag{6}$$

$$WP_k = U_{WP_k} S_{WP_k} V_{WP_k}^T, \qquad k = 1, 2. \tag{7}$$

Here, $S_{WP_k}, k = 1, 2$ are embedded into the HL and LH sub-bands of the cover image.

2.3. Secure Hash Algorithm (SHA-3)

SHA-3 is a secure hash function [46]. Compared to MD5, SHA-1, and SHA-2, SHA-3 is more secure. SHA-3, which is sensitive to the input information, can hash any type of message with different lengths to a fixed length of 256/512-bit hash values. In this work, the proposed encryption scheme uses a 256-bit hash value. Through SHA-3 computing, given any type of message, all hash values can ensure the consistency and integrity of the input message. For SHA-3, even if the original input information has changed a tiny bit, the new returned hash result will be different from the original hash result. At the same time, it can authenticate encryption and generate pseudorandom numbers. SHA-3 is a widely used hash function [46]. Furthermore, because the computing is based on bit-level operations, its time performance is superior. Because SHA-3 is sensitive to the initial message and can process messages with any size to a fixed length, it often is used to generate keys.

2.4. Chaotic System

The 4D hyperchaotic map can show the chaotic characteristic. Based on the chaotic characteristic, the chaotic system can be used to encrypt images. The 4D hyperchaotic system [47] is defined as follows:

$$\begin{cases} \dot{y}_1 = a(y_2 - y_1) - b y_2 y_3 + y_4 \\ \dot{y}_2 = y_1(1 - c y_3) \\ \dot{y}_3 = y_1 y_2 - d \\ \dot{y}_4 = -y_1 - y_2 \end{cases} \tag{8}$$

where the controls parameters are $a, b, c, d \in (0, +\infty)$, $y_i \in (0, 1)$, and $i = 1, 2, 3, 4$. The 4D hyperchaotic map can show chaotic characteristics. The above 4D hyperchaotic system can exhibit periodic and hyperchaotic behavior.

The 2D Hénon–Sine map (2D-HSM) is also a chaotic map; it can generate more complicated trajectories through a wider chaotic range. Therefore, its chaotic outputs are more random and unpredictable [48]. It is as follows:

$$\begin{cases} u_{n+1} = (1 - p \sin^2(u_n) + v_n) \bmod 1 \\ v_{n+1} = q u_n \bmod 1 \end{cases} \tag{9}$$

where p and q are two controls parameters, and for both of them, $\in (-\infty, +\infty)$. u_0 and v_0 are the initial values; $u_0 \in (0,1)$ and $v_0 \in (0,1)$. When all four parameters are in their value range, the 2D-HSM system will be chaotic.

The Hopfield Neural Network system is used to recognize or even to control the dynamics. The classical 3D Hopfield Neural Network (HNN) model is also a chaotic system because it can emulate dynamic behaviors. It can be ensured that the Hopfield neural network system [49] can also show chaotic characteristics. The 3D Hopfield Neural Network model is defined as follows:

$$\begin{cases} x_1' = -x_1 + 2f(x_1) - f(x_2) \\ x_2' = -x_2 + 1.7f(x_1) + 1.7f(x_2) + 1.1f(x_3) \\ x_3' = -x_3 - 2.5f(x_1) - 2.9f(x_2) + 0.56f(x_3) \end{cases} \tag{10}$$

$$f(x_i) = \tanh(x_i) \quad i = 1,2,3 \tag{11}$$

where $f(x_i)$ is the tangent function. The tangent function tanh can be used to design a Multiscroll Memristive Neural Network, which can be applied in image encryption.

In this paper, all three chaotic systems have been used to produce chaotic sequences to permut or diffuse the wavelet coefficients. The combination of these chaotic mappings can not only increase the key space but also provide different levels of security solutions in the DWT domain.

To verify the randomness of chaotic sequences, NIST SP800-22 was used [17]. We conducted numerous experiments based on NIST SP800-22 to further demonstrate the excellent randomness of the sequences produced by chaotic maps used in the work. Table 1 lists the related data obtained from the experimental results. According to Table 1, the p-value is significantly higher than the required confidence probability (0.01) for each statistical item. This once again proves that the used chaotic maps possess excellent randomness. Therefore, the proposed chaotic maps are highly suitable for image encryption.

Table 1. NIST randomness experiment results.

Statistical Item	***p*-Value**									**Result**
	$y_1(i)$	$y_2(i)$	$y_3(i)$	$y_4(i)$	u_i	v_i	$x_1(i)$	$x_2(i)$	$x_3(i)$	
Frequency Test (Monobit)	0.3821	0.3790	0.1280	0.2914	0.9278	0.4830	0.1540	0.3085	0.6146	Pass
Frequency Test within a Block	0.8319	0.6995	0.7365	0.1566	0.1736	0.0328	0.2912	0.8646	0.4244	Pass
Run Test	0.3765	0.5742	0.2197	0.7695	0.9954	0.2815	0.0506	0.7418	0.9478	Pass
Longest Run of Ones in a Block	0.7951	0.1923	0.7277	0.3258	0.6092	0.9231	0.1472	0.8116	0.3181	Pass
Binary Matrix Rank Test	0.1625	0.7279	0.1899	0.3522	0.5681	0.4456	0.1793	0.2066	0.2477	Pass
Discrete Fourier Transform (Spectral) Test	0.0733	0.2176	0.4594	0.9276	0.9482	0.5505	0.3303	0.2588	0.4753	Pass
Nonoverlapping Template Matching Test	0.7645	0.9071	0.9412	0.5703	0.9664	0.7229	0.1479	0.8534	0.0353	Pass
Overlapping Template Matching Test	0.4890	0.2783	0.8506	0.6160	0.1324	0.2412	0.1266	0.1675	0.5191	Pass
Maurer's Universal Statistical Test	0.8240	0.5062	0.3768	0.6408	0.4063	0.3342	0.8834	0.2349	0.2201	Pass
Linear Complexity Test	0.4544	0.5478	0.6383	0.8841	0.6421	0.9823	0.0435	0.4829	0.5291	Pass
Serial Test 1	0.4004	0.9097	0.3678	0.3846	0.0948	0.1023	0.4922	0.8292	0.3232	Pass
Serial Test 2	0.6459	0.9579	0.3531	0.1577	0.0809	0.0423	0.4317	0.9838	0.0544	Pass
Approximate Entropy Test	0.2644	0.8334	0.3689	0.5422	0.2658	0.7581	0.1156	0.5744	0.9836	Pass
Cumulative Sums (Forward) Test	0.6936	0.3463	0.1078	0.2811	0.8811	0.3490	0.2982	0.1604	0.9788	Pass
Cummulative Sums (Reverse) Test	0.4293	0.6619	0.2484	0.2244	0.9427	0.5550	0.2582	0.5673	0.7255	Pass
Random Excursions Test ($x = -1$)	0.3502	0.3503	0.1766	0.9909	0.8520	0.6111	0.3880	0.2565	0.0510	Pass
Random Excursions Test ($x = +1$)	0.7567	0.1183	0.7083	0.6772	0.9389	0.8434	0.3755	0.6420	0.5518	Pass
Random Excursions Variant Test ($x = -1$)	0.5074	0.4670	0.8161	0.9594	0.3271	0.8186	0.4095	0.7835	0.3819	Pass
Random Excursions Variant Test ($x = +1$)	0.4105	0.4132	1.0000	0.3338	0.3400	0.7964	0.5258	0.6802	0.4662	Pass

2.5. Combination of Encryption and Watermarking Technology

The proposed privacy protection scheme in Figure 1 is based on the JEW. Medical image secure sharing should be ensured as long as it lies in the smart healthcare system. Although medical image encryption can provide privacy protection in the communication stage, once the encrypted one is decrypted, the decrypted medical image is not protected. To protect the plain text of the image, watermark information is the second way to protect the decrypted content.

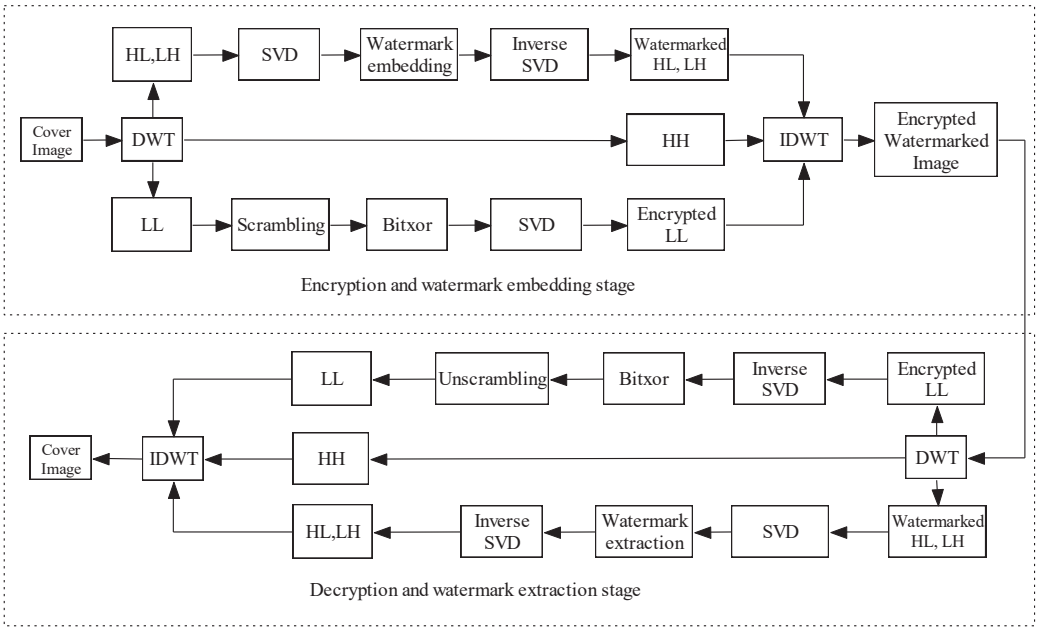


Figure 1. The proposed security scheme.

Digital watermarking and encryption can be applied to the proposed privacy protection scheme. Therefore, the proposed method can provide continuous image security for smart healthcare systems. The former embeds watermark information into the medical images. The second conducts an encryption operation; it can be part encryption or full encryption. For part encryption, only the key content is chosen to encrypt. As for the latter, which can also provide privacy protection, all content is encrypted. How to provide the actual medical image security in smart healthcare systems and meet real-time requirements at the same time is not easy. Because of resource-constrained medical devices in smart healthcare systems, it is difficult to strike a balance between privacy protection and performance. Undoubtedly, privacy protection for smart healthcare systems is very challenging. Understanding privacy protection requests and real-time requirements of smart healthcare systems may play an essential role.

3. The Proposed Scheme

Medical image sharing with a controllable security level becomes increasingly urgent in smart healthcare systems, which distribute medical images with privacy protection. Thus, privacy protection properties such as information confidentiality and image verification should be provided in smart healthcare systems. Encryption can ensure confidentiality. However, encryption provides no protection once the protected image is decrypted. Image verification can be provided with digital watermarking. Therefore, how to combine encryption and watermarking for image security in smart healthcare systems is very important.

The proposed security method will be introduced carefully. First, the medical image is encrypted with SVD computing and chaotic maps, and then the watermarking method

is discussed. The watermarking algorithm should concern the visual effect. Both medical image encryption and watermarking are performed based on SVD computing in the DWT domain. For an accurate diagnosis, the watermarked medical images should not be affected. The proposed JEW scheme is shown in Figure 2. First, we perform DWT on the original medical image. Second, we encrypt the LL sub-band and embed the watermark information into middle-frequency sub-bands. Finally, SVD diffusion will be operated according to the specific privacy protection request. We describe the proposed model with Algorithm 1 as follows:

Algorithm 1: The JEW algorithm

Input: original medical image, I
Output: encrypted and watermarked medical image, I^{JEW}

1 Permut and hash I to get the initial keys
2 For I, perform DWT to get $I_{LL}, I_{LH}, I_{HL}, I_{HH}$, $I \Rightarrow \{I_{LL}, I_{LH}, I_{HL}, I_{HH}\}$.
3 Perform SVD to LH and HL sub-bands, $LH = U_{LH} S_{LH} V_{LH}^T$, $HL = U_{HL} S_{HL} V_{HL}^T$.
4 Watermark embedding, $S_{LH}^W = S_{LH} + \lambda W_{LH}$, $S_{HL}^W = S_{HL} + \lambda W_{HL}$.
5 Permute the LL subband with 2D-HSM.
6 Diffuse the selective subbands with chaotic sequences $R_i = U_{R_i} S_{R_i} V_{R_i}^T$, where
$$i = 1,2,3.\ LL^{PE} = \begin{cases} U_{R_i} LL^P V_{R_i}^T, & M \le N \\ V_{R_i} LL^P U_{R_i}^T, & M > N \end{cases}.$$
7 Perform bitxor operation to the watermarked and permuted sub-bands,
$\boldsymbol{C_m}'(i,j) = \text{bitxor}(\boldsymbol{A_m}(i,j), \boldsymbol{I_k}(i,j))$, where $k = \{LL, LH, HL, HH\}$,
$i = \{1,2,3,\ldots,M/2\}$, $j = \{1,2,3,\ldots,N/2\}$.
8 Perform IDWT to get the encrypted and watermarked medical image I^{JEW}.

Algorithm 1 displays the pseudocode for the security procedure. The working of Algorithm 1 is explained in detail here.

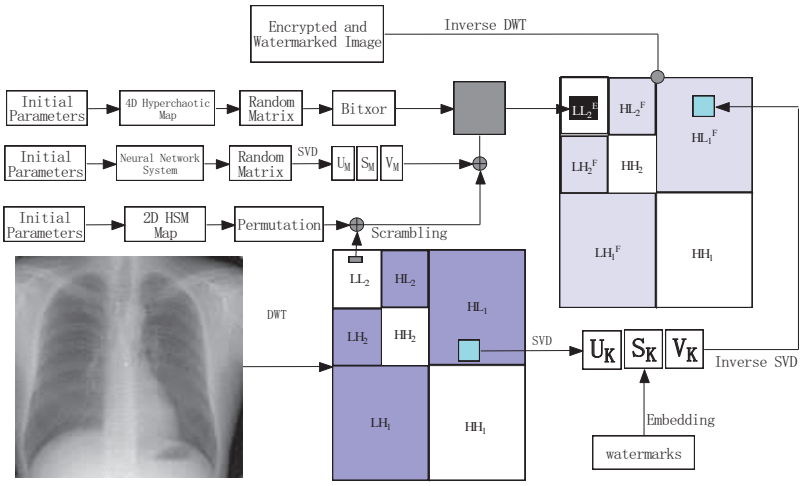


Figure 2. The proposed JEW scheme.

Image encryption in the paper is mainly based on the Hopfield Neural Network and chaotic maps. Selective encryption is efficient due to the low time complexity. However, the security level of privacy protection may be not high. To realize the controllable security level, an encryption method based on the Hopfield Neural Network and SVD has been proposed, as shown in Figure 2. First, the key is produced based on 2D-HSM. Perform DWT to the original image. Second, the approximation coefficient is selected for permutation. HL and LH sub-bands are chosen to embed watermarks based on SVD. In the end, the medical image is encrypted totally by SVD computing and bitxor computing. The joint of

permutation and diffusion operation has two steps: confusion based on chaotic sequence and diffusion based on SVD computing and bitxor computing. The joint watermarking and encryption method consists of three parts: keystream generation, coefficient permutation and watermarking, and coefficient diffusion.

3.1. Keystream Generation

The SHA-3 hash function, which possesses sensitivity to initial values, can resist plaintext attacks. It can generate an irreversible sequence. The original medical image I and SHA-3 function are used to compute initial values and control parameters for chaotic maps. Due to the sensitivity of initial values, the hash results can vary significantly between different images. Thus, the security of encryption can be enhanced significantly.

Step 1: Permute the original medical image I with 2D-HSM to obtain the permuted vector I^P, and change I^P into a 1D vector H^P. SHA-3 is used to hash H^P; then, a 128-bit hash value is generated.

Step 2: Assume V is the hash value of H^P. V is segmented into eight V_1, V_2, …, V_8, which are 16-bit. Values x_1, x_2, x_3, y_1, y_2, y_3, y_4 and parameters a, b, c, and d can be produced according to eight V_1 , V_2, …, V_8.

$$x_1 = \frac{V_1}{2^{17}}, x_2 = \frac{V_2}{2^{17}}, x_3 = \frac{V_3}{2^{17}} \tag{12}$$

$$y_1 = \frac{V_5}{2^{17}}, y_2 = \frac{V_6}{2^{17}}, y_3 = \frac{V_7}{2^{17}}, y_4 = \frac{V_8}{2^{17}} \tag{13}$$

$$\begin{cases} a = (\frac{V_1}{2^{17}} + \frac{V_2}{2^{17}})/2 \\ b = (\frac{V_3}{2^{17}} + \frac{V_4}{2^{17}})/2 \\ c = (\frac{V_5}{2^{17}} + \frac{V_6}{2^{17}})/2 \\ d = (\frac{V_7}{2^{17}} + \frac{V_8}{2^{17}})/2 \end{cases} \tag{14}$$

3.2. Coefficient Permutation and Watermarking

The key approximation coefficient is selected for permutation. HL and LH sub-bands are chosen to embed watermarks based on SVD.

Step 3: Given an image I with size $M \times N$, perform the discrete wavelet transform. Four sub-bands, LL, HL, LH, and HH, can be produced. The LL sub-band can be further decomposed into the second-level DWT transform.

Step 4: Perform SVD to LH and HL sub-bands for watermark embedding.

$$LH = U_{LH} S_{LH} V_{LH}^T \tag{15}$$

$$HL = U_{HL} S_{HL} V_{HL}^T \tag{16}$$

Step 5: Permute the LL sub-band with 2D-HSM to obtain the permuted matrix LL^P. The watermark information was embedded into the S_{LH} and S_{LH} as follows:

$$S_{LH}^W = S_{LH} + \lambda W_{LH} \tag{17}$$

$$S_{HL}^W = S_{HL} + \lambda W_{HL} \tag{18}$$

where λ is the information embedding strength, and $W_{LH} = S_{WP_1}$ and $W_{HL} = S_{WP_2}$, are both principal components of the original watermark information.

3.3. Coefficient Diffusion

The permuted and watermarked coefficients are encrypted totally by SVD computing and bitxor computing for security enhancing.

Step 6: To increase the security level, SVD inverse computing can diffuse the selective sub-bands using the neural network system to produce three random sequences R_i. Perform SVD of R_i; then, $R_i = U_{R_i} S_{R_i} V_{R_i}^T$, where $i = 1, 2, 3$.

Step 7: Diffuse the selective sub-band with U_{R_i} and $V_{R_i}^T$ as follows:

$$LL^{PE} = \begin{cases} U_{R_i} LL^P V_{R_i}^T, & M \le N \\ V_{R_i} LL^P U_{R_i}^T, & M > N \end{cases} \tag{19}$$

$$LH^{PE} = \begin{cases} U_{R_i} LH_W V_{R_i}^T, & M \le N \\ V_{R_i} LH_W U_{R_i}^T, & M > N \end{cases} \tag{20}$$

$$HL^{PE} = \begin{cases} U_{R_i} HL_W V_{R_i}^T, & M \le N \\ V_{R_i} HL_W U_{R_i}^T, & M > N \end{cases} \tag{21}$$

where LH_W and HL_W are watermarked LH and HL sub-bands.

Step 8: The 4D hyperchaotic system is used to generate four initial matrices randomly, which are called A_1, A_2,A_3, and A_4. Then, the matrices A_m, and $m = 1, 2, 3, 4$ are used for diffusion operation for the watermarked and permuted sub-bands, respectively.

$$\boldsymbol{C_m}'(i,j) = \text{bitxor}(\boldsymbol{A_m}(i,j), \boldsymbol{I_k}(i,j)) \tag{22}$$

where $k = \{LL, LH, HL, HH\}$, $i = \{1, 2, 3, \ldots, M/2\}$, $j = \{1, 2, 3, \ldots, N/2\}$.

Step 9: The encrypted and watermarked medical image I^{JEW} can be obtained with IDWT. Perform IDWT on $C_m{}'(i,j), m = 1, 2, 3, 4$ to obtain I^{JEW}, where $C_m (m = 1, 2, 3, 4)$ are the encrypted LL sub-band, encrypted and watermarked HL sub-band, encrypted and watermarked LH sub-band, and encrypted HH sub-band.

The process used for decryption and watermark information extraction is just the opposite of the proposed JEW algorithm and is described in Algorithm 2 and Algorithm 3, respectively. The decrypted process is as follows.

Step 1: Obtain encrypted and watermarked image I^{JEW}, and perform DWT on I^{JEW}. Then, encrypted and watermarked subbands $I_{LL}^{JEW}, I_{LH}^{JEW}, I_{HL}^{JEW}, I_{HH}^{JEW}$ can be obtained. $I^{JEW} \Rightarrow \{I_{LL}^{JEW}, I_{LH}^{JEW}, I_{HL}^{JEW}, I_{HH}^{JEW}\}$.

Step 2: Perform bitxor operation to the watermarked and permuted sub-bands, for example, $\boldsymbol{I_k}(i,j)) = \text{bitxor}(\boldsymbol{A_m}(i,j), \boldsymbol{C_m}'(i,j)$, where $k = \{LL, LH, HL, HH\}$, $i = \{1, 2, 3, \ldots, M/2\}$, $j = \{1, 2, 3, \ldots, N/2\}$.

Step 3: Obtain the reverse diffused sub-band with inverse SVD computing: $LL^P = \begin{cases} U_{R_i}^T LL^{PE} V_{R_i}, & M \le N \\ V_{R_i}^T LL^{PE} U_{R_i}, & M > N \end{cases}$.

Step 4: Obtain the reverse permuted the LL sub-band with 2D-HSM.

Step 5: Perform IDWT on $I_{LL}, I_{LH}^W, I_{HL}^W, I_{HH}$ to obtain the watermarked medical image I^W.

The watermark detection can be performed in the encrypted domain. The main process is as follows.

Step 1: Obtain encrypted and watermarked image I^{JEW}, perform DWT on I^{JEW}. Then, encrypted and watermarked sub-bands $I_{LL}^{JEW}, I_{LH}^{JEW}, I_{HL}^{JEW}, I_{HH}^{JEW}$ can be obtained. $I^{JEW} \Rightarrow \{I_{LL}^{JEW}, I_{LH}^{JEW}, I_{HL}^{JEW}, I_{HH}^{JEW}\}$.

Step 2: Perform bitxor operation to the watermarked and permuted sub-bands, for example, $\boldsymbol{I_k}(i,j)) = \text{bitxor}(\boldsymbol{A_m}(i,j), \boldsymbol{C_m}'(i,j)$, where $k = \{LL, LH, HL, HH\}$, $i = \{1, 2, \ldots, M/2\}$, $j = \{1, 2, \ldots, N/2\}$.

Algorithm 2: The decryption algorithm

Input: Encrypted medical image, I^{JEW}
Output: Watermarked medical image, I^{W}
1 For I^{JEW}, perform DWT to obtain $I_{LL}^{JEW}, I_{LH}^{JEW}, I_{HL}^{JEW}, I_{HH}^{JEW}$, $I^{JEW} \Rightarrow \{I_{LL}^{JEW}, I_{LH}^{JEW}, I_{HL}^{JEW}, I_{HH}^{JEW}\}$.
2 Perform bitxor operation to the watermarked and permuted sub-bands, $\boldsymbol{I_k}(i,j)) = \text{bitxor}(\boldsymbol{A_m}(i,j), \boldsymbol{C_m}'(i,j)$, where $k = \{LL, LH, HL, HH\}$, $i = \{1,2,\ldots,M/2\}, j = \{1,2,\ldots,N/2\}$.
3 Get the reverse diffused sub-band with inverse SVD computing,
$$LL^{P} = \begin{cases} U_{R_i}^{T} LL^{PE} V_{R_i}, & M \leq N \\ V_{R_i}^{T} LL^{PE} U_{R_i}, & M > N \end{cases}.$$
4 Obtain the reverse permuted the LL sub-band with 2D-HSM.
5 Perform IDWT on $I_{LL}, I_{LH}^{W}, I_{HL}^{W}, I_{HH}$ to obtain the watermarked medical image I^{W}.

Step 3: Perform SVD to LH^{W} and HL^{W} sub-bands $LH^{W} = U_{LH} S_{LH}^{W} V_{LH}^{T}$, $HL^{W} = U_{HL} S_{LH}^{W} V_{HL}^{T}$.

Step 4: Watermark information extraction to obtain $S_{WP_k}, k = 1,2$. $W_{LH} = (S_{LH}^{W} - S_{LH})/\lambda$ and $W_{HL} = (S_{HL}^{W} - S_{HL})/\lambda$, where $S_{WP_1} = W_{LH}$ and $S_{WP_2} = W_{HL}$.

Step 5: Perform $WP_k = U_{W_k} S_{W_k} = U_{WP_k} S_{WP_k} V_{WP_k}^{T}$ and $W_k = U_{W_k} S_{W_k} V_{W_k}^{T}$ to obtain watermark image.

Algorithm 3: The watermark extraction algorithm

Input: Encrypted medical image, I^{JEW}
Output: Watermark, I^{W}
1 For I^{JEW}, perform DWT to obtain $I_{LL}^{JEW}, I_{LH}^{JEW}, I_{HL}^{JEW}, I_{HH}^{JEW}$, $I^{JEW} \Rightarrow \{I_{LL}^{JEW}, I_{LH}^{JEW}, I_{HL}^{JEW}, I_{HH}^{JEW}\}$.
2 Perform bitxor operation to the watermarked and permuted sub-bands, $\boldsymbol{I_k}(i,j)) = \text{bitxor}(\boldsymbol{A_m}(i,j), \boldsymbol{C_m}'(i,j)$, where $k = \{LL, LH, HL, HH\}$, $i = \{1,2,3,\ldots,M/2\}, j = \{1,2,3,\ldots,N/2\}$.
3 Perform SVD to LH^{W} and HL^{W} sub-bands, $LH^{W} = U_{LH} S_{LH}^{W} V_{LH}^{T}$, $HL^{W} = U_{HL} S_{LH}^{W} V_{HL}^{T}$.
4 Watermark information extraction to obtai $S_{WP_k}, k = 1,2$. $W_{LH} = (S_{LH}^{W} - S_{LH})/\lambda$, $W_{HL} = (S_{HL}^{W} - S_{HL})/\lambda$, where $S_{WP_1} = W_{LH}$ and $S_{WP_2} = W_{HL}$.
5 Perform $WP_k = U_{W_k} S_{W_k} = U_{WP_k} S_{WP_k} V_{WP_k}^{T}$, and $W_k = U_{W_k} S_{W_k} V_{W_k}^{T}$ to obtain watermark image.

4. Experiment Results and Discussion

Related simulation results and security analysis are shown in the following. In these experiments, some classic medical images were used as the original test images. They are 256 gray-level medical images, which include MRI, CT scan, X-Ray, and Ultrasound. Both JEW operation and decryption process were performed on a Windows 11 operating system with Pentium(R) Dual-Core i5-10500 CPU, and 16GB of RAM, and the software platform used is MATLAB R2022a. In order to show the effectiveness of the JEW, the experiment results were evaluated. The evaluation of image security used the following parameters: Number of Pixel Change Rate (NPCR) and Uniform Average Change Intensity (UACI), Peak Signal-to-Noise Ratio (PSNR), Correlation Coefficient (NC), and Entropy.

In Figure 3, (a) lists some original medical images, (b) exhibits their corresponding encrypted image, (c) shows their decrypted medical images. According to those encrypted ones in Figure 3b, it is difficult to know what the original medical image looks like. Accord-

ing to Figure 3c, with the key, those encrypted images can be decrypted as watermarked images. The proposed scheme can protect the privacy of medical images.

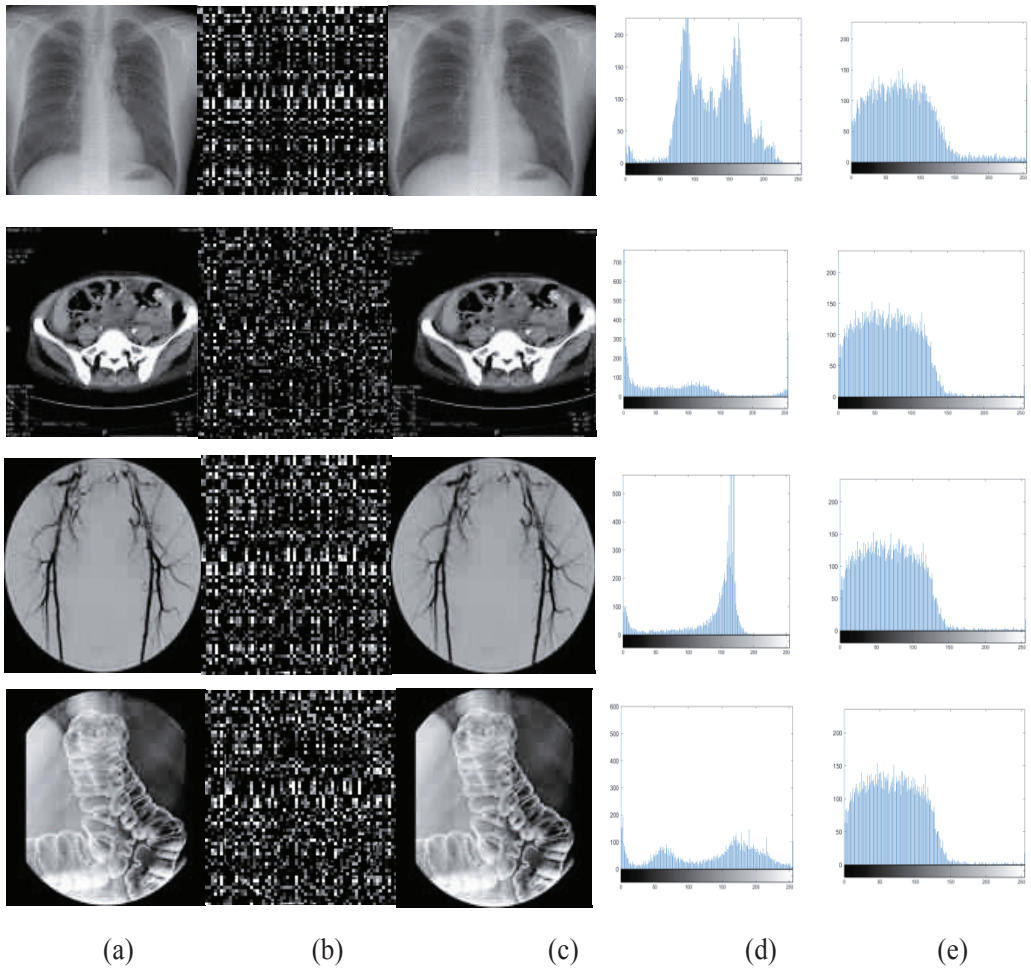


Figure 3. Encryption results: (**a**) original images, (**b**) encrypted images, (**c**) decrypted and watermarked images, (**d**) original histograms, (**e**) encrypted histograms.

4.1. Perceptual Effect

Generally speaking, it should not be possible to see the original content of the encrypted object in order to maintain confidentiality for secure sharing. The watermark information hidden in the images should not be perceived. The watermarked medical images' visual quality should not be affected by the watermark embedding. The HSM chaotic map is first used to permute the LL sub-band in the proposed technique. The proposed approach initially permutes the LL sub-band using the HSM chaotic map. The middle sub-bands, such as LH and HL, are then selected to be embedded in the watermark information by altering the singular values of their respective matrices. Finally, the permuted and watermarked content is disfused using SVD computation and bitxor operations. Figure 3 displays the encrypted and decrypted results. All encrypted images were not percieved. Their visual quality was quite bad. Figure 3b does not reveal the original information. As a result, the proposed technique can have a strong perceptual effect.

Watermark information is contained in the LH and HL sub-bands, whereas the LL sub-band's wavelet coefficients are confused and then diffused. Figure 3c shows the watermarked results. Figure 3c shows that watermarked images appear to be unchanged from their original counterparts. To have verification capabilities later, it should not be

possible to detect any watermark information from decrypted images. Figure 3c shows that the watermark is not visible in decrypted or watermarked images. The watermarked medical images have the same visual quality as the original medical image.

Watermark information is concealed in the LH and HL sub-bands to achieve invisibility. The hidden watermark should not reduce the quality of the image. The visual quality of the encrypted medical images was unaffected by the proposed watermarking approach when compared to the originals. Watermark information embedding into the middle sub-bands when the coefficients in the LL sub-band are confused can reduce the computational complexity of the suggested JEW method. A fast security request can be achieved.

4.2. Ability to Resist Exhaustive Attack

A image encryption algorithm should be resistant against exhaustive attacks. The proposed encryption method involves confusion for the LL sub-band and diffusion for the LL, LH, and HL subbands. To assure a large key space, the authors employed chaotic neural network systems, 4D chaotic map, and 2D-HSM for image encryption. These systems have initial values and control parameter sensitivity properties. The keys were mostly utilized for permutation and diffusion. All of them belonged to the key space. As a result, the keys included their starting values u, v, x_1, x_2, x_3, y_1, y_2, y_3, and y_4, as well as control parameters a, b, c, d, p, and q. The sensitivity of keys was 10^{-15}, while the entire key space was $10^{15\times15} = 10^{225}$. Therefore, the proposed scheme has a very large key to resist a brute-force attack.

4.3. Histogram Analysis

To evaluate the encryption effect, statistical attack should be analyzed. Statistical attacks include histogram analysis. For different original medical images, an effective encryption method should have similar encrypted results, wherein all of them have uniform histograms. Some important content is selected to encrypt in the proposed JEW scheme. The encryption scheme is effective if those different encrypted images have similar visual results.

In this work, image encryption was based on confusion and diffusion of important wavelet coefficients. For all encrypted images, their gray histograms should be fairly uniform. If encrypted histograms are different from their corresponding original gray histograms, the encryption method is regarded as perfect. In Figure 3d,e, the original histograms and the corresponding encrypted histograms are shown, respectively. From Figure 3d, it is apparent that the original histograms are different; however, all the histograms of their corresponding encrypted images are similar, and the similar encrypted histograms are different from their original ones from Figure 3e. Therefore, histogram analysis shows the medical image encryption scheme can resist statistical attacks.

4.4. Information Entropy Analysis

In the following equation is described information entropy of the image:

$$H(m) = -\sum_{i=0}^{L} P(m_i)\log_2 P(m_i) \tag{23}$$

where m_i represents the ith gray value of an image, and $P(m_i)$ is the probability of the ith gray value; then,

$\sum_{i=0}^{L} P(m_i) = 1$. The information entropy value of an encrypted medical image should be different from the original medical image. The information entropy of those decrypted medical images is compared with that of their original images. The information entropy is shown in Table 2. In Table 2, (b) is the entropy of encrypted images in Figure 4b and

so are (c) and (d). Figure 4b–d show that all those encrypted images were not perceived. According to the entropy of original images, the information entropy of decrypted image is not apparently changed. The visual quality of those decrypted images has not been affected. Therefore, their visual metric is not decreased, although watermarks are hidden.

Table 2. Entropy.

Image No.	(a)	(b)	(c)	(d)	(e)
1	5.7615	7.3832	7.4264	7.9056	5.7615
2	5.7336	7.4245	7.3967	7.6865	5.7336
3	6.7269	7.2968	7.2965	7.8589	6.7269
4	6.3829	7.4510	7.2910	7.6912	6.3829
5	5.8691	7.6023	7.3703	7.8359	5.8619

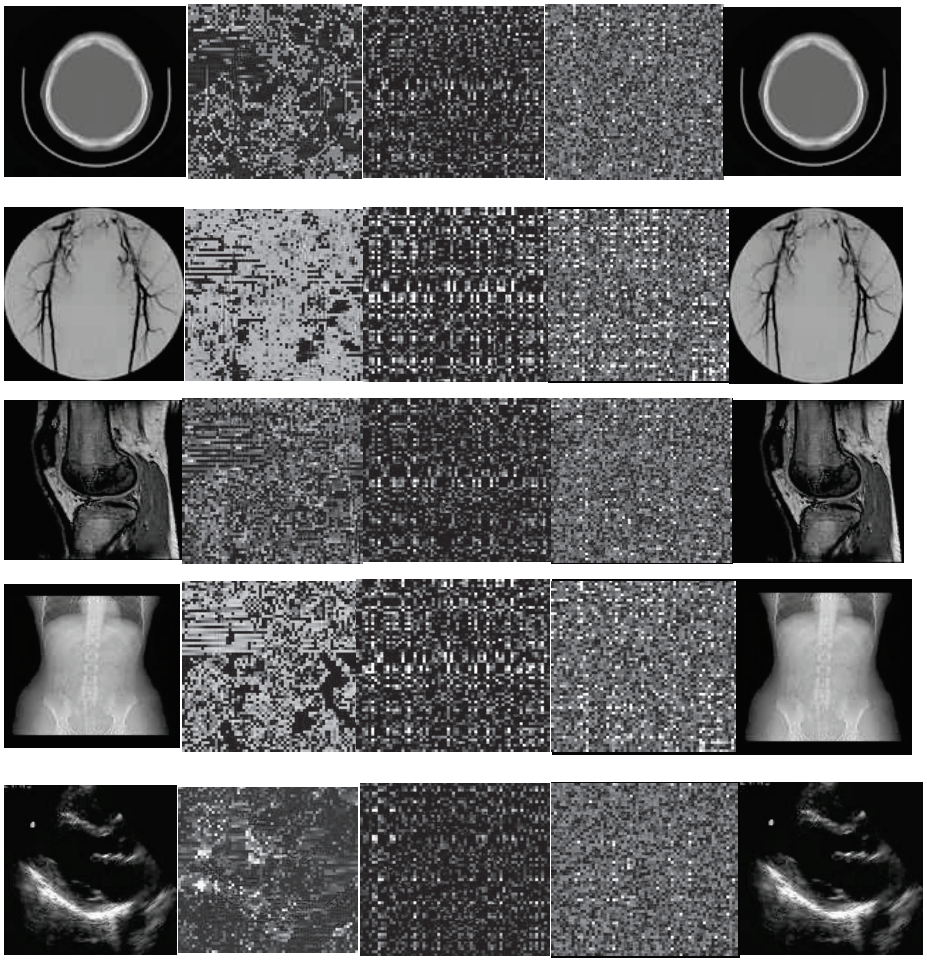


Figure 4. Discussion of the selective encryption: (**a**) original medical images, (**b**) permutation in the LL subband, (**c**) diffusion with SVD operation, (**d**) diffusion with bitxor operation, (**e**) decrypted images.

4.5. Differential Attack Analysis

Differential attack can be used to evaluate the change between the original pixels and the encrypted ones. NPCR and UACI are two main differential attack analysis methods. NPCR and UACI represent the number of change pixels between two encrypted images and the average change intensity between two encrypted images, respectively. Compared to those encrypted images and their corresponding original ones, the change between

them can be found. NPCR and UACI can be used to measure the difference between encrypted pixels and their original ones. NPCR and UACI can be calculated using the following equations:

$$C(i,j) = \begin{cases} 0, & if\ T_1(i,j) = T_2(i,j) \\ 1, & if\ T_1(i,j) \neq T_2(i,j) \end{cases} \tag{24}$$

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} C(i,j)}{M \times N} \times 100\% \tag{25}$$

$$UACI = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} ||T_1(i,j) - T_2(i,j)||}{M \times N \times 255} \times 100\% \tag{26}$$

where T_1 is an image, and T_2 is also an image. Both of them have sizes of M and N. $C(i,j)$, which is a bipolar array to be determined using Equation (24), has the same sizes of M and N as image T_1. NPCR reflects the proportion of pixels in the same position but not equal in two images to the total number of pixels in the image. UACI measures the change of the average intensity between the encrypted and the original. The higher the NPCR value, the better the encryption security performance, which means the pixels are dramatically randomized. UACI is the overall average change density, which mainly reflects the strength of the average change in the difference between the original image and its encrypted image. To evaluate the encryption performance, Table 3 lists the NPCR and UACI results. According to Table 3, the proposed encryption algorithm can resist differential attack.

4.6. PSNR

The PSNR is shown as follows:

$$PSNR(I_1, I_2) = 10log_{10}\left(\frac{\left[2^{dep} - 1\right]^2}{MSE(I_1, I_2)}\right) \tag{27}$$

$$MSE(I_1, I_2) = \frac{1}{L}\sum_{k=1}^{L}\left[I_1(k) - I_2(k)\right]^2 \tag{28}$$

where L presents the total pixel number of a medical image I, and k is the serial number. I_1 and I_2 are two different medical images, and dep, which equals 8, is the depth. $PSNR = 10 \times \log_{10}(255^2/MSE)$. The visual quality of images can be evaluated with the PSNR. Table 4 shows the PSNR for images in Figure 4. Figure 4a,e list the original images and watermarked images. In Table 4, (b) lists the PSNR of encrypted images in Figure 4b, as do (c), (d), and (e). From Table 4, the PSNR values of all encrypted images are below 30 dB. From Figure 4, all encrypted images can not disclose the original information. The decrypted watermarked images have high PSNR values. With the proposed joint encryption and watermarking method, the visual quality did not decrease.

Table 3. NPCR and UACI.

	NPCR			**UACI**		
	b	**c**	**d**	**b**	**c**	**d**
1	0.9955	0.9948	0.9936	0.3305	0.3315	0.3328
2	0.9947	0.9938	0.9949	0.3296	0.3321	0.3362
3	0.9939	0.9942	0.9936	0.3287	0.3314	0.3326
4	0.9958	0.9943	0.9939	0.3385	0.3397	0.3315
5	0.9947	0.9951	0.9942	0.3325	0.3308	0.3311

Table 4. PSNR.

Image	(b)	(c)	(d)	(e)
1	25.5329	25.5225	25.3674	78.3625
2	25.3658	25.3247	25.3241	76.2513
3	26.2891	25.1873	24.6872	76.3524
4	26.1502	25.2013	23.6855	73.2819
5	25.6987	24.4289	23.2864	75.9127

4.7. Encryption Process Discussion

In the proposed joint watermarking and encryption scheme, important coefficients are chosen to encrypt. The proposed selective encryption process is shown in Figure 2. The medical images from top to bottom in Figure 4 are numbered 1, 2, 3, 4, and 5, respectively. The LL sub-band was chosen to confuse. The encrypted results are shown in Figure 4b. The LL sub-band was permuted; here, the single coefficient was permuted in the LL sub-band. Only permutation in the LL sub-band could obtain unintelligible visual results. From Figure 4b, all permuted images are not perceptual.

Compared to the corresponding original medical image, the single-coefficient permutation for the LL sub-band only via the HSM chaotic map could achieve good effects. The corresponding encrypted images are shown in Figure 4b. Figure 4c,d show the encrypted results based on the diffusion of those encrypted images listed in Figure 4b. The diffusion was based on bitwise XOR computing and an inverse SVD multiply operation. Figure 4c shows the encrypted results when an inverse SVD operation was applied. From Figure 4c, the perceived quality is apparently decreased compared to that listed in Figure 4b. According to Figure 4b,c, it is apparent that an inverse SVD operation can increase the security level. The security level of Figure 4d is higher than that of Figure 4c. From the experimental results of Figure 4b–d, all of them were not able to obtain the visual information of the original images. Only the single-coefficient permutation in the LL sub-band took less time than the combination of permutation and diffusion. Therefore, from Figure 4b–d, the selective approach could meet different security requests in the smart healthcare system.

Therefore, if a higher security level is requested, the diffusion process is adopted. On the contrary, only the permutation operation can be applied, because the original information cannot be told in Figure 4b. For medical image encryption in smart healthcare systems, without detailed medical information, the diagnosis will not be accurate. The encrypted and watermarked images in Figure 4b make the perceptual quality unacceptable. Privacy will be ensured.

Therefore, the proposed watermarking and encryption methods can not only meet fast service requests but also ensure that the privacy of the image is not violated. If the selective permutation is broken, the broken operation is still not able to tell the original medical image information because the diffusion operation can still make the protected image is not intelligible.

Therefore, the proposed watermarking and encryption methods can not only meet fast service requests but also ensure that the privacy of the image is not violated. If the selective permutation is broken, the broken operation is still not able to tell the original medical image information because the diffusion operation can still make the protected image unintelligible.

4.8. Encryption and Watermarking Efficiency

For the security of smart healthcare systems, medical image encryption is essential. The balance of efficiency and privacy protection will be achieved to meet the special security request in smart healthcare systems. The efficiency of the proposed scheme JEW

was evaluated, where performance analysis has been discussed. There are many resource-constrained medical devices in the smart healthcare system with IoMT technology. For fast diagnosis in smart healthcare systems, if the proposed security scheme takes a large amount of time to encrypt and embed watermark information, then it will not be a good scheme for smart healthcare systems.

In the proposed method, performance is mainly affected by encryption and watermarking operations. The time efficiency has been analyzed and is shown in Table 5. All experiments were run on an Intel(R) Dual-Core i5 computer with the MATLAB R2022a software platform. Through Table 5, the total encryption and watermarking operation took about 1.2 s or so. However, the decryption operation only took 0.5 to 0.6 s. Thus, the security scheme is efficient. With the proposed security scheme, medical image security services can be provided, and time efficiency can meet strict real-time deadlines for smart healthcare systems. Table 5 shows the runtime of the related experiment in Figure 4. Those medical images are labeled 1, 2, 3, 4, and 5 from top to bottom.

Table 5. Algorithm efficiency(s).

Image	JEW	Decryption	Total
1	1.1200	0.547	1.6675
2	1.1598	0.586	1.7458
3	1.1945	0.595	1.7895
4	1.1986	0.592	1.7906
5	1.2035	0.579	1.7825

4.9. Encryption Comparison Analysis

The proposed JEW method was compared with related schemes. The considered techniques include encryption algorithms [50–52]. Because both encryption algorithms [50,51] were performed in the spatial domain, making it inefficient to encrypt and watermark all pixels. Their image protection schemes encrypt pixels for communication and storage stages only. They can only provide partial protection. Image encryption schemes in the spatial domain cannot provide a multilevel scalable security way for smart healthcare systems. A more comprehensive medical image privacy protection is not possible for encryption algorithms [50,51]. Their encryption algorithms have a high time complexity because of the full encryption. In addition, all security operations are performed in the spatial domain.

Image encryption algorithm in [50] consists of three steps. Firstly, a one-dimensional chaotic mapping is used to generate a chaotic matrix, and the image is divided into many blocks. Then, the values of the chaotic matrix are XORed with the values in each block. Secondly, use one-dimensional logical mapping to generate a pixel matrix that is equal in size to the length and width of the image, and shuffle the positions of the image pixels. Finally, generate a new chaotic matrix using the new initial values and perform an XOR operation with the blocks divided by the image. Diaconu et al. proposed a cyclic displacement and chaos encryption technique [51], which mainly consists of two steps. The first step is to convert the pixel values of the original image into an 8-bit binary array, count the number of 1s, and divide the count by 2 to find the remainder. If the remainder is 0, the binary array is cyclically shifted to the right by counting bits in the form of a linked list. If the remainder is 1, the binary array is cyclically shifted to the left by counting bits in the form of a linked list; The second step is to use logical mapping to generate two encryption matrices equal in size to the length and width of the image, and then perform two XOR operations with the pixel values of the three color components of the image to obtain the encrypted image.

Medical image security in smart healthcare systems is necessary for the privacy protection scheme, which should be scalable. A different security service request can be met with a scalable scheme. This scalability can be achieved when joint encryption and watermarking operations are conducted in the transform domain. The proposed JEW scheme can improve the performance problem through selective important content permutation and SVD diffusion. Wavelet decomposition makes all security operations perform in parallel. Apparently, the permutation and diffusion process in parallel will be faster than the encryption algorithms in [50,51]. In the proposed technique, SVD and bitxor diffusion operation can meet higher security requests in the smart healthcare system. SVD operation is also reversible, and the decryption will be fast. Table 6 lists the performance of the proposed security scheme and the methods in [50–52]. In comparison with the methods [50–52], the proposed encryption scheme took less time.

Table 6. Encryption analysis.

Image	Proposed		[50]		[51]		[52]	
	Entropy	Time(s)	Entropy	Time(s)	Entropy	Time(s)	Entropy	Time(s)
1	7.9056	0.6324	7.9997	48.3652	7.9997	182.693	4.8610	0.8223
2	7.6865	0.6189	7.9997	51.2581	7.9997	192.3542	4.6363	0.8256
3	7.8589	0.6253	7.9997	55.9128	7.9997	169.3257	4.6704	0.8239
4	7.6912	0.6171	7.9997	53.2187	7.9997	170.2561	4.8778	0.8268
5	7.8359	0.6128	7.9997	53.2187	7.9997	170.2561	4.4484	0.8247

With the proposed joint watermarking and encryption scheme, important coefficients were chosen to encrypt. The proposed selective scheme encryption process is shown in Figure 2. First, the LL sub-band was chosen to confuse. The encrypted results are shown in Figure 4. Here, the single coefficient was permutated in the LL sub-band. Only permutation in the LL subband could obtain unintelligible visual results. From Figure 4, all permuted images are not perceptual.

The proposed JEW scheme can improve the performance through selective permutation and SVD diffusion. Wavelet decomposition makes all security operations perform in parallel. The permutation and diffusion process in parallel will be fast. In the proposed scheme, SVD diffusion operation can meet higher security requests. SVD operation is also reversible, so the decryption will be fast.

We encrypted five images using the above methods and the method described in this article, and the result is shown in Table 6. From Table 6, it can be seen that the entropy values of the proposed algorithm are lower than algorithms in [50,51]. From the perspective of time complexity analysis, the algorithm proposed in this article only took 0.7 s, while Rostami's algorithm required 56 s, and Diaconu's algorithm had a computation time of up to 192 s. By comparing and analyzing the above two parameters, the algorithm proposed in this paper is significantly superior to the other two encryption algorithms in run time.

Table 7 compares the proposed approach with existing security schemes, i.e., the dual watermarking method [4], the secure medical image sharing scheme [52], digital watermarking [53], and the joint watermarking and encryption method [54]. In Table 7, the NPCR, UACI, PSNR, and entropy are analyzed. Because the key coefficients are encrypted, the NPCR and entropy values are lower than encryption schemes in the spatial domain. For secure methods in which all pixels are encrypted in the spatial domain, watermarking must needed to be conducted in the decrypted domain. Watermark embedding and extraction were mostly carried out in the transform domain of plaintext images. At last, the original information of the plaintext image could not be protected in the watermark embedding and extraction stage. With the joint watermarking and encryption scheme in this paper,

the encrypted part was different from the content that was to be watermarked. Therefore, watermark embedding and watermark detection could be conducted on the encrypted domain to avoid privacy disclosure. Although the proposed encryption scheme did not encrypt all pixels in the spatial domain, the average PSNR and UACI values outperformed most image security schemes in Table 7. Most important of all, different security level requirements could be met with the proposed image security scheme.

Table 7. Quantitative measurements comparison.

Average Value	Ours	[53]	[54]	[4]	[52]
Entropy	7.6988	7.9872	7.9921	7.9439	4.7583
PSNR	76.2543	56.3915	59.4128	49.2721	87.3521
NPCR	0.9947	0.9936	0.9987	0.9973	0.9621
UACI	0.3329	0.2725	0.2698	0.2691	0.2937

4.10. Secret Key Space Comparison

An effective image encryption scheme should have a large key space, which is enough to withstand brute force attacks. The size of the key space needs to be larger than 10^{31} [13]. The secret key in the proposed algorithm consists of nine initial values and six parameters of chaotic maps. If the computational accuracy is 10^{15}, the size of key space meets $10^{15\times15} > 10^{31}$. In addition, Table 8 shows the key space compared with that of several typical encryption schemes concerning key space. The comparison data show that the key space of the proposed scheme is larger than that of most encryption algorithms.

Table 8. Secret key space comparison.

Algorithm	Proposed	[55]	[13]	[17]	[52]	[14]
Key space	10^{225}	10^{210}	10^{60}	10^{70}	10^{150}	10^{120}

4.11. Watermarking Comparison Analysis

The algorithm proposed by Anand et al. is designed to perform DWT transform on the host image, select its horizontal and vertical components for singular value decomposition, and then divide the image watermark into two equal parts multiplied by an incremental factor K and added to two singular-value matrices. Then, the inverse transform is used to obtain the embedded watermark image [56]. The algorithm was used to embed and extract image watermarks for Image No. 1, Image No. 3, and Image No. 5 in Figure 4. We compared the watermark NC value with Anand's algorithm [56]. The data obtained are shown in Table 9. The algorithm exhibited good robustness in dealing with some attacks, which was better than the proposed algorithm. However, the algorithm's robustness in handling cropping attacks and noise attacks was not as good as the algorithm proposed in this paper. Both algorithms have their advantages, so different watermarking algorithms can be selected for embedding watermarks and fingerprints in different application fields.

Table 9. Watermark performance analysis.

Attack	Image No. 1		Image No. 3		Image No. 5	
	Proposed	**[56]**	**Proposed**	**[56]**	**Proposed**	**[56]**
No attack	0.9981	0.9935	0.9926	0.9581	0.9734	0.9629
Upper left corner cropping (1/16)	0.8524	0.6281	0.7925	0.3928	0.7659	0.4218
Center cropping (1/16)	0.6821	0.4519	0.7829	0.3128	0.7539	−0.0091
Around cropping (1 /8)	0.6825	−0.0358	0.7598	0.2305	0.8935	−0.3016
Salt & pepper (0.005)	0.8014	0.7567	0.8324	0.7158	0.8924	0.7928
Salt & pepper (0.01)	0.7632	0.6925	0.7519	0.6524	0.7521	0.6758
Salt & pepper (0.02)	0.6521	0.4320	0.7541	0.3698	0.7749	0.3575
Gaussian noise (0.001)	0.7532	0.7391	0.7921	0.7259	0.7531	0.7324
Gaussian noise (0.005)	0.6821	0.6369	0.6829	0.6755	0.6958	0.6595
Gaussian noise (0.01)	0.5369	0.4678	0.5726	0.4628	0.5960	0.5146

4.12. Image Security Scheme Discussion

These joint watermarking and encryption methods first embed the watermark and then encrypt the watermarked image [53,54,57]. Their watermarked image encryption methods are all performed in the spatial domain. These methods of encrypting the image embedded with watermark in the spatial domain are prone to privacy leakage. The encrypted and watermarked image needs to be decrypted first to extract the watermark information. These methods are not scalable, because they need to decrypt and then extract the watermark. However, the proposed JEW method can address this scalability problem. The proposed method can perform encryption and watermarking operations in the DWT domain in parallel. Most important of all, watermark information can be extracted in the encrypted domain. Extracting watermark information in the encrypted domain can avoid frequent encryption and decryption, and it can also achieve privacy protection.

Table 10 summarizes the roles of the proposed security method and some image security schemes such as the watermarking technique [53], joint encryption/watermarking algorithm [54], and the multilayer security scheme [57]. In Table 10, selective encryption means that only the important part, rather than the whole content, is encrypted. In contrast, RC4 represents a stream cipher algorithm.

Table 10. Comparisons of the related schemes.

	Ours	**[54]**	**[53]**	**[57]**
Watermarking	Yes	Yes	Yes	Yes
Selective encryption	Yes	No	No	No
Tracing	Yes	Yes	No	Yes
Scalability	Yes	No	No	No
Encryption domain	DWT	Spatial	Spatial	Spatial
Encryption scheme	Chaos	RC4	RC4	Chaos
Watermark domain	DWT	Spatial	Spatial	DWT/DCT
Watermark detection	Encrypted	Plaintext	Plaintext	Plaintext
Controllable security level	Yes	No	No	No
Total overhead (S)	1.7552	108.4726	162.3524	29.6545

The existing image security schemes only provide part security protection, and encryption in the spatial domain only provides communication and storage security. A highly comprehensive security measure is not guaranteed. Smart medical systems will suffer heavy trust crisis in the case of decrypted image redistribution. For a secure medical image sharing method, the scheme should be sensitive to scalability so that the watermarked

content can be protected according to the security requirements. This can be achieved by introducing scalable joint encryption and watermarking for medical images.

With the proposed method, only the most important content is selected to be encrypted in the transform domain. Selective encryption can provide advantages such as parallel security computing, controllable privacy protection, scalability, lower encryption time, and watermarking in the encrypted domain. Thus, the proposed joint selective encryption and watermarking method can not only protect medical images in smart medical systems but also improve the performance of the proposed security algorithm.

5. Conclusions

A JEW algorithm has been proposed for smart healthcare systems. The middle subbands are used to embed watermark information. The encryption includes selective permutation and further diffusion with SVD and bitwise XOR computing. Selective permutation, which can meet the fast request in smart healthcare systems, encrypts important parts. The research will help the development of related areas such as secure storage and multimedia communication for both academic sense and applied value. Related analysis shows that the proposed scheme can not only resist brute-force attacks and histogram attacks but also own visual security. Furthermore, because only the important parts are chosen to encrypt, and confusion and watermarking operations can be performed in parallel, it has a lower time complexity than those encryption schemes in the spatial domain. Finally, the time efficiency of JEW scheme is desirable, so it is a good candidate technology for privacy protection in smart healthcare systems.

However, although the proposed JEW scheme can overcome the shortcomings of the existing image encryption schemes in the spatial domain, it does not research the watermarking and encryption in the compressed domain as in other related image encryption methods. In the future, the authors will research medical image security algorithms in the compressed domain, especially watermarking in the encrypted–compressed domain.

Author Contributions: Conceptualization, C.Y.; formal analysis, C.Y. and L.S.; investigation, J.W., S.T., B.X. and L.S.; writing, C.Y. and Q.Z.; funding acquisition, C.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Natural Science Foundation of China under grant 61502154, 61972136, and 52201363), NSF of the Chinese Hubei Province, grant number 2024AFB544, and the Project in Hubei Provincial Department of Education, grant number Q20232206 and 23Y116.

Data Availability Statement: The data generated and analyzed in this study are included in this published article.

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

Abbreviations

The following abbreviations are used in this manuscript:

IoMT	Internet of Medical Things
SVD	Singular-Value Decomposition
DWT	Discrete Wavelet Transform
IDWT	Inverse DWT
JEW	Joint Encryption and Watermarking
SHA	Secure Hash Algorithm
2D-HSM	2D Hénon–Sine map
HNN	Hopfield Neural Network
NPCR	Number of Pixel Change Rate

UACI	Uniform Average Change Intensity
PSNR	Peak Signal-to-Noise Ratio
DNA	Deoxyribonucleic Acid)
NC	Correlation Coefficient
2D-CHSLM	2D Cross-Hyperchaotic Sine-Modulation-Logistic Map
FOMHS	Fractional-Order Memristive Hyperchaotic System

References

1. Almas, A.; Iqbal, W.; Altaf, A.; Saleem, K.; Mussiraliyeva, S.; Iqbal, M.W. Context-Based Adaptive Fog Computing Trust Solution for Time-Critical Smart Healthcare Systems. *IEEE Internet Things J.* **2023**, *10*, 10575–10586. [CrossRef]
2. Sarosh, P.; Parah, S.A.; Malik, B.A.; Hijji, M.; Muhammad, K. Real-Time Medical Data Security Solution for Smart Healthcare. *IEEE Trans. Ind. Inform.* **2023**, *19*, 8137–8147. [CrossRef]
3. Qu, Z.; Meng, Y.; Liu, B.; Muhammad, G.; Tiwari, P. QB-IMD: A Secure Medical Data Processing System With Privacy Protection Based on Quantum Blockchain for IoMT. *IEEE Internet Things J.* **2024**, *11*, 40–49. [CrossRef]
4. Anand, A.; Singh, A.K. Dual Watermarking for Security of COVID-19 Patient Record. *IEEE Trans. Dependable Secur. Comput.* **2023**, *20*, 859–866. [CrossRef]
5. Huang, J.; Cui, Q.; Zhou, Z.; Yu, K.; Yang, C.N.; Choo, K.K.R. Encrypted Domain Secret Medical-Image Sharing With Secure Outsourcing Computation in IoT Environment. *IEEE Internet Things J.* **2024**, *11*, 2382–2393. [CrossRef]
6. Anand, A.; Singh, A.K. Hybrid Nature-Inspired Optimization and Encryption-Based Watermarking for E-Healthcare. *IEEE Trans. Comput. Soc. Syst.* **2023**, *10*, 2033–2040. [CrossRef]
7. Ping, P.; Wei, P.; Fu, D.; Guo, B.; Bloh, O.T.; Xu, F. IMIH: Imperceptible Medical Image Hiding for Secure Healthcare. *IEEE Trans. Dependable Secur. Comput.* **2024**, *21*, 4652–4667. [CrossRef]
8. Meng, B.; Yuan, X.; Zhang, Q.; Lam, C.T.; Huang, G. Encryption-then-embedding-based hybrid data hiding scheme for medical images. *J. King Saud Univ.-Comput. Inf. Sci.* **2024**, *36*, 101932. [CrossRef]
9. Chai, X.; Tang, Z.; Gan, Z.; Lu, Y.; Wang, B.; Zhang, Y. SE-NDEND: A novel symmetric watermarking framework with neural network-based chaotic encryption for Internet of Medical Things. *Biomed. Signal Process. Control* **2024**, *90*, 105877. [CrossRef]
10. Nawaz, S.A.; Li, J.; Bhatti, U.A.; Shoukat, M.U.; Li, D.; Raza, M.A. Hybrid watermarking algorithm for medical images based on digital transformation and MobileNetV2. *Inf. Sci.* **2024**, *653*, 119810. https://doi-org-s.hubu.yitlink.com:443/10.1016/j.ins.2023.119810. [CrossRef]
11. Mao, J.; Tang, H.; Lyu, S.; Zhou, Z.; Cao, X. Content-Aware Quantization Index Modulation: Leveraging Data Statistics for Enhanced Image Watermarking. *IEEE Trans. Inf. Forensics Secur.* **2024**, *19*, 1935–1947. [CrossRef]
12. Wang, M.; Teng, L.; Zhou, W.; Yan, X.; Xia, Z.; Zhou, S. A new 2D cross hyperchaotic Sine-modulation-Logistic map and its application in bit-level image encryption. *Expert Syst. Appl.* **2025**, *261*, 125328. [CrossRef]
13. Kocak, O.; Erkan, U.; Toktas, A.; Gao, S. PSO-based image encryption scheme using modular integrated logistic exponential map. *Expert Syst. Appl.* **2024**, *237*, 121452. [CrossRef]
14. Toktas, F.; Erkan, U.; Yetgin, Z. Cross-channel color image encryption through 2D hyperchaotic hybrid map of optimization test functions. *Expert Syst. Appl.* **2024**, *249*, 123583. [CrossRef]
15. Zhang, Z.; Cao, Y.; Zhou, N.; Xu, X.; Mou, J. Novel discrete initial-boosted Tabu learning neuron: Dynamical analysis, DSP implementation, and batch medical image encryption. *Appl. Intell.* **2025**, *55*, 61. [CrossRef]
16. Feng, W.; Wang, Q.; Liu, H.; Ren, Y.; Zhang, J.; Zhang, S.; Qian, K.; Wen, H. Exploiting Newly Designed Fractional-Order 3D Lorenz Chaotic System and 2D Discrete Polynomial Hyper-Chaotic Map for High-Performance Multi-Image Encryption. *Fractal Fract.* **2023**, *7*, 887. [CrossRef]
17. Feng, W.; Zhang, J.; Chen, Y.; Qin, Z.; Zhang, Y.; Ahmad, M.; Woźniakd, M. Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption. *Expert Syst. Appl.* **2024**, *246*, 123190. [CrossRef]
18. Feng, W.; Yang, J.; Zhao, X.; Qin, Z.; Zhang, J.; Zhu, Z.; Wen, H.; Qian, K. A Novel Multi-Channel Image Encryption Algorithm Leveraging Pixel Reorganization and Hyperchaotic Maps. *Mathematics* **2024**, *12*, 3917. [CrossRef]
19. Wang, S.; Pan, J.; Cui, Y.; Chen, Z.; Zhan, W. Fast Color Image Encryption Algorithm Based on DNA Coding and Multi-Chaotic Systems. *Mathematics* **2024**, *12*, 3297. [CrossRef]
20. Teng, L.; Du, L.; Leng, Z.; Wang, X. Chaotic image encryption based on partial face recognition and DNA diffusion. *Appl. Intell.* **2024**, *54*, 10360–10373. [CrossRef]
21. Yan, X.; Hu, Q.; Teng, L.; Su, Y. Unmanned ship image encryption method based on a new four-wing three-dimensional chaotic system and compressed sensing. *Chaos Solitons Fractals* **2024**, *185*, 115146. [CrossRef]
22. Wen, H.; Lin, Y. Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding. *Expert Syst. Appl.* **2024**, *237*, 121514. [CrossRef]

23. Wen, H.; Lin, Y. Cryptanalyzing an image cipher using multiple chaos and DNA operations. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 101612. [CrossRef]
24. Feng, W.; Zhang, J. Cryptanalzing a Novel Hyper-Chaotic Image Encryption Scheme Based on Pixel-Level Filtering and DNA-Level Diffusion. *IEEE Access* **2020**, *8*, 209471–209482. [CrossRef]
25. Deng, Q.; Wang, C.; Sun, Y.; Deng, Z.; Yang, G. Memristive Tabu Learning Neuron Generated Multi-Wing Attractor With FPGA Implementation and Application in Encryption. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2024**, 1–12. [CrossRef]
26. Li, J.; Wang, C.; Deng, Q. Symmetric multi-double-scroll attractors in Hopfield neural network under pulse controlled memristor. *Nonlinear Dyn.* **2024**, *112*, 14463–14477. [CrossRef]
27. Wu, W.; Zhou, J. Constructing new high-order polynomial chaotic maps and application in pseudorandom number generator. *Phys. Scr.* **2024**, *99*, 035238. [CrossRef]
28. Mou, J.; Han, Z.; Cao, Y.; Banerjee, S. Discrete Second-Order Memristor and Its Application to Chaotic Map. *IEEE Trans. Circuits Syst.-Express Briefs* **2024**, *71*, 2824–2828. [CrossRef]
29. Wu, Z.; Zhang, Y.; Bao, H.; Lan, R.; Hua, Z. nD-CS: A circularly shifting chaotic map generation method. *Chaos Solitons Fractals* **2024**, *181*, 114650. [CrossRef]
30. He, S.; Hu, K.; Wang, M.; Wang, H.; Wu, X. Design and dynamics of discrete dual-memristor chaotic maps and its application in speech encryption. *Chaos Solitons Fractals* **2024**, *188*, 115517. [CrossRef]
31. Hua, Z.; Yao, J.; Zhang, Y.; Bao, H.; Yi, S. Two-Dimensional Coupled Complex Chaotic Map. *IEEE Trans. Ind. Inform.* **2024**. [CrossRef]
32. Li, C.; Li, Y.; Yu, W.; Moroz, I.; Volos, C. Constructing conditional symmetry in a chaotic map. *Nonlinear Dyn.* **2025**, *113*, 3857–3868. [CrossRef]
33. Zeng, Y.; Hu, H.; Shuai, Y. A general method for constructing high-dimensional chaotic maps with topological mixing on the global phase space. *Chaos Solitons Fractals* **2024**, *182*, 114818. [CrossRef]
34. Bao, H.; Xi, M.; Wang, N.; Xu, Q.; Bao, B. Designing multi-cavity chaotic maps via multistage step state extension. *Nonlinear Dyn.* **2024**, *112*, 12521–12535. [CrossRef]
35. Wang, M.m.; Song, X.g.; Liu, S.h.; Zhao, X.q.; Zhou, N.r. A novel 2D Log-Logistic-Sine chaotic map for image encryption. *Nonlinear Dyn.* **2025**, *113*, 2867–2896. [CrossRef]
36. Liu, X.; Mou, J.; Zhang, Y.; Cao, Y. A New Hyperchaotic Map Based on Discrete Memristor and Meminductor: Dynamics Analysis, Encryption Application, and DSP Implementation. *IEEE Trans. Ind. Electron.* **2024**, *71*, 5094–5104. [CrossRef]
37. Yu, F.; Zhang, W.; Xiao, X.; Yao, W.; Cai, S.; Zhang, J.; Wang, C.; Li, Y. Dynamic Analysis and Field-Programmable Gate Array Implementation of a 5D Fractional-Order Memristive Hyperchaotic System with Multiple Coexisting Attractors. *Fractal Fract.* **2024**, *8*, 271. [CrossRef]
38. Yu, F.; Xu, S.; Lin, Y.; He, T.; Wu, C.; Lin, H. Design and Analysis of a Novel Fractional-Order System with Hidden Dynamics, Hyperchaotic Behavior and Multi-Scroll Attractors. *Mathematics* **2024**, *12*, 2227. [CrossRef]
39. Lai, Q.; Yang, L.; Hu, G.; Guan, Z.H.; Iu, H.H.C. Constructing Multiscroll Memristive Neural Network With Local Activity Memristor and Application in Image Encryption. *IEEE Trans. Cybern.* **2024**, *54*, 4039–4048. [CrossRef]
40. Wang, C.; Luo, D.; Deng, Q.; Yang, G. Dynamics analysis and FPGA implementation of discrete memristive cellular neural network with heterogeneous activation functions. *Chaos Solitons Fractals* **2024**, *187*, 115471. [CrossRef]
41. Ma, X.; Wang, Z.; Wang, C. An Image Encryption Algorithm Based on Tabu Search and Hyperchaos. *Int. J. Bifurc. Chaos* **2024**, *34*, 2450170. [CrossRef]
42. Yu, F.; Lin, Y.; Yao, W.; Cai, S.; Lin, H.; Li, Y. Multiscroll hopfield neural network with extreme multistability and its application in video encryption for IIoT. *Neural Netw.* **2025**, *182*, 106904. [CrossRef] [PubMed]
43. Thanki, R.; Kothari, A. Multi-level security of medical images based on encryption and watermarking for telemedicine applications. *Multimed. Tools Appl.* **2021**, *80*, 4307–4325. [CrossRef]
44. Liu, R.; Tan, T. An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Trans. Multimed.* **2002**, *4*, 121–128. [CrossRef]
45. Anand, A.; Singh, A.K. Health Record Security Through Multiple Watermarking on Fused Medical Images. *IEEE Trans. Comput. Soc. Syst.* **2022**, *9*, 1594–1603. [CrossRef]
46. Jungk, B.; Stoettinger, M. Serialized lightweight SHA-3 FPGA implementations. *Micorprocessors Microsyst.* **2019**, *71*, 102857. [CrossRef]
47. Vaidyanathan, S.; Sambas, A.; Tlelo-Cuautle, E.; El-Latif, A.A.A.; Abd-El-Atty, B.; Guill n Fern ndez, O.; Benkouider, K.; Mohamed, M.A.; Mamat, M.; Ibrahim, M.A.H. A New 4-D Multi-Stable Hyperchaotic System With No Balance Point: Bifurcation Analysis, Circuit Simulation, FPGA Realization and Image Cryptosystem. *IEEE Access* **2021**, *9*, 144555–144573. [CrossRef]
48. Wu, J.; Liao, X.; Yang, B. Image encryption using 2D Hénon-Sine map and DNA approach. *Signal Process.* **2018**, *153*, 11 – 23. [CrossRef]

49. Hopfield.; J., J. Neural networks and physical systems with emergent collective computational abilities. *Proc. Natl. Acad. Sci. USA* **1982**, *79*, 2554–2558. [CrossRef]
50. Rostami, M.J.; Shahba, A.; Saryazdi, S.; Nezamabadi-pour, H. A novel parallel image encryption with chaotic windows based on logistic map. *Comput. Electr. Eng.* **2017**, *62*, 384–400. [CrossRef]
51. Diaconu, A.V. Circular inter-intra pixels bit-level permutation and chaos-based image encryption. *Inf. Sci.* **2016**, *355*, 314–327. [CrossRef]
52. Ye, C.; Chen, C. Secure medical image sharing for smart healthcare system based on cellular neural network. *Complex Intell. Syst.* **2023**, *9*, 1653–1670. [CrossRef]
53. Al-Haj, A.; Abdel-Nabi, H. An efficient watermarking algorithm for medical images. *Multimed. Tools Appl.* **2021**, *80*, 26021–26047. [CrossRef]
54. Bouslimi, D.; Coatrieux, G.; Cozic, M.; Roux, C. A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images. *IEEE Trans. Inf. Technol. Biomed.* **2012**, *16*, 891–899. [CrossRef]
55. Meng, F.Q.; Wu, G. A color image encryption and decryption scheme based on extended DNA coding and fractional-order 5D hyper-chaotic system. *Expert Syst. Appl.* **2024**, *254*, 124413. [CrossRef]
56. Anand, A.; Singh, A.K. An improved DWT-SVD domain watermarking for medical information security. *Comput. Commun.* **2020**, *152*, 72–80. [CrossRef]
57. Thakur, S.; Singh, A.K.; Ghrera, S.P.; Elhoseny, M. Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. *Multimed. Tools Appl.* **2019**, *78*, 3457–3470. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.