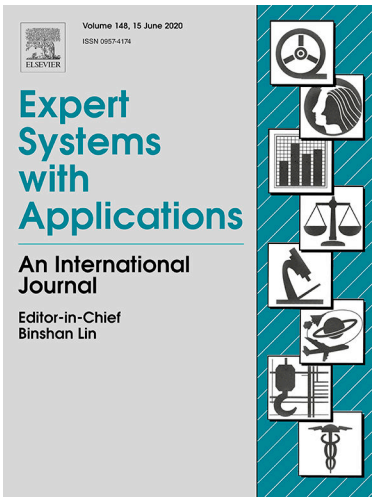
Journal Pre-proofs



ASB-CS: Adaptive sparse basis compressive sensing model and its application to medical image encryption

Donghua Jiang, Nestor Tsafack, Wadii Boulila, Jawad Ahmad, J.J. Barba-Franco

PII: S0957-4174(23)01880-8
DOI: https://doi.org/10.1016/j.eswa.2023.121378
Reference: ESWA 121378

To appear in: *Expert Systems with Applications*

Received Date: 19 June 2023
Revised Date: 28 August 2023
Accepted Date: 28 August 2023

Please cite this article as: Jiang, D., Tsafack, N., Boulila, W., Ahmad, J., Barba-Franco, J.J., ASB-CS: Adaptive sparse basis compressive sensing model and its application to medical image encryption, *Expert Systems with Applications* (2023), doi: https://doi.org/10.1016/j.eswa.2023.121378

ASB-CS: Adaptive sparse basis compressive sensing model and its application to medical image encryption

Donghua Jiang, Nestor Tsafack, Wadii Boulila, Jawad Ahmad, and Barba-Franco J.J.

Abstract—Recent advances in intelligent wearable devices have brought tremendous chances for the development of healthcare monitoring system. However, the data collected by various sensors in it are user-privacy-related information. Once the individuals' privacy is subjected to attacks, it can potentially cause serious hazards. For this reason, a feasible solution built upon the compression-encryption architecture is proposed. In this scheme, we design an Adaptive Sparse Basis Compressive Sensing (ASB-CS) model by leveraging Singular Value Decomposition (SVD) manipulation, while performing a rigorous proof of its effectiveness. Additionally, incorporating the Parametric Deformed Exponential Rectified Linear Unit (PDE-ReLU) memristor, a new fractional-order Hopfield neural network model is introduced as a pseudo-random number generator for the proposed cryptosystem, which has demonstrated superior properties in many aspects, such as hyperchaotic dynamics and multistability. To be specific, a plain medical image is subjected to the ASB-CS model and bidirectional diffusion manipulation under the guidance of the key-controlled cipher flows to yield the corresponding cipher image without visual semantic features. Ultimately, the simulation results and analysis demonstrate that the proposed scheme is capable of withstanding multiple security attacks and possesses balanced performance in terms of compressibility and robustness.

Index Terms—Compressive sensing, adaptive sparse representation, singular value decomposition, chaotic neural network, image encryption

1. INTRODUCTION

At present, the widespread usage of wearable medical data collection and surveillance devices, including but not limited to the intelligent bracelet, blood glucose monitor and defibrillator, leads to massive amounts of private data being generated. In the meantime, the emergence of social platforms has facilitated the convenient dissemination of data, thereby boosting their accessibility. With this comes the increasing concern of users about the privacy and security of data. In addition, digital image with vivid, visual, and intuitive features has become one of the most popular multimedia data formats. In this context, preventing digital images from divulging user-privacy-related information becomes extremely challenging for cryptologists owing to their large data volume, high redundancy, and strong relevance. Hence, it has emerged as one of research focuses on the information security field.

In other aspects, for the resource-constrained applications, such as wearable devices and portable medical data collection sensors, it is extremely significant to encrypt sensitive data while taking into account the compression of its redundant data to conserve overhead. Then, considering as an emerging information acquisition technology, the Compressive Sensing (CS) (*Donoho*, 2006; *Candes*, 2006) can not only throw off the frequency constraint of the traditional Nyquist-Shannon sampling theorem and greatly curtail the redundancy among data, but also accomplish data compression while performing sampling, thereby effectively diminishing the complexity of information acquisition system (*Jiang*, 2021). Therefore, in the latest years, this promising technology has gained the close attention of widespread scholars and cryptographers.

The remarkable advances in compressive sensing technology have promoted a tremendous success in the privacy preservation field. However, through a comprehensive analysis for the existing related works in the following section, we found out that there exist some limitations in the compression stage of the current CS-based data encryption schemes. Accordingly, the primary focus of this paper is to propose an adaptive sparse basis compressive sensing model. Meanwhile, when applying this model to the healthcare monitoring system, we also devote to designing a high-performance memristive Hopfield neural network as a pseudo-random number generator.

1.1. Related Works

From a cryptographic point of view, the CS-based information acquisition system can be considered as a variant of symmetric cryptosystem to some extent (*Zhu*, 2022a). More specifically, it is known to all that a basic cryptosystem comprises five primary components, namely, plaintext, ciphertext, secret key, encryption and decryption processes. Moreover, these correspond precisely to original signal, measured signal, measurement matrix, sampling and reconstruction processes in the CS theory. However, note that the remarkable discrepancy between them is that the latter is an irreversible system. Afterward, it has gained unprecedented advancements in the information security field (*Xue*, 2021).

Corresponding author: Jawad Ahmad (E-mail: J.Ahmad@napier.ac.uk).

Donghua Jiang is with the School of Information Engineering, Chang'an University, Xi'an 710064, China. (E-mail: jiangdonghua@chd.edu.cn).

Nestor Tsafack is with the Research Unit of Laboratory of Energy and Artificial Intelligence, Electrical Engineering Department and Industrial Computing of ISTAMA, University of Douala, P.O. Box 3223, Douala, Cameroon. (E-mail: nestor.tsafack@yahoo.fr).

Wadii Boulila is with the Robotics and Internet-of-Things Laboratory, Prince Sultan University, Riyadh 12435, Saudi Arabia (E-mail: wboulila@ psu.edu.sa).

Jawad Ahmad is with the School of Computing, Edinburgh Napier University, Edinburgh, United Kingdom.

Barba-Franco, J.J. is with the Departamento de Ciencias Exactas y Tecn-ología, Centro Universitario de los Lagos, Universidad de Guadalajara, Enrique Díaz de León, Paseos de la Montaña, 47460 Lagos de Moreno, Jalisco, Mexico. (E-mail: dejesus.barba@alumnos.udg.mx).

The research on applying CS technology to digital image encryption can be traced back to as early as around 2008. For example, Kumar et al. projected the plain image after linear transform operation onto a random Gaussian matrix to implement synchronized compression and encryption of data. Later, the original image is reconstructed with high probability at the decoding end by means of the modified basis pursuit approach (*Kumar and Makur*, 2009). Although there exist several shortcomings, such as high burden of key transmission and low image fidelity, it is admittedly a successful attempt. Moreover, the similar drawbacks are also present in (*Huang* and *Sakurai,* 2011). To tackle the first above-mentioned issue, scholars have successively introduced a variety of approaches to construct the deterministic measurement matrices, including chaotic measurement matrix (*Sethi*, 2022; *Zhang*, 2022), restricted structural random matrix (*Canh and Jeon*, 2021), expander-graphs-based measurement matrix (Jafarpour, 2009), and so on, thereby eliminating the constraint condition of transmitting whole stochastic measurement matrix that is viewed as a shared key. Regarding the second issue, (*Xiao*, 2021; *Hua*, 2021; *Zhu*, 2022b) coincidentally exploited the adaptive thresholding mechanism to ameliorate the sparsity of the transform domain coefficients which in turn enhances the fidelity of reconstructed image. In other aspects, (*Fang*, 2014) revealed that performing scrambling manipulation on 2-D sparse data before compressed sampling parallelly can significantly relax the constraint of the Restricted Isometry Property (RIP). Whereafter, various CS models with distinctive features, such as 2-D CS (*Yang*, 2022), semi-tensor product CS (*Niu*, 2020) and Bayesian CS (*Zhu*, 2022a), were successively applied into privacy protection.

Besides its application level, some scholars have also comprehensively analyzed the security level of the CS technology. It has been mentioned in (*Rachlin and Baron*, 2008; *Hossein*, 2012) that although it cannot guarantee the absolute security of sampled data in terms of information theory, it can make the brute force attacks against key or ciphertext computationally infeasible. Furthermore, its compressed sampling process is a linear projection process in essence (*Zhu*, 2020), which means it is effortless for the illegitimate attacker to figure out a particular employed measurement matrix, when he/she holds sufficient plaintext-ciphertext pairs. To arrive at a higher secure level, the CS-based symmetric cryptosystems would require updating key frequently, even using the one-time-pad pattern. Apparently, it will instead contribute to the serious data disaster. More importantly, it is contrary to the design concept of the CS. At this moment, a feasible solution is to adopt the counter mechanism against the powerful chosen-plaintext attacks (*Hu*, 2017).

1.2. Motivations and Contributions

In the previous paragraphs, we have reviewed minutely the CS technology applied to the privacy protection field from the aspects of application and security levels, respectively. Although, outstanding advances have been made after more than a decade of development, there remain certain issues that have been overlooked by us over the long-term. One of them is the demand for designing an adaptive sparse representation model. To be more specific, the existing CS-based encryption schemes all adopt static (or fixed) orthogonal bases to sparsely represent plain images, including but not limited to Fourier basis, wavelet basis, Gabor basis, and Contourlet basis. Nevertheless, it is well known that the sparsity of natural images with identical texture complexity is not consistent over distinct orthogonal bases. Undoubtedly, the selection of a sparse representation basis is crucial in the design of a security system, as it can significantly affect both the execution efficiency and the reconstruction quality. Inspired by this, we have carried out a series of experiments on image sparse representation proceed from data content itself. As a result, the contributing and innovative points of this work are threefold, summarized as follows:

- Design an adaptive sparse representation model for digital images by leveraging SVD theorem and then apply it into the CS technology.
- Construct a new fractional-order Hopfield neural network with hyperchaotic dynamical behavior, while rigorously proving its inherent properties.
- Propose a novel data encryption scheme for medical image to trade off its privacy, compressibility and fidelity by fully exploiting the properties of newly designed models.

1.3. Paper Organization

To facilitate readers to comprehend our work better, the remaining sections are arranged as follows. First, in Section 2, we provide a brief overview of the prior knowledge and underlying models. Next, in Section 3, the dynamics equation of the proposed memristive Hopfield neural network model and its intrinsic properties are given. Meanwhile, we also analyze its dynamics in multiple aspects. Section 4 then describes in detail the proposed ASB-CS model. In Section 5, the technical details and application scenarios of our scheme designed for medical image carrying user sensitive information are demonstrated. We follow this up with the analytical results of its performance from multiple aspects in Section 6. Finally, in Section 7, we review and summarize our work, as well as outline our future research plans.

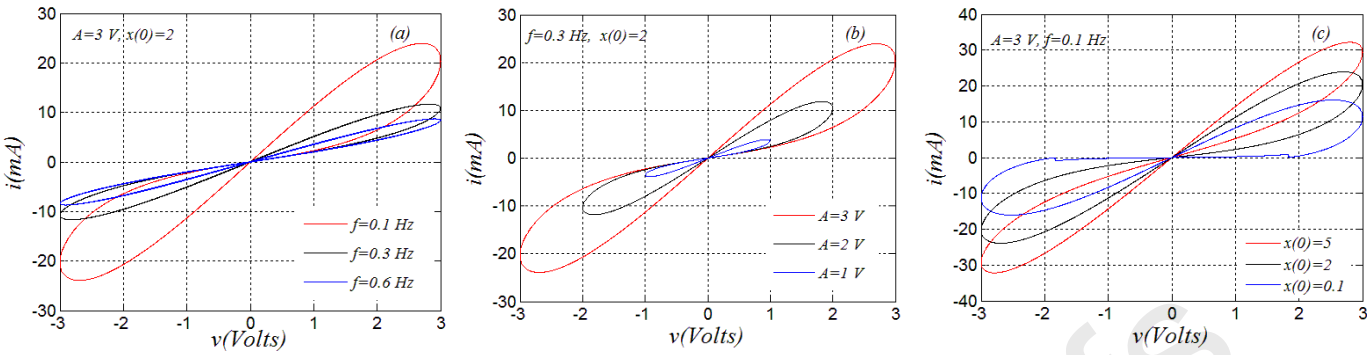


Fig. 1. Pinched hysteresis loops of the PDE-ReLU memristor.

2. Preliminaries and Model Description

2.1. Fractional Calculus Theory

Giving its suitability for describing physical systems, the Caputo derivative is widely applied in engineering applications. Considering a function $f(x)$ and a fractional order $m-1<\alpha<m\left(m\in\mathbb{N},\alpha\in\mathbb{R}^{+}\right)$, its mathematical definition is provided by Eqs. (1) and (2). Besides, the adopted numerical approach to solve the proposed fractional-order nonlinear system in this work is described in the sequel.

$$ {}_{C}D_{0,t}^{\lambda}f(t)=D_{0,t}^{-(n-\lambda)}\frac{d^{n}}{dt^{n}}f(t). \tag{1}$$

$$ {}_{C}D_{0,t}^{\lambda}f(t)=\frac{1}{\Gamma(n-\lambda)}\int_{o}^{t_0}(t-t_0)^{n-\lambda-1}f^{(n)}(t_0)dt_0. \tag{2}$$

where $\Gamma(z)$ signifies the gamma function. The following are two crucial properties of the Caputo derivative (*Ahmad*, 2021).

(1) The Laplace Transform (LT) can be applied to Eq. (2) and the corresponding outcome is provided on Eq. (3), where $F(s)=LT\left[f(t)\right](s)$.

$$ LT\left[{}_{C}D_{0,t}^{\lambda}f(t)\right](s)=s^{\lambda}F(s)-\sum_{m=0}^{n}s^{\lambda-m-1}f^{m}(0). \tag{3}$$

(2) Considering any constant number α, ${}_{C}D_{0,t}^{\lambda}\alpha=0$.

2.2. Parametric Deformed Exponential ReLU Memristor

In 1971, Chua introduced the idea of existence of a fourth passive electronic component beside resistor, capacitor and inductor. This device, termed as memristor, can be exploited to store information considering that the corresponding varies from a low value to a high value. In neurocomputing and information theory, various models of this empirical device have been proposed to emulate its behavior including the ReLU memristor model (*Cheng*, 2020). In this paper, we considered an improved version of ReLU memristor to design a new neural network model with complicated dynamics. The proposed memristor is defined mathematically in Eq. (4).

$$\begin{cases} i=M(x)v=\left[a-bg(x)\right]v \\ \dfrac{dx}{dt}=m(x,v)=v \end{cases}. \tag{4}$$

where v and i are the voltage and current through memristor, respectively. x is its internal variable. M is its memductance and m is a function of voltage and internal parameter. $g(x)$ indicates the parametric deformed exponential ReLU function, which is defined in Eq. (5).

$$\begin{cases} g(x)=x,\forall x>0 \\ g(x)=\alpha\left[-1+\left(1+(1-\beta)x\right)^{\frac{1}{1-\beta}}\right],\forall x\le 0 \end{cases}. \tag{5}$$

With the objective to exhibit the pinched characteristics of the designed memristor, various sinusoidal excitation with the form $v=A\sin(2\pi Ft)$ have been applied to this model, where its hyper-parameters are fixed firmly as $\alpha=0.005$ and $\beta=0.9$. The corresponding evaluation results are visualized in Fig 1. Apparently, it is observed from Fig. 1(a) that the loop tends to a unique function. Then, judging from Fig. 1(b), the lobe of the characteristic increases with the amplitude of the external excitation. Besides, as demonstrated in Fig. 1(c), it is clearly seen that many hysteresis loops coexist in the current voltage plane depending solely on the initial value. Therefore, we can conclude that the designed memristor satisfied the fingerprint characteristics of a memristor as predicted by (*Chua*, 1971).

2.3. Singular Value Decomposition

Up to now, SVD has been broadly used in machine learning, recommendation system, natural language processing and other fields (*Klema and Laub*, 1980). It refers that for any non-zero real matrix $A\in\mathbb{R}^{m\times n}$, it can be decomposed into the product form of three real matrices, as shown in Eq. (6), where U and V are the m- and n-order orthogonal matrices, respectively. Besides, Σ is a $m\times n$-sized rectangular diagonal matrix composed of non-negative diagonal elements arranged in descending order.

$$A = U\Sigma V^T. \tag{6}$$

There exist the following properties in SVD of a matrix.

(1) The rank of matrix A is equal to that of matrix Σ, while being equal to the number of positive singular values (including repeated singular values).

(2) There exists a certain quantitative relationship between the Frobenius norm of matrix A and its singular value matrix $\Sigma = \mathrm{diag}(\sigma_1, \sigma_2, ..., \sigma_p)$ (*Gass and Rapcsak*, 2004), as displayed in Eq.(7), where $p = \min\{m, n\}$.

$$\|A\|_F = \left(\sigma_1^2 + \sigma_2^2 + ... + \sigma_p^2\right)^{1/2}. \tag{7}$$

(3) Arbitrary real matrix A can be represented by its outer product expansion, as formulated in Eq. (8).

$$A = \sigma_1 u_1 v_1^T + \sigma_2 u_2 v_2^T + ... + \sigma_n u_n v_n^T. \tag{8}$$

3. New Fractional-Order HNN Model Based on PDE-ReLU Memristor

Since the structure of the Hopfield Neural Network (HNN) (*Rech*, 2011) is highly similar to that of the real biological neural network, it is broadly used to mimic some dynamic behaviors occurring in the human brain. This is the reason why this topic is still a hot spot in nonlinear dynamics field until now. The HNN is mathematically formulated as Eq. (9).

$$C_\alpha \dot{v}_\alpha = -\frac{v_\alpha}{R_\alpha} + \sum_{\beta=1}^{m} \omega_{\alpha,\beta} \tanh(v_\alpha) + I_\alpha. \tag{9}$$

Where $\alpha, \beta \in \mathbb{N}^*$. v_α indicates the membrane potential of the neuron α. R_α and C_α are the resistance and the capacitance between inside and outside of neuron. I_α represents the bias current of neuron. $\omega_{\alpha,\beta}$ is a $\alpha \times \beta$-sized matrix containing the synaptic weights of m neurons in the global network. $\tanh(v_\alpha)$ represents the activation function of neuron.

Intuitively, the dynamics of this global network significantly depends on the synaptic weights. Next, we construct a neural network model with five neurons by adding the above described memristor to the basic HNN network and attempting to search for the correct synaptic weights, which is abbreviated as PDE-ReLU-MHNN. Then, its kinetic equation is mathematically defined in Eq. (10) using the Caputo method for fractional derivative.

$$\begin{cases} {}_C D_{0,t}^{\lambda} x_1 = -x_1 + \tanh(x_1) + 0.5\tanh(x_2) - 3\tanh(x_3) - \tanh(x_4) \\ {}_C D_{0,t}^{\lambda} x_2 = -x_2 + 0.1\tanh(x_1) + \omega_{22}\tanh(x_2) + 3\tanh(x_3) \\ \qquad - 0.1\tanh(x_4) \\ {}_C D_{0,t}^{\lambda} x_3 = -x_3 + 3\tanh(x_1) - 3\tanh(x_2) + \omega_{33}\tanh(x_3) - \tanh(x_4). \\ {}_C D_{0,t}^{\lambda} x_4 = -100x_4 + 100\left(a - bg(x_5)\right)\tanh(x_1) - 0.1\tanh(x_2) \\ \qquad + 0.1\tanh(x_3) + 170\tanh(x_4) \\ {}_C D_{0,t}^{\lambda} x_5 = \tanh(x_1) \end{cases} \tag{10}$$

where $g(\cdot)$ signifies the PDE-ReLU function defined in Eq. (5). ω_{22} and ω_{33} can be tuned to reveal its rich dynamics. The dynamics of the proposed model is evaluated with both cases of integer- and fractional-orders. Therefore, the constructed model performs better dynamics compared to some previous HNN models.

3.1. Analysis of Model Properties

Before diving into the various dynamics of the proposed PDE-ReLU-MHNN model, we first rigorously proof its properties from a mathematical point of view.

(1) Boundedness proof: The boundness property is necessary for a nonlinear system to yield chaotic or hyperchaotic behaviors. Therefore, we intend to proof that the proposed PDE-ReLU-MHNN model is bounded in this sub-section. Let us consider the Lyapunov function defined in Eq. (11).

$$V(x_1, x_2, x_3, x_4, x_5) = \frac{1}{2}\left(x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2\right). \tag{11}$$

The corresponding derivative with respect to time is provided by Eq. (12).

$$\begin{aligned} D_{0,t}^{-(n-\lambda)} \frac{d^n}{dt^n} V\left(\{x_i\}_{i=1}^5\right) &= x_1 D_{0,t}^{-(n-\lambda)} \frac{d^n x_1}{dt^n} + x_2 D_{0,t}^{-(n-\lambda)} \frac{d^n x_2}{dt^n} + x_3 D_{0,t}^{-(n-\lambda)} \frac{d^n x_3}{dt^n} \\ &+ x_4 D_{0,t}^{-(n-\lambda)} \frac{d^n x_4}{dt^n} + x_5 D_{0,t}^{-(n-\lambda)} \frac{d^n x_5}{dt^n} \\ &= -x_1^2 - x_2^2 - x_3^2 - x_4^2 \\ &+ \left[x_1 + 0.1x_2 + 3x_3 + 100\left(a - bg(x_5)\right)x_4 + x_5^2\right]\tanh(x_1) \\ &+ \left[0.5x_1 + \omega_{22}x_2 - 3x_3 - 0.1x_4\right]\tanh(x_2) \\ &+ \left[-3x_1 + 3\omega_{33}x_2 x_3 - 0.1x_4\right]\tanh(x_3) \\ &+ \left[-x_1 - 0.1x_2 - x_3 + 170x_4\right]\tanh(x_4). \end{aligned} \tag{12}$$

For calculations simplifications, let us define:

$$\begin{aligned} V\left(\{x_i\}_{i=1}^5\right) = \tanh(x_1)\sum_{\alpha=1}^{4}\omega_{\alpha 1}x_\alpha + \tanh(x_2)\sum_{\alpha=1}^{4}\omega_{\alpha 2}x_\alpha + \\ \tanh(x_4)\sum_{\alpha=1}^{4}\omega_{\alpha 3}x_\alpha + \tanh(x_4)\sum_{\alpha=1}^{4}\omega_{\alpha 4}x_\alpha. \end{aligned} \tag{13}$$

For $x_\alpha \in \mathbb{R}, \tanh(x_\alpha) < 1 (\alpha = 1, 2, 3, 4)$, the above Eq. (13) can be rewritten as

$$\begin{aligned} V\left(\{x_i\}_{i=1}^5\right) &= \tanh(x_1)\sum_{\alpha=1}^4 \omega_{\alpha 1}x_\alpha + \tanh(x_2)\sum_{\alpha=1}^4 \omega_{\alpha 2}x_\alpha + \\ &\quad \tanh(x_3)\sum_{\alpha=1}^4 w_{\alpha 3}x_\alpha + \tanh(x_4)\sum_{\alpha=1}^4 \omega_{\alpha 4}x_4 \\ &\le \left|\tanh(x_1)\sum_{\alpha=1}^4 \omega_{\alpha 1}x_\alpha\right| + \left|\tanh(x_2)\sum_{\alpha=1}^4 \omega_{\alpha 2}x_\alpha\right| + \\ &\quad \left|\tanh(x_3)\sum_{\alpha=1}^4 \omega_{\alpha 3}x_\alpha\right| + \left|\tanh(x_4)\sum_{\alpha=1}^4 \omega_{\alpha 4}x_\alpha\right| \\ &< \left|\sum_{\alpha=1}^4 \omega_{\alpha 1}x_\alpha\right| + \left|\sum_{\alpha=1}^4 \omega_{\alpha 2}x_\alpha\right| + \left|\sum_{\alpha=1}^4 \omega_{\alpha 3}x_\alpha\right| + \left|\sum_{\alpha=1}^4 \omega_{\alpha 4}x_\alpha\right| \\ &\le \sum_{\alpha=1}^4 \omega_{\alpha 1}|x_\alpha| + \sum_{\alpha=1}^4 \omega_{\alpha 2}|x_\alpha| + \sum_{\alpha=1}^4 \omega_{\alpha 3}|x_\alpha| + \sum_{\alpha=1}^4 \omega_{\alpha 4}|x_\alpha| \\ &< x_1^2 + x_2^2 + x_3^2 + x_4^2. \end{aligned} \tag{14}$$

Integrating Eq. (14) into Eq. (12), Eq. (15) can be obtained.

$$\begin{aligned} D_{0,t}^{-(n-\lambda)} V\left(\{x_i\}_{i=1}^5\right) &= -x_1^2 - x_2^2 - x_3^2 - x_4^2 + x_5^2 \tanh(x_1) + V\left(\{x_i\}_{i=1}^5\right) \\ &< x_5^2 \tanh(x_1). \end{aligned} \tag{15}$$

Considering $R_0 > 0$ as the sufficiently large region for all $\{x_i\}_{i=1}^5$ satisfying $V\left(\{x_i\}_{i=1}^5\right) = A$ with $A > A_0$, the following condition is satisfied.

$$x_5^2 \tanh(x_1) < 0. \tag{16}$$

Consequently,

$$\left\{(x_1, x_2, x_3, x_4, x_5) \mid V(x_1, x_2, x_3, x_4, x_5) = A\right\}. \tag{17}$$

With $A > A_0$, we have

$$D_{0,t}^{-(n-\lambda)} \frac{d^n}{dt^n} V(x_1, x_2, x_3, x_4, x_5) < 0. \tag{18}$$

In brief, the proposed PDE-ReLU-MHNN model defined in Eq. (10) is bounded.

(2) Stability analysis: The stability of equilibrium points for a nonlinear system is crucial in the analysis of its global dynamics. In the following, we will analyze the equilibrium of the proposed PDE-ReLU-MHNN model and evaluate its stability by solving Eq. (19).

$$\begin{cases} 0 = -x_1 + \tanh(x_1) + 0.5\tanh(x_2) - 3\tanh(x_3) - \tanh(x_4) \\ 0 = -x_2 + 0.1\tanh(x_1) + \omega_{22}\tanh(x_2) + 3\tanh(x_3) - 0.1\tanh(x_4) \\ 0 = -x_3 + 3\tanh(x_1) - 3\tanh(x_2) + \omega_{33}\tanh(x_3) - \tanh(x_4) \\ 0 = -100x_4 + 100\left(a - bg(x_5)\right)\tanh(x_1) - 0.1\tanh(x_2) + 0.1\tanh(x_3) \\ \qquad + 170\tanh(x_4) \\ 0 = \tanh(x_1) \end{cases}. \tag{19}$$

From Eq. (19), it is observed that our newly proposed model has a line of equilibrium stated as $P(0,0,0,0,k)$, where $k \in \mathbb{R}$. The corresponding Jacobian matrix can be computed as defined in Eq. (20).

$$M_J = \begin{bmatrix} 0 & 0.5 & -3 & -1 & 0 \\ 0 & -0.9 + w_{22} & 3 & -0.1 & 0 \\ 3 & -3 & -1 + \omega_{33} & -1 & 0 \\ 100\xi & -0.1 & 0.1 & 70 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{20}$$

where $\xi = M(k)v = a - bg(x)$.

It should be noted that $\xi \in \mathbb{R}$. The polynomial characteristic equation is computed in Eq. (21).

$$\det(I\sigma - J) = \sigma^5 + \gamma_4\sigma^4 + \gamma_3\sigma^3 + \gamma_2\sigma^2 + \gamma_1\sigma = 0. \tag{21}$$

where

$$\begin{cases} \gamma_4 = -\omega_{22} - \omega_{33} - 68.1 \\ \gamma_3 = 69\omega_{22} + \omega_{22}\omega_{33} + 69.1\omega_{33} + 100\xi - 114.01 \\ \gamma_2 = -70\omega_{22}\omega_{33} + 63.01\omega_{33} + 60.9\omega_{22} - 100\xi\omega_{22} - \\ \qquad 100\xi\omega_{33} - 105\xi - 1319.35 \\ \gamma_1 = 200\xi\omega_{22} - 95\xi\omega_{33} + 100\xi\omega_{22}\omega_{33} + 629.7\omega_{22} + 965\xi - 252.705 \end{cases}. \tag{22}$$

Note that ω_{22} and ω_{33} are positive real numbers and $\xi \in \mathbb{R}$. With these considerations, it is obvious that the polynomial characteristic equation has both positive and negative coefficients. Consequently, in the light of the Routh-Hurwitz stability criteria, the equilibrium points on the line $P(0,0,0,0,k)$ are unstable. From this conclusion, it clearly comes out that the attractors generated by the proposed model are self-excited.

3.2. Analysis of Model Dynamics

This section considers the numerical analysis of the proposed PDE-ReLU-MHNN model including bifurcation diagram, phase portrait and Lyapunov spectrum to reveal its global dynamic. 10^{-3} is the fixed time step used for simulations with the synaptic weights defined in extended precision mode. Note that fixed time step in extended precision mode is known to reveal the suitable dynamics of oscillators and reduce errors. Besides, two cases will be considered in this section, namely, the integer order case and the Caputo fractional order case.

(1) Global dynamic for the integer order case: In this subsection, we will consider the integer order case of the proposed PDE-ReLU-MHNN model with the system parameters configured as $\lambda = 1, w_{22} = 3, \alpha = 0.005, \beta = 0.9, a = 1, b = 0.2$. Increasing variations of the control parameter w_{33} in the range $[0.5, 1.5]$ is exploited to compute the bifurcations of the proposed nonlinear model and its corresponding Lyapunov spectrum, as elaborated in Fig. 2. The good concordance is observed between the Lyapunov exponents and bifurcations. This simply shows the exactness of the computations. Additionally, from Fig. 3 various behaviors can be observed in the dynamics of the proposed HNN model including periodic attractor for $w_{33} = 1.22$ in Fig. 3(a), single scroll hyperchaotic attractor for $w_{33} = 1.112$ in Fig. 3(b), double scroll hyperchaotic attractor structure 1 for

$w_{33} = 1.042$ in Fig. 3(c), double scroll hyperchaotic attractor structure 2 for $w_{33} = 0.95$ in Fig. 3(d). Inverse period doubling route to hyperchaos is also observed. Therefore, it can be observed that various structures of hyperchaotic attractors can be obtained with this model.

Multistability is also observed in the dynamics of the proposed PDE-ReLU-MHNN model. To illustrate this behavior, various bifurcations have been plotted with the system parameters configured as $w_{33} = 1, \alpha = 0.005, \beta = 0.9, a = 1, b = 0.2$, which are drawn in Fig. 4. The control parameter w_{22} has been simultaneously upward and downward varied in the range $[0, 4]$ with a tiny step. Hysteresis is observed in the range $1.984 \le w_{22} \le 2.2$. This simply indicates the coexistence of periodic attractor with hyperchaotic attractor. More illustrations of this behavior are shown on Fig. 5 where the phase space coexisting attractors are computed using the same model parameters but with different initial conditions, defined as $x_1(0) = \pm 1, x_2(0) = \pm 0.02, x_3(0) = 0, x_4(0) = 0, x_5(0) = \pm 1$.

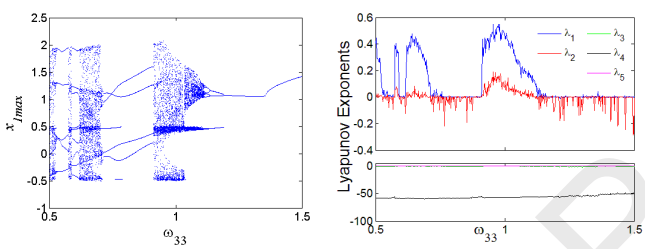


Fig. 2. Bifurcation and corresponding Lyapunov spectrum of the PDE-ReLU-MHNN model.

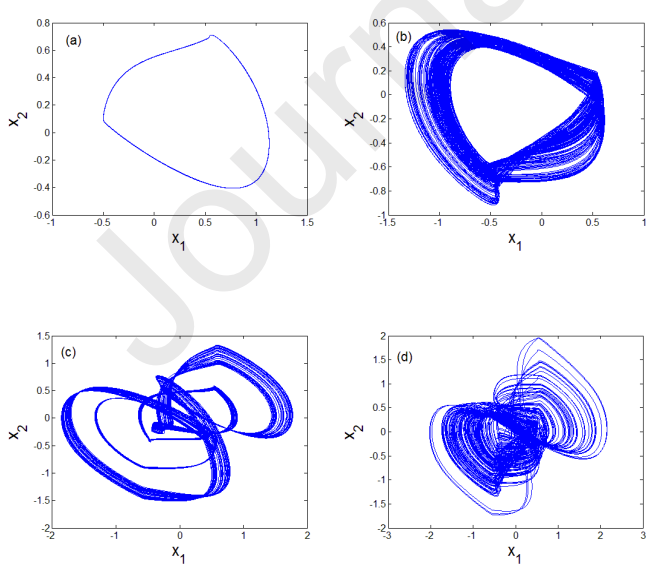


Fig. 3. Various attractor structures obtained from the proposed PDE-ReLU-MHNN model.

(2) Global dynamic for the fractional order case: In this subsection, we will analyze the dynamics of the new HNN model with respect to ω_{33} to compare the results with those of the integer order case of the previous section. Then, we set the system parameters as $\lambda = 0.9, \omega_{22} = 3, \alpha = 0.005, \beta = 0.9, a = 1, b = 0.2$. The proposed PDE-ReLU-MHNN model is solved with tiny variations of ω_{33} in the range $[0, 1.5]$. The local maximum of variables is stored for each iteration and the numerical results are plotted in Fig. 6. It is observed that the dynamics of the proposed model has completely changed from what we observed with $\lambda = 1$. Besides, we extend this dynamic study in term of the fractional index to show a general view on its behavior. The experimental results are visualized in Fig. 7. Apparently, some periodic and chaotic states can be perceived in both cases though hyperchaos only exist in integer order case.

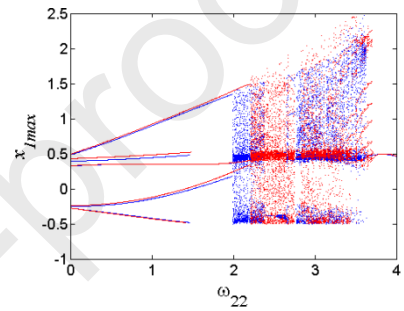


Fig. 4. Bifurcation diagram showing the coexistence of attractors.

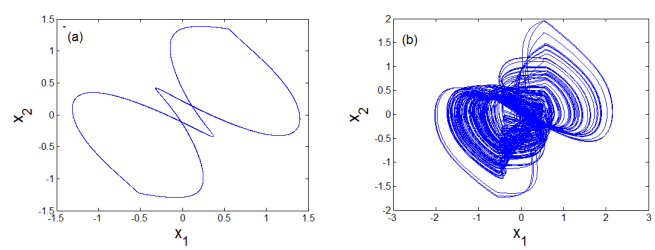


Fig. 5. Coexisting phase portraits of the proposed PDE-ReLU-MHNN model.

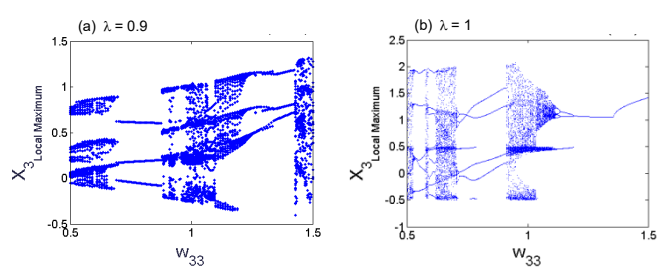


Fig. 6. Bifurcation diagrams for decimal and integer fractional indexes.

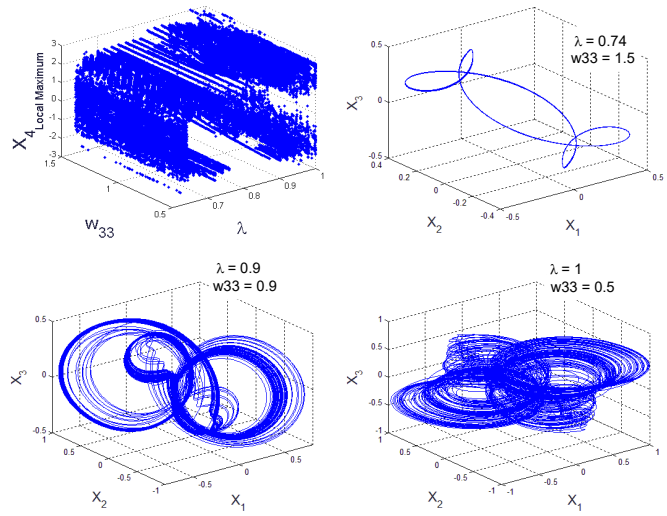


Fig. 7. Bifurcation diagram for varying both ω_{33}, λ and some periodic and chaotic attractors.

4. Adaptive Sparse Basis Compressive Sensing Model

As the emerging signal sampling paradigm, the compressive sensing technology with sparsity constraint breaks the sampling frequency limitation stipulated by the Nyquist sampling theorem, thereby greatly relieving the burden on sensor nodes. It points out that the finite-dimensional real natural signal with sparse representation can be accurately reconstructed from a small number of linear and non-adaptive sampling values.

In fact, given that natural signals generally have strong correlations in the spatial domain, their orthogonal transform coefficients tend to be sparse. We assume that $\{\psi_i\}_{i=1}^{N}$ is an orthogonal basis, then the natural signal $x \in \mathbb{R}^{N\times 1}$ can be expressed as $x = \Psi s$, where $s_i = \langle x, \psi_i \rangle$. Accordingly, the process of performing compressed sampling on signal x can be characterized as

$$y = \Phi x = \Phi \Psi s = \Theta s. \tag{23}$$

where $\Phi \in \mathbb{R}^{M\times N}$ and $\Theta \in \mathbb{R}^{M\times N}$ are denoted as measurement matrices acting on different domains, respectively.

For the decoder side, in the absence of noise perturbation, when the observed value y and the measurement matrix Φ are known, the reconstruction process of original signal can be characterized as the convex optimization problem with the minimum ℓ_0 norm as the optimization target, as given in the following equation.

$$P_0: \min \|s\|_0 \text{ s.t. } y = \Phi x = \Phi \Psi s. \tag{24}$$

Regarding the above equation, two issues need to be considered. The first one is whether the P_0 solution is unique and the second is whether Eq. (24) can be solved in polynomial time. For the first issue, when the measurement matrix satisfies the RIP, of whose the sufficient condition is that the measurement matrix is incoherent with the sparse transformation matrix, P_0 has a unique solution. For the remaining issue, although the P_0 solution is sparse, the arrangement of elements is uncertain, which belongs to the non-deterministic polynomial hard problem. Fortunately, scholars have proposed other countermeasures to accurately recover original signal, such as the base pursuit algorithm based on ℓ_1 norm, expressed as Eq. (25).

$$P_1: \min \|s\|_1 \text{ s.t. } y = \Phi x = \Phi \Psi s. \tag{25}$$

In short, the primary research contents of CS theory involve sparse representation, measurement encoding and decoding reconstruction. Therefore, one of the contributions for this work is to propose an approach of constructing adaptive sparse basis based on matrix decomposition theory. Specific details are as follows.

For the real signal $x \in \mathbb{R}^{N\times 1}$, assuming that the two orthogonal matrices (or called unitary matrices) generated after performing SVD on xx^T are denoted as U and V^T, as well as the diagonal matrix is expressed as Σ. Then, the signal x can be decomposed sparsely as Eq. (26), where its strict proof is provided in the Appendix at the end of this paper. Note that since xx^T is a real positive definite symmetric matrix, thus $U = V$ holds true.

$$x = Us \text{ or } s = U^T x. \tag{26}$$

Adequately, it indicates that the coefficient vector s has k-sparsity in the orthogonal space spanned by U. It is worth taking a moment to consider the security of proposed ASB-CS model, *i.e.*, whether the original real signal can be roughly reconstructed from the sparse orthonormal basis U without the matrix Σ. The answer is no that is because in the singular value decomposition, the orthogonal matrices U and V are not sole, while the opposite is true for the singular value matrix Σ. Therefore, its ambiguity that guarantees the security of proposed ASB-CS model does. Besides, the proposed adaptive sparse representation approach can be applied to the images with arbitrary resolution, since the SVD algorithm does not impose restriction on the dimensionality of matrix.

5. Application of Proposed ASB-CS Model in Medical Image Field

5.1. Technical Details of Proposed Medical Cryptosystem

The newly designed ASB-CS model is put into medical image manipulation to consider both its privacy and compressibility. The overall framework is presented in Fig. 8. As indicated in this figure, the cryptosystem is composed of adaptive compression, encryption and cipher stream construction processes. Concretely, taking advantage of its rich dynamics, the PDE-ReLU-MHNN model driven by the user-

specified keys is applied to construct the cipher streams for controlling the compression-encryption process. Later, the sparse coefficient matrix adaptively decomposed from plain medical image after undergoing a series of optimization manipulations is synchronously compressed and sampled through a hardware-friendly measurement matrix constructed via the hash chain algorithm. Afterwards, the bidirectional diffusion manipulation is performed on the compressed data to cover up its inherent statistical properties and simultaneously enhance its avalanche effect. For the sake of description, we assume that there exists a relationship $M = N$ for the dimensionality of a plain image. The specific implementation details are listed as following.

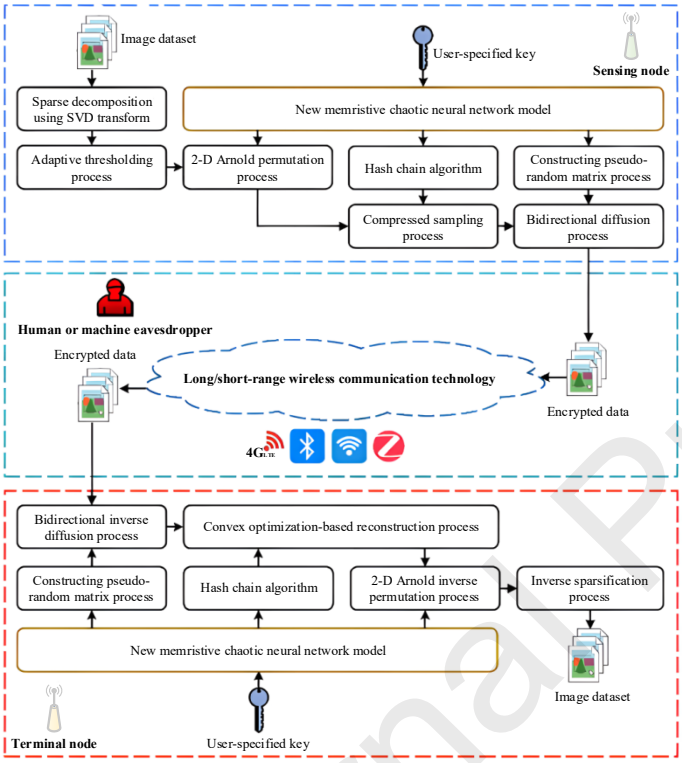


Fig. 8. Schematic diagram for the proposed medical data cryptosystem.

Step 1: First, in terms of the value of the fractional-order parameter λ, the algorithm for solving the differential equation defined in Eq. (10), including the Runge-Kutta method (*Butcher*, 1996) and predictor-corrector method (*Jhinga and Gejji*, 2018), is selected. Then, under the control of the user-specified key, the PDE-ReLU-MHNN model is iterated several times to construct the five pseudo-stochastic sequences $\left[\{X_i, Y_i, Z_i, U_i, W_i\}_{i=1}^{MN}\right]$ after their transient effects are eliminated.

Step 2: Referring to Section 4, the medical image data collected by sensor after the DCT process $P_1 \in \mathbb{N}^{M\times N}$ is adaptively decomposed into the coefficient matrix $P_2 \in \mathbb{R}^{M\times N}$. Considering that most of the coefficients after the orthogonal transform converge to 0, it is imperative to adopt some optimization treatments to ameliorate the sparsity of the matrix P_2.

Step 3: To this end, the coefficient matrix P_2 is first subjected to adaptive thresholding process. Specifically, the elements on the main diagonal of the singular value matrix Σ for the real positive definite matrix $P_1P_1^T$ are respectively recorded as the $\Delta = [\sigma_1, \sigma_2, \sigma_3, ..., \sigma_M]$. Later, the first index value for which the $\{\sigma_i\}_{i=2}^{M} \le \sigma_1 \times 10^{-b_1}$ $(b_1 \in \mathbb{N}^+)$ holds is recorded as pi. Next, the coefficient matrix P_2 is arranged in descending order, obtaining the ordered vector TP_2. Hence, the threshold value TV can be determined by Eq. (27). Finally, the adaptive thresholding process can be expressed by Eq. (28).

$$TV = \mathrm{abs}\left(TP_2\left(\mathrm{floor}\left(pi^2\right)\right)\right). \tag{27}$$

$$P_2\left(\ \mathrm{abs}\left(P_2\right) \le TV\right) = 0. \tag{28}$$

Step 4: During the inchoate experiments, we found that the main energy of the matrix P_1 is concentrated on the left side of the matrix P_2, which is obviously not conducive to parallel compression. Note that this kind of energy distribution is radically differs from the one obtained by means of wavelet decomposition. Therefore, we employ the fast and efficient 2-D Arnold scrambling algorithm to distribute the primary energy uniformly over the entire region, as displayed in Eq. (29).

$$P_3(i,j) = P_2(k_1, k_2), i, j \in \{1, 2, ..., M\}. \tag{29}$$

where

$$[k_1, k_2]^T = \mathrm{mod}\left(\begin{bmatrix} 1 & T_1 \\ T_2 & T_1T_2+1 \end{bmatrix}\begin{bmatrix} i \\ j \end{bmatrix}, \begin{bmatrix} M \\ N \end{bmatrix}\right) + \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix}. \tag{30}$$

Here, the parameter $\varepsilon \in \mathbb{N}^+$ is adopted to adjust the index disparities that exist in various implementation platforms. For example, the ε is set to one in the MATLAB simulation platform. Moreover, the symbols T_1 and T_2 are the ordered index vectors obtained by sorting two stochastic chaotic sequences selected from the set $\left[\{X_i, Y_i, Z_i, U_i, W_i\}_{i=1}^{MN}\right]$.

Step 5: In the following, under the control of the generated chaotic sequence, iterative operations are carried out on the hashing algorithm considering its pseudo-random and sensitive properties to construct the hardware-friendly measurement matrix $\Phi \in \mathbb{N}^{\mathrm{floor}(C_R M)\times N}$, where the symbol C_R means the user-specified compression ratio. Please refer to (*Li*, 2018) for more implementation details. In the meantime, to minimize the information loss in the compression process, all the 0 elements in the matrix Φ are altered to -1. Afterward, the compressed sampling process for the matrix P_3 with the parallel-wise manner can be expressed by Eq. (31).

$$P_4 = \Phi P_3 \approx \Phi U^T P_1. \tag{31}$$

Step 6: After trading off the operation complexity and error loss of various quantization approaches, we utilize the uniform quantization to process the matrix P_4, as provided in Eq. (32), where the symbol $b_2 \in \mathbb{N}^+$ signifies the bit depth of stored medical image data.

$$P_5 = \text{round}\left(2^{b_2} \cdot \left(P_4 - \min(P_4)\right) \cdot \left(\max(P_4) - \min(P_4)\right)^{-1}\right). \quad (32)$$

Step 7: Segments S_1 and S_2 of both length $\text{floor}(C_R M) \cdot N$ are stochastically truncated from the sequences generated in **Step 1** and then mapped into integers between 0 and 2^{b_2}. The mapping function is $\{MS_i\}_{i=1}^{2} = \text{mod}\left(\text{floor}\left(\{S_i\}_{i=1}^{2} \cdot 10^{10}\right), 2^{b_2}\right)$, concretely. In the end, the encrypted medical image data P_7 can be determined by Eq. (33), where $Q = \text{floor}(C_R M)$.

$$\begin{cases} \begin{cases} P_6(1) = \text{mod}\left(B_0 + MS_1(1) + P_5(1), 2^{b_2}\right) \\ P_6(i) = \text{mod}\left(P_6(i-1) + MS_1(i) + P_5(i), 2^{b_2}\right) \end{cases} \\ \begin{cases} P_7(QN) = \text{mod}\left(B_1 + MS_2(QN) + P_6(QN), 2^{b_2}\right) \\ P_7(QN-i) = \text{mod}\left(P_7(QN-i+1) + MS_2(QN-i) + P_6(QN-i), 2^{b_2}\right) \end{cases} \end{cases} \quad (33)$$

With respect to the corresponding decryption scheme, given that the proposed privacy protection scheme belongs to the category of symmetric cryptography, the decrypted image can be reconstructed accurately by performing the inverse process of **Steps 2-7** on the cipher image P_7 when the sender-specified key is mastered by the legitimate recipient. Furthermore, another inescapable issue worth taking time to consider is how to transfer the sparse representation matrix U. Currently, the alternative solution is to fit this matrix by a specific orthogonal polynomial for alleviating the transmission burden, which is also our further research route.

5.2. Engineering Application of Our Proposal

With the growing maturity of lightweight wearable medical data collection devices, family members or medical specialists can conveniently access various physical data of patients by means of the visualization program installed in mobile devices. Considering that these data are extremely sensitive for patients, we introduce a novel data encryption scheme based on the proposed ASB-CS model. Its model architecture at the application level is illustrated in Fig. 9. First, the newly designed memritive chaotic neural network is placed in the physical layer of sensing device for generating cipher flows under the control of secret keys. Then, the data collected in the information perception layer is fed into the proposed cryptosystem, followed by being packaged in the network layer and sent to the third-party cloud providers for storage. Finally, when authorized users need to access the patient's raw data, they can decrypt the cipher data downloaded from the cloud via their mobile device or terminal.

In fact, the core component, the proposed ASB-CS model, is a complexity transfer process, which means that the low-power sampling at the transmitter side comes at the cost of the high-complexity reconstruction algorithm at the receiver side. Fortunately, with the increasing computational power of smart terminals and the rapid development of cloud computing technology, the high complexity issue of reconstruction algorithm can be effectively solved in the cloud or at the terminal.

In comparison with the medical image encryption schemes built upon the scrambling-diffusion architecture, such as (*Wu*, 2023; *Jain*, 2021; *Banu and Amirtharajan*, 2020), our scheme possesses a lightweight compression layer and a chaotic system with more complicated dynamics, thereby conserving the overhead and providing a higher level of key security. Besides, as far as the related schemes (*Chai*, 2023; *Zhang*, 2015) that also incorporate compressive sensing are concerned, they suffer from the performance constraint in terms of reconstruction owing to using a static sparse basis. Moreover, the performance superiority of our proposed scheme will be verified in the following.

Last but not least, for the ethical considerations, we need to inform user about the hazards of privacy leakage, and it is required to obtain the users' consent to handle their medical image data with the proposed cryptographic scheme in the practical applications. Additionally, the data processing procedure is transparent to the user, while they are also entitled to the access control and authorization for secondary use of private data to minimize the potential moral hazards.

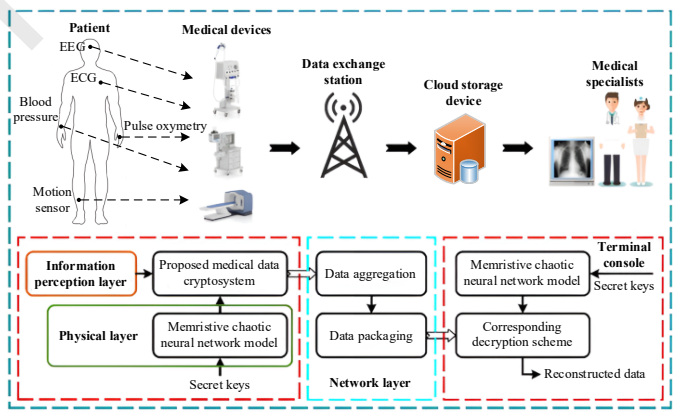


Fig. 9. Engineering application model of the proposed medical data encryption scheme.

6. Simulation Results and Performance Evaluation

6.1. Implementation Details

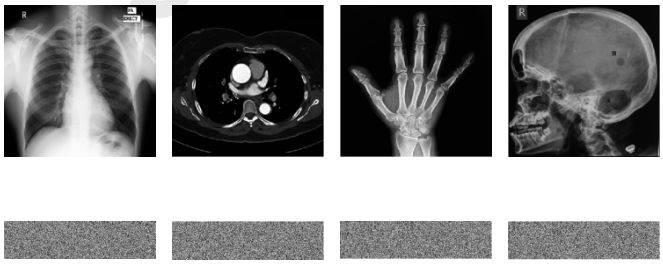
The mainstream simulation platform MATLAB R2015b is adopted to verify the correctness and effectiveness of proposed medical cryptosystem in this paper, which is installed in the Windows 11 operating system with an i7-13700KF central processor. Besides, the parameters to be specified by user in the encryption phase are configured as follows. The compression rate C_R is 0.25. The bit depth of medical image data b_2 is 16.

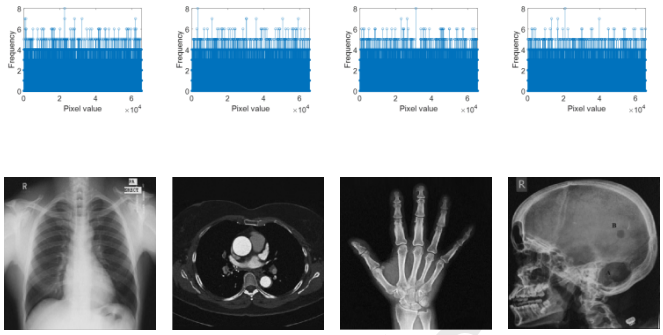
The diffusion parameters B_0 and B_1 are both 1270. The initial states and the fractional order λ of the proposed PDE-ReLU-MHNN model are respectively $[0.1,-0.02,0.1,0.1,1.0]^T$ and 1. Meanwhile, the first 100 elements of chaotic trajectories are dropped to remove its transient effects. Then, the value of adjustment parameter b_1 should be determined in accordance with the category of medical image. In decryption phase, the Orthogonal Newton Smoothing ℓ_0 norm (ONSL0) method is employed to precisely reconstruct the sparse coefficient matrix from compressed data. Last but not the least, the medical images for simulation are downloaded from the Open Access Biomedical Image Search Engine (OABISE: https://openi.nlm.nih.gov/).

6.2. Encryption and Decryption Results

First, the resolution of four medical images downloaded from the OABISE are reshaped to 512×512. The purpose of this manipulation is to be convenient for the sparse decomposition. Afterward, they are subjected to the proposed medical data encryption manipulations. The acquired simulation images and numerical results are presented in Fig. 10. Thereinto, the symbols $PSNR_{\text{dec}}$ and $SSIM_{\text{dec}}$ indicate the Peak Signal-to-Noise Ratio (PSNR) and Structural SIMilarity (SSIM) between the image to be encrypted and the corresponding decrypted image, whose specific mathematical definitions can be referred to (*Xiao*, 2021).

From the qualitative point of view, the plain medical images are synchronously compressed and encrypted into the unrecognizable images without any semantic features. Moreover, the histograms of encrypted images tend to be flat, effectively masking the statistical properties of their corresponding plain images. In other respects, the decrypted images recovered from cipher images have no obvious visual discrepancy with the matching plain medical images. Numerically, the values of $PSNR_{\text{dec}}$ and $SSIM_{\text{dec}}$ all exceed 35.50 *dB* and 0.85, respectively. In general, our proposed medical cryptosystem can balance its security and compressibility well. In the following, the proposed scheme will be quantitatively evaluated from the perspective of its security, robustness and execution efficiency, where the commonly used metrics to evaluate security include key space and its sensitivity, correlation coefficient, number of pixel change rate, as well as unified average change intensity.



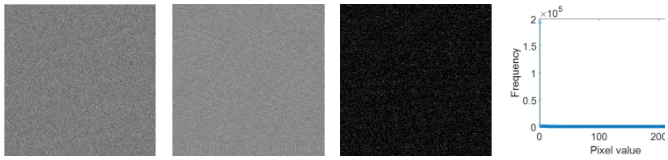


$PSNR_{\text{dec}}=37.92$ $PSNR_{\text{dec}}=35.62$ $PSNR_{\text{dec}}=37.21$ $PSNR_{\text{dec}}=37.42$

Fig. 10. Simulation results of the proposed scheme. The first to fourth rows are medical images, denoted as "*image-01P~image-04P*", compressed cipher images, histograms of corresponding cipher images and decrypted images.

6.3. Security Evaluation

(1) Analysis of anti-exhaustive attack: The computational security strength of our proposed encryption scheme depends primarily on the key space size and key sensitivity, i.e., whether an attacker can successfully traverse the entire key space in polynomial time by invoking all the computational resources available to him. Unfortunately, this kind of exhaustive enumeration-based attacks are generally futile for chaotic cryptosystems. Looking back at this scheme, the key space comprises mainly the five initial states of the newly designed PDE-ReLU-MHNN model. Under the condition that the double precision is 10^{-14}, the key space of our scheme exceeds $10^{70}\gg2^{100}$ considerably, exhibiting an exponential form. It is worth mentioning that the other encryption parameters can also be considered as the user-specified secret keys. In addition, the results of key sensitivity analysis for the decryption process are drawn in Fig. 11, where the perturbation added to key x_1 is $\pm10^{-14}$. Apparently, deriving the prior knowledge associated with plaintext data from a series of reconstructed images is difficult when there exists a subtle discrepancy in one of the decryption keys. Therefore, it can be concluded that our proposed medical data encryption scheme is effectually immune to various exhaustive attacks.



(a) Decrypted image D_1 (b) Decrypted image D_2 (c) Differential image $|D_1-D_2|$ (d) Histogram of differential image

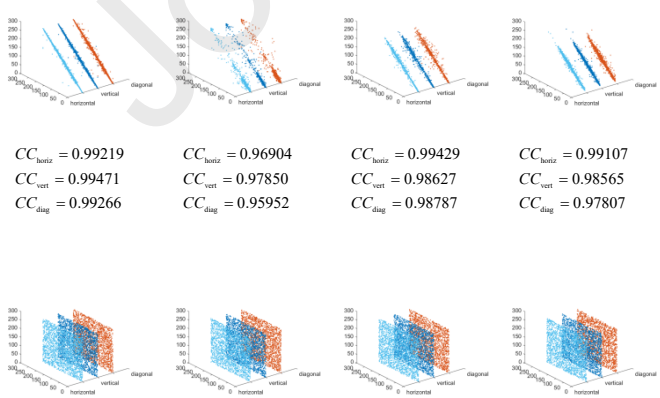
Fig. 11. Results of key sensitivity analysis for image "*image-04P*".

(2) Analysis of anti-statistical attack: According to the definition of information-theoretic security proposed by Shannon, an absolutely secure cryptosystem requires a guarantee that the attacker has no access to any useful information about the plaintext u from the illegally stolen ciphertext v, i.e., it satisfies $P(u|v)=P(u)$. In other words, the mutual information between plaintext and ciphertext is zero, that is, $I(u;v)=0$. Unfortunately, the image distribution for calculating mutual information is extremely difficulty to be described precisely by modeling. Besides, if and only if the energy information of ciphertext leaks the plaintext-related information, this case is termed the asymptotic spherical security (*Candes and Tao*, 2005). It also means that the data can be theoretically secure by masking the energy and statistical information of plaintext. Hence, we adopt Correlation Coefficient (CC) to approximately evaluate the correlation distribution of pixels between plain medical image and matched cipher image. Its mathematical definition is determined by the following Eq. (34).

$$CC(x,y)=\frac{\sum_{i=1}^{N}\left(x_i-E(x)\right)\left(y_i-E(y)\right)}{\sqrt{\sum_{i=1}^{N}\left(x_i-E(x)\right)^2}\sqrt{\sum_{i=1}^{N}\left(y_i-E(y)\right)^2}} \tag{34}$$

where $E(x)=\sum_{i=1}^{N}x_i\Big/N$. This is the same for $E(y)$. N represents the randomly sampled pixel pairs.

Under the condition that $N=2000, C_R=0.75$ and the medical images to be encrypted are chosen as the "*image-01P~ image-04P*", the qualitative and quantitative simulation results regarding the correlation coefficient analysis are elaborated into Fig. 12. From the obtained experimental results, it seems that the distribution among adjacent pixels in the plain image exhibits a positive correlation, which is completely opposite to that of the cipher image. Numerically, the absolute value for the correlation coefficient of adjacent pixels in cipher image is approaching zero. Finally, in conjunction with the simulation results in Figs. 10 and 12, it appears that our encryption scheme can effectively conceal the energy of plain medical images as well as the statistical properties of adjacent pixels.



$CC_{horiz}=0.99219$	$CC_{horiz}=0.96904$	$CC_{horiz}=0.99429$	$CC_{horiz}=0.99107$
$CC_{vert}=0.99471$	$CC_{vert}=0.97850$	$CC_{vert}=0.98627$	$CC_{vert}=0.98565$
$CC_{diag}=0.99266$	$CC_{diag}=0.95952$	$CC_{diag}=0.98787$	$CC_{diag}=0.97807$

$CC_{horiz}=-0.00251$	$CC_{horiz}=0.02194$	$CC_{horiz}=-0.00394$	$CC_{horiz}=-0.00716$
$CC_{vert}=-0.030027$	$CC_{vert}=0.00473$	$CC_{vert}=0.0028960$	$CC_{vert}=-0.040571$
$CC_{diag}=0.0048570$	$CC_{diag}=0.00058$	$CC_{diag}=0.0018220$	$CC_{diag}=0.0057340$

Fig. 12. Results of correlation coefficient analysis. The first and second rows of correlation coefficient figures represent that of the plain images and the cipher images, separately.

(3) Analysis of anti-differential attack: Differential analysis-based attack paradigm is highly favored by the attacker and cryptanalyst. Currently, the main-stream metrics for measuring the immunity of cryptosystem to this type of attack are the Number of Pixel Change Rate (NPCR) and the Unified Average Change Intensity (UACI). Their mathematical definitions are determined by the following Eqs. (35) and (36), where the $[\![\cdot]\!]$ denotes the Iverson bracket, i.e., its output value is one if the condition inside bracket is satisfied and the opposite is zero. Besides, the symbols $C_1\in\mathbb{N}^{M\times N}$ and $C_2\in\mathbb{N}^{M\times N}$ stand for the cipher images generated from encrypting two plain images that differ by only one bit.

$$NPCR=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[\![C_1(i,j)\neq C_2(i,j)]\!]\times 100\% \tag{35}$$

$$UACI=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|C_1(i,j)-C_2(i,j)\right|}{255}\times 100\% \tag{36}$$

Sequentially select a pixel value in the medical images "*image-01P~image-04P*" at random to add 1 bit. Then, the modified image and the original version are fed into the proposed encryption scheme individually. Finally, the performance metrics between the generated cipher image pairs are calculated and listed in Table I. As known to us, the expected NPCR and UACI values are 99.61% and 33.46%, respectively. From the obtained numerical results, it clearly appears that the proposed encryption scheme built upon the ASB-CS model can withstand the differential analysis-based attack schemes. This is largely attributed to employing the bidirectional diffusion ma-

nipulation with avalanche effect.

TABLE I

RESULTS OF CORRELATION COEFFICIENT ANALYSIS

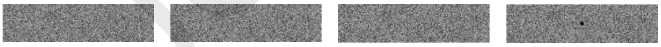
(4) Comparison of quantitative security performance: In the preceding sub-sections, the proposed medical data encryption scheme is analyzed minutely from multiple perspectives of security, respectively. Next, we will quantitatively compare our scheme with the existing state-of-the-art schemes from the aspects of correlation coefficient, NPCR, UACI, and key space. Following the mainstream comparative approach, the image "*Lena*" with resolution of 512×512 is selected as plain image to

be encrypted in the performed experiments and the adopted secret keys are consistent with those described in Section 6.1. Eventually, the numerical results are elaborated in Table II. Besides, it is worth noting that the simulation results of the comparison scheme are derived from references.

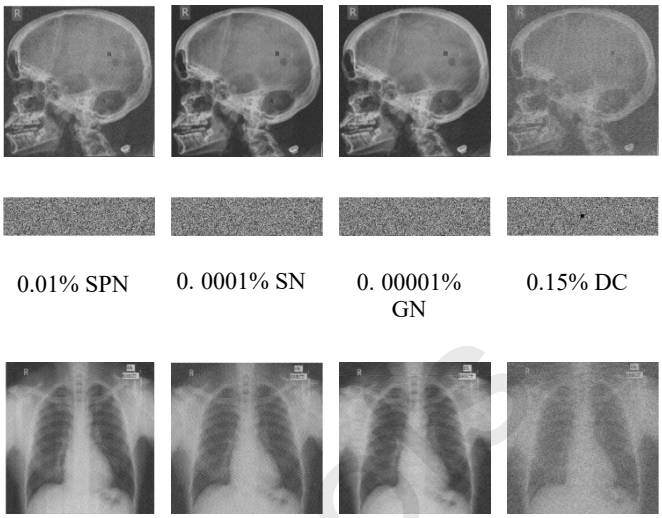
By comparing the numerical values of the security performance metrics for all schemes separately, it is observed that the cipher image yielding from our scheme has a considerably lower level of correlation coefficient. Its NPCR and UACI values are more closely approximated to the expected values. Apart from that, our scheme possesses other superiorities, such as the single-round encryption mechanism to diminish the time expenditure and the compression-encryption architecture, thereby enhancing its transmission efficiency. When considering together, it can be concluded that the proposed medical data cryptosystem can more effectively withstand a variety of commonly used attack paradigms, including statistical attack, differential attack, and exhaustive attack.

6.4. Robustness Evaluation

Besides its security, robustness is also an essential criterion for the performance of an algorithm, which is motivated by the realistic channel conditions. In general, we adopt three types of noise, namely, Salt & Pepper Noise (SPN), Speckle Noise (SN) and Gaussian Noise (GN), as well as Data Cropping (DC) to simulate the channel noise and the data packet loss. Not surprisingly, we load each of these four emulated attacks with different normalization strengths onto cipher image. Later, the corresponding reconstructed images are presented in Fig. 13. Apparently, the decrypted images recovered from the contaminated cipher images are visually semantic and recognizable, indicating that the proposed scheme possesses a certain degree of immunity to these four attacks. Besides, it is worth taking a moment to clearly explain the influence of diffusion operation, the essential component of cryptosystem, on the robustness of an algorithm. The purpose of this component is to spread the elements of plaintext to the whole ciphertext as much as possible. In turn, the tampered ciphertext will affect the reconstructed plaintext to some extent. Given that medical image is of ultra-redundant and semantic properties, therefore reconstructed image will certainly contain a certain amount of raw plaintext information.



0.01% SPN 0. 0001% SN 0. 00001% GN 0.15% DC



0.01% SPN 0. 0001% SN 0. 00001% GN 0.15% DC

Fig. 13. Results of robustness analysis.

6.5. Execution Efficiency Evaluation

Finally, let us analyze the execution efficiency of the proposed encryption scheme. Given that there exist multiple factors affecting the encryption time, including but not limited to central processor, simulation platform and parallel computing, we first evaluate the percentage of each part of the encryption scheme to the total manipulation time, as depicted in Fig. 14. Secondly, its time complexity is calculated. As can be seen in Fig. 14, the time cost for solving the chaotic trajectories of the proposed PDE-ReLU-MHNN model accounts for more than 89% of the total manipulation time. In the practical application scenarios, the cipher flows can be prestored into the random-access memory of medical devices to economize on time over-head and computational resources. Inversely, the time expenditure for the other parts is comparatively lower.

By carefully analyzing the proposed encryption scheme, we find that the time complexity occupied by solving the trajectory of the newly designed PDE-ReLU-MHNN model and performing the SVD manipulation on medical image is the two largest.Moreover, their respective time complexity is $O(k_1N^2)$ and $O(k_2N^3)$ under the condition that the dimensionality of medical image exists $M=N$, where the symbols k_1 and k_2 denote a certain constant, respectively. Since the maximum magnitude of time complexity greatly determines the actual running time, the gross time complexity of our scheme is $O(N^3)$. With respect to the corresponding decryption scheme, its time complexity is highly dependent on the employed sparse coefficient reconstruction algorithm.

TABLE II

QUANTITATIVE COMPARISON WITH SOME EXISTING ENCRYPTION SCHEMES IN TERMS OF SECURITY

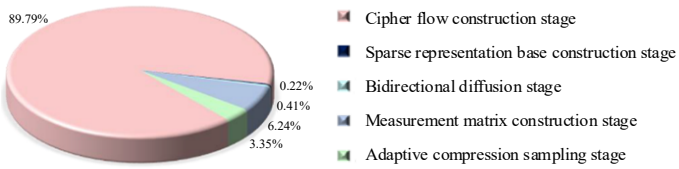


Fig. 14. Percentage of total encryption time for each phase.

7. Conclusion

In this paper, we proposed a novel adaptive sparse basis compressive sensing model by leveraging SVD approach for medical image manipulation, aimed at addressing users' concerns regarding the security of their personal medical data. The proposed data encryption scheme involves three phases. First, we exploit the hyperchaotic property of the newly designed PDE-ReLU-MHNN model to construct unpredictable cipher flows and random seeds for generating a hardware-friendly measurement matrix. Afterward, with the assistance of the hashing algorithm, the plain medical image is adaptively compressed through the ASB-CS model. Next, the bidirectional nonlinear diffusion manipulation is applied on the compressed image to yield an unrecognizable cipher image. Finally, the feasibility of the proposed data encryption scheme is evaluated from multiple perspectives, including reconstruction performance, security, robustness, and execution efficiency. Moreover, the comparative results indicate that our scheme is comparable to existing state-of-the-art schemes. In future research, we intend to investigate a convenient approach for transferring the sparse representation matrix to alleviate the transmission burden.

Acknowledgment

We are especially grateful to Professor Jianhua Wu of the School of Information Engineering, Nanchang University in China for reviewing our manuscript and providing valuable comments.

Appendix

Proof: Let us assume that the singular values σ_i of matrix xx^T are mainly concentrated in the first k elements on the diagonal of matrix Σ and the remainder tends to 0. Besides, there exists inequality $\sigma_1 > \sigma_2 > ... > \sigma_k > ... > \sigma_N$. The estimated value of coefficient vector $s = [s_1, ..., s_k, ..., s_N]$ is $\hat{s} = [\hat{s}_1, ..., \hat{s}_k, 0, ..., 0]$, then the estimated error is:

$$\begin{aligned} E\left(\| s - \hat{s} \|_2^2\right) &= E\left(\sum_{i=k+1}^{N} s_i^2\right) = E\left(\sum_{i=k+1}^{N} U_i^T x \left(U_i^T x\right)^T\right) \\ &= E\left(\sum_{i=k+1}^{N} U_i^T x x^T U_i\right) = \sum_{i=k+1}^{N} U_i^T E\left(x x^T\right) U_i \\ &= \sum_{i=k+1}^{N} U_i^T \sigma_i U_i \\ &= \sum_{i=k+1}^{N} \sigma_i \to 0. \end{aligned} \tag{37}$$

Conflicts of Interest

The authors report no conflicts of interest. The authors alone are responsible for content and writing of this paper.

Data Availability Statements

The datasets generated and analyzed during the current study are available from the corresponding author upon a reasonable request.

References

Ahmad, S., Ullah, A., and Akgul, A. (2021). Investigating the complex behaviour of multi-scroll chaotic system with Caputo fractal-fractional operator. Chaos, Solitons & Fractals, https://doi.org/10.1016/j.chaos.2021.110900.

Banu S, A., Amirtharajan, R. (2020). A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach. Med. Biol. Eng. Comput., 58, 1445-1458. https://doi.org/10.1007/s11517-020-02178-w.

Butcher, J. C. (1996). A history of Runge-Kutta methods. Appl. Numer. Math., 20, 247-260. https://doi.org/10.1016/0168-9274(95)00108-5.

Candes, J. E., and Tao, T. (2005). Decoding by linear programming. IEEE Trans. Inf. Theory, 51, 4203-4215. https://doi.org/10.1109/TIT.2005.858979.

Candes, J. E., Romberg, J., and Tao, T. (2006). Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. IEEE Trans. Inf. Theory, 52, 489-509. https://doi.org/10.1109/TIT.2005.862083.

Canh, T. N., and Jeon, B. (2021). Restricted structural random matrix for compressive sensing. Signal Process.-Image Commun., https://doi.org/10.1016/j.im-age.2020.116017.

Chai, X. L., Fu, J. Y., Gan, Z. H., Lu, Y., Zhang, Y. S., Han, D. J. (2023). Exploiting semi-tensor product compressed sensing and hybrid cloud for secure

medical image transmission. IEEE Internet of Things Journal, 10, 7380-7392, https://doi.org/10.1109/JIOT.2022.3228781.

Chua, L. (1971). Memristor-the missing circuit element. IEEE. Trans. Circuit Theory, 18, 507-519, https://doi.org/10.1109/TCT.1971.1083337.

Chen, C., Sun, K. H., and He, S. B. (2020). An improved image encryption algorithm with finite computing precision. Signal Process., https://doi.org/10.1016/j.sigpro.2019.107340.

Cheng, Q. S., Li, H. L., Wu, Q. B., Ma, L., and Ngan, K. N. (2020). Parametric deformable exponential linear units for deep neural networks. Neural Netw. 125, 281-289. https://doi.org/10.1016/j.neunet.2020.02.012.

Donoho, L. D. (2006). Compressed sensing. IEEE Trans. Inf. Theory, 52, 1289-1306. https://doi.org/10.1109/TIT.2006.871582.

Fang, H., Vorobyov, S. A., Jiang, H., and Taheri, O. (2014). Permutation meets parallel compressed sensing: How to relax restricted isometry property for 2D sparse signals. IEEE Trans. Signal Process., 62, 196-210. https://doi.org/10.1109/TSP.2013.2284762.

Gass, S. I., and Rapcsak, T. (2004). Singular value decomposition in AHP. Eur. J. Oper. Res., 154, 573-584. doi: 10.1016/S0377-2217(02)00755-5.

Gayathri, J., and Subashini, S. (2019). An efficient spatiotemporal chaotic image cipher with an improved scrambling algorithm driven by dynamic diffusion phase. Inf. Sci., 489, 227-254. https://doi.org/10.1016/j.ins.2019.01.082.

Huang, R., and Sakurai, K. (2011). A robust and compression-combined digital image encryption method based on compressive sensing. In Proceedings of the Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, https://doi.org/10.1109/IIHMSP.2011. 53.

Hossein, S. A., Tabatabaei, A. E., and Zivic, N. (2012). Security analysis of the joint encryption and compressed sensing. In Proceedings of the 20th Telecommunications Forum (TELFOR). https://doi.org/10.1109/TELFOR.2012. 6419328.

Hu, G. Q., Xiao, D., Wang, Y., and Xiang, T. (2017). An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications. J. Vis. Commun. Image Represent, 44, 116-127. https://doi.org/10.1016/j.jvcir.2017.01.022.

Hu, G. Z., and Li, B. B. (2021). Coupling chaotic system based on unit transform and its applications in image encryption. Signal Process., https://doi.org/10.1016/j.sigpro.2020.107790.

Hua, Z. Y., Zhang, K. Y., Li, Y. M., and Zhou, Y. C. (2021). Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing. Signal Process., https://doi.org/10.1016/j.sigpro.2021.107998.

Jafarpour, S., Xu, W. Y., Hassibi, B., and Calderbank, R. (2009). Efficient and robust compressed sensing using optimized expander graphs. IEEE Trans. Inf. Theory, 55, 4299-4308. https://doi.org/10.1109/TIT.2009.2025528.

Jain, K., Aji, A., Krishnan, P. (2021). Medical image encryption scheme using multiple chaotic maps. Pattern Recogn. Lett., 152, 356-364. https://doi.org/10.1016/j.patrec.2021.10.033.

Jhinga, A., and Gejji, V. D. (2018). A new finite-difference predictor-corrector method for fractional differential equations. Appl. Math. Comput., 336, 418-432. https://doi.org/10.1016/j.amc.2018.05.003.

Jiang, D. H., Liu, L. D., Zhu, L. Y., Wang, X. Y., Rong, X. W. and Chai, H. X. (2021). Adaptive embedding: A novel meaningful image encryption scheme based on parallel compressive sensing and slant transform. Signal Process., https://doi.org/10.1016/j.sigpro.2021.108220.

Klema, V., and Laub, A. (1980). The singular value decomposition: Its computation and some applications. IEEE Trans. Autom. Control, 25, 164-176. https://doi.org/10.1109/TAC.1980.1102314.

Kumar, A. A., and Makur, A. (2009). Lossy compression of encrypted image by compressive sensing technique. In Proceedings of the TENCON 2009 - 2009 IEEE Region 10 Conference. https://doi.org/10.1109/TENCON.2009.5395999.

Kari, A. P., Navin, A. H., Bidgoli, A. M., and Mirnia, M. (2021). A new image encryption scheme based on hybrid chaotic maps. Multimed. Tools Appl., 80, 2753-2772. https://doi.org/10.1007/s11042-020-09648-1.

Li, L. X., Peng, H. P., Liu, L. W., and Yang, Y. X. (2018). An efficient and secure transmission model based on compressive sensing. In Proceedings of the International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec), https://doi.org/10.1109/SocialSec.2018.8760382.

Lai, Q., Hu, G. W. Erkan, U., and Toktas, A. (2023). High-efficiency medical image encryption method based on 2D Logistic-Gaussian hyperchaotic map. Appl. Math. Comput., https://doi.org/https://doi.org/10.1016/j. amc.2022.127738.

Niu, Z. F., Zheng, M. W., Zhang, Y. P., and Wang, T. Z. (2020). A new asymmetrical encryption algorithm based on semitensor compressed sensing in WBANs. IEEE Internet Things J. 7, 734-750. https://doi.org/10.1109/JIOT.2019.2953519.

Rachlin Y., and Baron, D. (2008). The secrecy of compressed sensing measurements. In Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing, https://doi.org/10.1109/ALLERTON.2008.4797641.

Rech, P. C. (2011). Chaos and hyperchaos in a Hopfield neural network. Neurocomputing, 74, 3361-3364. https://doi.org/10.1016/j.neucom.2011.05.016.

Raza, S. F., and Satpute, V. (2019). A novel bit permutation-based image encryption algorithm. Nonlinear Dyn., 95, 859-873. https://doi.org/10.1007/s11071-018-4600-8.

Sethi, J., Bhaumik, J., and Chowdhury, A. S. (2022). Joint video compression and encryption using parallel compressive sensing and improved chaotic maps. Digit. Signal Prog., https://doi.org/10.1016/j.dsp.2022.103746.

Wu, Y. R., Zhang, L. L., Berretti, S., Wan, S. (2023). Medical image encryption by content-aware DNA computing for secure healthcare. IEEE T. Ind. Inform., 19, 2089-2098. https://doi.org/10.1109/TII.2022.3194590.

Xue, W. L., Luo, C. W., Shen, Y. R., Rana, R., Lan, G. H., Jha, S., Seneviratne, A., and Hu, W. (2021). Towards a compressive-sensing-based lightweight encryption scheme for the internet of things. IEEE. Trans. Mob. Comput., 20, 3049-3065. https://doi.org/10.1109/TMC.2020.2992737.

Xiao, D., Zhao, M. H., and Wang, M. D. (2021). Low-cost and secure multi-image encryption scheme based on P-tensor product compressive sensing. Opt. Laser Technol., https://doi.org/10.1016/j.optlastec.2021.107077.

Yang, Y. G., Wang, B. P., Yang, Y. L., Zhou, Y. H., Shi, W. M., and Liao, X. (2022). A visually meaningful image encryption algorithm based on adaptive 2D compressive sensing and chaotic system. Multimed. Tools Appl., 82, 22033-22062. https://doi.org/10.1007/s11042-021-11656-8.

Zhu, L. Y., Song, H. S., Zhang, X., Yan, M. D., Zhang, T., Wang, X. Y., and Xu, J. (2020). A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding. Signal Process. https://doi.org/10.1016/j.sigpro.2020.107629.

Zhu, L. Y., Jiang, D. H., Ni, J. Q., Wang, X. Y., Rong, X. W., Ahmad, M., and Chen, Y. P. (2022a). A stable meaningful image encryption scheme using

the newly-designed 2D discrete fractional-order chaotic map and Bayesian compressive sensing. Signal Process., https://doi.org/10.1016/j.sigpro.2022.108489.

Zhu, L. Y., Jiang, D. H., Ni, J. Q., Wang, X. Y., Rong, X. W., and Ahmad, M. (2022b). A visually secure image encryption scheme using adaptive-thresholding sparsification compression sensing model and newly-designed memristive chaotic map. Inf. Sci., 607, 1001-1022. https://doi.org/10.1016/j.ins.2022.06.011.

Zhang, H., Chen, J. X., Zhang, L. Y., Fu, C., Gravina, R., Fortino, G., and Lv, Z. H. (2022). Low-cost and confidential ECG acquisition framework using compressed sensing and chaotic systems for wireless body area network. IEEE J. Biomed. Health Inform., 26, 5783-5792. https://doi.org/10.1109/JBHI. 2022.3206232.

Zhang, L. B., Zhu, Z. L., Yang, B. Q., Liu, W. Y., Zhu, H. F., Zou, M. Y. (2015). Medical image encryption and compression scheme using compressive sensing and pixel swapping based permutation approach. Math. Probl. Eng., 2015, 940638. https://doi.org/10.1155/2015/940638

Credit Author Statement

Donghua Jiang: Methodology, Data curation, Writing-Original draft preparation.

Nestor Tsafack: Data curation, Software, Writing- Reviewing and Editing.

Wadii Boulila: Data curation, Conceptualization, **Writing- Reviewing and Editing.**

Jawad Ahmad: Methodology, **Writing- Reviewing and Editing.**

Barba-Franco J.J.: Software**, Writing- Reviewing and Editing.**