A Novel Dynamic Hill Cipher and Its Applications on Medical IoT

Jie Jin, Mengfan Wu, Aijia Ouyang, Keqin Li, *Fellow, IEEE*, and Chaoyang Chen, *Senior Member, IEEE*

***Abstract*—Cryptography is one of the most important areas in information security. Cryptography ensures secure communication and data privacy, and it is increasingly being applied in healthcare and related fields. As an important classical cryptographic method, the Hill cipher has always been closely studied by experts and scholars. In order to enhance the security of the conventional Hill cipher (CHC), a novel dynamic Hill cipher (NDHC) is proposed in this work. The proposed NDHC not only replaces the static key matrix of the CHC with a time-varying dynamic key matrix (TVDKM) to change the image pixel values over time t but also uses the Logistic chaos sequence scrambling the image pixel positions, which greatly enhances the security of the CHC. However, how to effectively obtain the dynamic inversion key matrix (DIKM) of the TVDKM becomes an urgent issue in the NDHC decryption. In order to quickly find the DIKM, a fixed-time convergence fuzzy zeroing neural network (FTCF-ZNN) model is constructed, and the convergence and robustness of the FTCF-ZNN model for solving the DIKM are verified through theoretical analysis and comparative experimental results. Moreover, the effectiveness and security of the proposed NDHC for medical images encryption and decryption are also validated by experiments.**

***Index Terms*—Chaos sequence, encryption and decryption, fuzzy logic, Hill cipher, zeroing neural network.**

I. Introduction

With the widespread popularization of the IoT and the advent of the information age, numerous information security issues have emerged, such as privacy breaches, information security becomes increasingly important nowadays. The emergence and development of cryptography provide a safeguard for solving information security problems, and play a crucial role in medical confidentiality. In medical diagnostics, various imaging techniques are used to process different cellular or organ lesions, including positron emission tomography (PET) [1], single-photon emission computed tomography (CT) (SPECT) [2], CT [3], and magnetic resonance imaging (MRI) [4]. Medical institutions encrypt sensitive information, such as patient records, diagnostic results, and case histories to ensure that unauthorized personnel cannot access or view this information during storage. Medical data sharing forms the basis of cooperation between medical institutions, but privacy issues are also the main obstacle to data sharing between institutions. Therefore, to address the issue of information leakage, encrypting private information is very necessary. Cryptography, as a popular research field, has important applications in message authentication [5], secure communication [6], [7], and digital currency [8], among other areas [9]. With the continuous development of cryptography, various encryption methods have emerged, such as the Vigenère cipher [10], [11], [12], Caesar cipher [13], [14], [15], chaotic cipher [16], [17], [18], [19], and Hill cipher [20], [21]. Although there are many types of encryption methods, they mainly consist of five components: 1) plaintext; 2) key; 3) ciphertext; 4) encryption; and 5) decryption. As an important mathematical tool, matrix theory has been widely used in the aforementioned cryptography.

Based on the above analysis, to encrypt important medical image information and ensure that only authorized medical personnel can access sensitive patient information, this article focuses on the study and improvement of the Hill cipher. The conventional Hill cipher (CHC) algorithm was proposed by American mathematician Lester S. Hill in 1929, and it belongs to the symmetric key cryptosystem, where the same key is used for both encryption and decryption. The Hill cipher mainly includes three parts: 1) plaintext; 2) key; and 3) ciphertext. The plaintext is the information to be encrypted; the ciphertext is the secret information obtained from the encryption system; and the key is the encryption parameter that makes the encryption more flexible and secure. The Hill cipher is a polygraphic substitution cipher that uses linear algebra principles for encryption and decryption. It is worth noting that the CHC uses static and invariant keys. For example, Chen et al. [22], Chen et al. [23], Hua et al. [24], and Yu et al. [25] used static sequence ciphers generated by keys to encrypt plaintext. However, due to its time-invariant nature, if an attacker obtains multiple sets of ciphertext and plaintext pairs, they may reconstruct the key matrix through linear algebra techniques, thereby compromising the entire encryption system and affecting the security of the CHC.

Received 10 December 2024; accepted 29 December 2024. Date of publication 3 January 2025; date of current version 9 May 2025. This work was supported in part by the National Natural Science Foundation of China under Grant 62273141, Grant 62372495, and Grant 62062071. *(Corresponding author: Aijia Ouyang.)*

Jie Jin is with the Sanya Institute of Hunan University of Science and Technology, Sanya 572024, Hainan, China, and also with the College of Computer Science and Engineering, Jishou University, Jishou 416000, China (e-mail: jj67123@hnust.edu.cn).

Mengfan Wu and Chaoyang Chen are with the Sanya Institute of Hunan University of Science and Technology, Sanya 572024, Hainan, China (e-mail: 23020402018@mail.hnust.edu.cn; cychen@hnust.edu.cn).

Aijia Ouyang is with the School of Information Engineering, Changsha Medical University, Changsha 410219, Hunan, China, and also with the School of Information Engineering, Zunyi Normal University, Zunyi 563002, Guizhou, China (e-mail: oyaj@foxmail.com).

Keqin Li is with the Department of Mathematics and Computer Science, State University of New York, New Paltz, NY 12561 USA (e-mail: lik@newpaltz.edu).

Digital Object Identifier 10.1109/JIOT.2025.3525623

Chaos theory, originating from the "butterfly effect" has developed into a typical field of nonlinear science. Essentially, chaos is a quasi-random and irregular motion generated by deterministic nonlinear systems. Its fundamental characteristic is extreme sensitivity to initial conditions and small parameter changes, leading to long-term unpredictability of trajectories. In recent years, with the maturation of chaos theory, its application research has received widespread attention. Fields, such as chaotic synchronization control [26], [27], [28], [29], chaotic cryptography [30], [31], [32], and chaotic neural networks [33], [34], [35], have become current research frontiers.

It should be noted that the aforementioned CHC typically involves modifying the pixel values of the encrypted images to some specific values, the image pixel positions are not changed, and the security of the CHC is limited. Therefore, to further enhance the security of CHC for image transmission, a novel dynamic Hill cipher (NDHC) not only scrambles the image pixel positions with Logistic chaotic system [36], [37], [38] but also makes the pixel values of the encrypted images change over time t is proposed. The NDHC image encryption not only replaces the static matrix key of the CHC with a time-varying dynamic key matrix (TVDKM) but also inherits the advantages of the CHC, which significantly increases the difficulty of decryption and enhances the ciphertext security. Moreover, as the TVDKM of the proposed NDHC changes over time t, which also causes the NDHC encrypted image ciphertext to change over time t as well.

However, introducing the TVDKM in the NDHC increases the security of the CHC, but it also presents challenges for the NDHC decryption. In the NDHC encryption, the TVDKM is multiplied with the original image pixel matrix to modify its pixel values, but the dynamic inversion key matrix (DIKM) of the TVDKM should be multiplied in the NDHC decryption to recover its original pixel values, and how to effectively obtain the DIKM of the TVDKM becomes an urgent issue in the NDHC decryption.

As an effective method to deal with dynamic problems, ZNN model is popularly applied in scientific and industrial fields. Unlike the traditional gradient-based neural networks, the ZNN takes full consideration of the time-varying coefficient speed compensation, and it has been successfully applied in dynamic matrix inversion [39], [40], [41], dynamic quadratic minimization [42], [43], time-varying linear equation solving [44], robots control [45], [46], and chaotic synchronization [47]. Additionally, considering the inevitability of noise during information transmission, it is necessary to have devices with anti-interference capabilities during decryption to eliminate the impact of noise in ciphertext transmission for security, and there are a lot of ZNN models with anti-noise ability have been reported in recent years. Therefore, this work chooses the ZNN to deal with the above mentioned dynamic problem, and a fixed-time convergence fuzzy zeroing neural network (FTCF-ZNN) model with superior convergence and robustness is constructed to solve the above DIKM of the TVDKM for the NDHC decryption.

TABLE I
SUMMARY OF THE ABBREVIATIONS AND SYMBOLS

ZNN	Zeroing neural network
CHC	Conventional Hill cipher
NDHC	Novel dynamic Hill cipher
TVDKM	Time-varying dynamic key matrix
DIKM	Dynamic inversion key matrix
FTCF-ZNN	Fixed-time convergence fuzzy ZNN
$\Diamond$	The fuzzy operation
$\vee$	The maximum value operation
$\wedge$	The minimum value operation
$\cup$	Union of Fuzzy Rules

This article consists of six sections. Section I introduces the main work of this article and its development history. Section II details the basic principles and methods of the Hill cipher system and chaotic permutation algorithm. Section III demonstrates the construction process of the original ZNN model and the constructed FTCF-ZNN for solving the DIKM of the TVDKM for the NDHC decryption. Section IV rigorously proves the superior performance of the constructed FTCF-ZNN model for solving the DIKM. Section V presents comparative simulation experiments of the FTCF-ZNN model with other recently reported models for solving the DIKM of the TVDKM for the NDHC decryption, and the experiments of the proposed NDHC for medical images encryption and decryption. Section VI summarizes the work of this article and envisions future development areas. The abbreviations appearing in this work are counted in Table I, and the main work includes the following.

1) Replacing the static key matrix of the CHC with a TVDKM, an NDHC for medical images encryption is proposed. Additionally, the proposed NDHC not only scrambles the image pixel positions with Logistic chaotic system but also makes the pixel values of the encrypted images change over time t, which further enhances the security of the medical images transmission.
2) In order to quickly and effectively find DIKM of the TVDKM for the NDHC decryption at the receiver, an FTCF-ZNN model with superior convergence and robustness is constructed.
3) Theoretical analysis and comparative simulation experiments of the FTCF-ZNN model with other models validate its superior performance for solving the DIKM of the TVDKM in the NDHC decryption. Moreover, the feasibility of the proposed NDHC for medical image encryption and decryption is also validated.

II. CHC AND PROPOSED NDHC

A. CHC

The CHC was first proposed by Richard Hill in 1929, where he used matrix theory and mathematical methods to design a new type of cryptographic algorithm. The CHC is a classical block cipher algorithm that employs principles of linear algebra and matrix theory for image encryption. The encryption and decryption of CHC is shown in Fig. 1, and the detailed steps of the CHC are presented below.

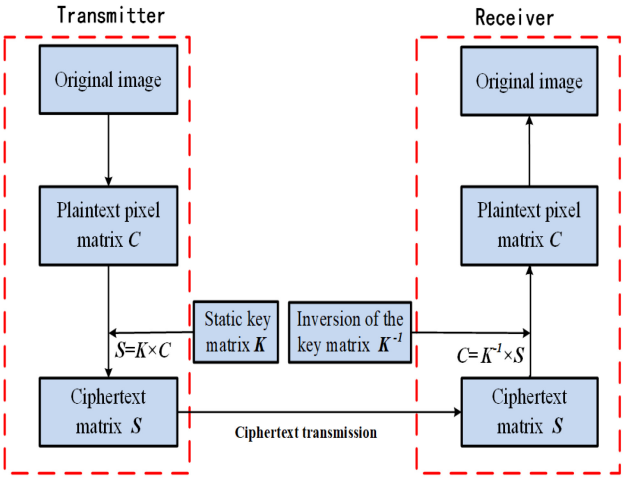

Fig. 1. Diagram of CHC.

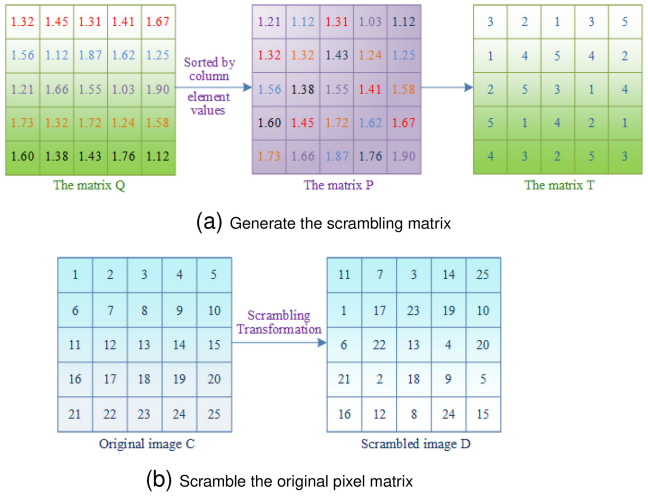

Fig. 2. Illustration of the process of image pixel positions scrambling. (a) Generate the scrambling matrix. (b) Scramble the original pixel matrix.

The encryption process of CHC is as follows.

1) *Step 1:* Transform and store the original medical image in the plaintext pixel matrix $C \in R^{n\times n}$.
2) *Step 2:* Design an n-dimensional reversible matrix $K \in R^{n\times n}$ as the key for the CHC.
3) *Step 3:* By multiplying the key matrix K with the plaintext matrix C, the ciphertext matrix $S = K * C$ is obtained.

The decryption process of CHC is as follows.

1) *Step 1:* Calculate the inversion matrix K^{-1} of the key matrix K.
2) *Step 2:* Multiply the inversion key matrix K^{-1} with the ciphertext matrix $S = K * C$ to obtain the decrypted plaintext matrix, denoted as $C = K^{-1} * S = K^{-1} * K * C$.
3) *Step 3:* Transform the plaintext matrix C to the original medical image.

The above is the detailed medical image encryption and decryption of the CHC. It should be noted that the key matrix K of the CHC is static and time-invariant, and the CHC algorithm only changed the original image pixel values to some specific values, which significantly increases the risk of ciphertext being cracked. In view of the confidentiality requirements of medical information, the CHC does not satisfy the requirements of practical applications.

Therefore, this work replaces the traditional static key matrix K of the CHC with a TVDKM $K(t)$ to achieve better confidentiality, and the elements of $K(t)$ will change their values with time t, which poses a significant challenge to illegal decryption. Moreover, the chaos-based permutation encryption algorithm is also used, and the proposed NDHC not only changes the image pixel values but also rearranges the image pixel positions. The following section will detail the encryption and decryption of the proposed NDHC with TVDKM $K(t)$.

B. Proposed NDHC

Unlike the above CHC, the proposed NDHC not only scrambles the image pixel positions with Logistic chaotic system but also modifies the image pixel values. Therefore, the Logistic chaos-based scrambling algorithm for image pixel positions scrambling is introduced in advance.

1) Logistic Chaos Scrambling Algorithm: Scrambling based on Logistic chaos is a common data encryption technique that utilizes the properties of Logistic chaos mapping to confuse and scramble data, thereby enhancing data security. Logistic chaos is a simple yet effective nonlinear dynamical system, with the iterative formula as follows:

$$x_{n+1} = r \cdot x_n \cdot (1 - x_n) \tag{1}$$

where x_n is the current state, x_{n+1} is the next state, and r is the chaos parameter, typically ranging between $[3.57, 4.0]$.

The general procedure for Logistic chaotic scrambling is as follows. First, initialize and generate a chaotic sequence using (1). Then, cut out a segment of the generated sequence that is the same size as the plaintext matrix C, and arrange it into matrix Q. Next, rearrange each column of matrix Q to obtain matrix P. Simultaneously, generate a new matrix T to record the index of the original position of each element in matrix Q. For example, the element "1.21" in matrix P is in the third position of the first column in matrix Q, so its corresponding position in matrix T is recorded as "3." The element "1.32" in matrix P is in the first position of the first column in matrix Q, so its corresponding position in matrix T is recorded as "1," and the analogy is repeated to obtain the matrix T. The schematic is presented in Fig. 2(a), and Fig. 2(b) illustrates its scrambling process, detailed as follows.

1) *Step 1:* For the first row elements $(3, 2, 1, 3, 5)$ of matrix T, select the corresponding elements $(p_{31}, p_{22}, p_{13}, p_{34}, p_{55})$ from each column of matrix C and shift them in sequence to the first row in matrix D, presenting as $(11, 7, 3, 14, 25)$.
2) *Step 2:* For the second row elements $(1, 4, 5, 4, 2)$ of matrix T, select the corresponding elements $(p_{11}, p_{42}, p_{53}, p_{44}, p_{25})$ from each column of matrix C and shift them in sequence to the second row in matrix D, presenting as $(1, 17, 23, 19, 10)$.

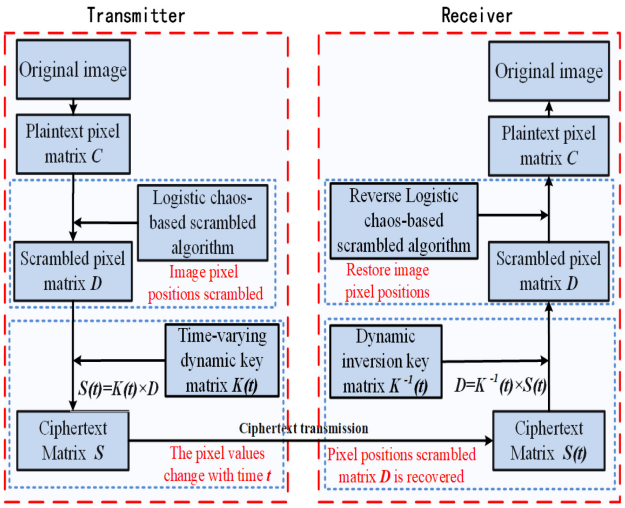

Fig. 3. Diagram of the proposed NDHC.

3) *Step 3:* For the third row elements $(2, 5, 3, 1, 4)$ of matrix T, select the corresponding elements $(p_{21}, p_{52}, p_{33}, p_{14}, p_{45})$ from each column of matrix C and shift them in sequence to the third row in matrix D, presenting as $(6, 22, 13, 4, 20)$.
4) *Step 4:* For the fourth row elements $(5, 1, 4, 2, 1)$ of matrix T, select the corresponding elements $(p_{51}, p_{12}, p_{43}, p_{24}, p_{15})$ from each column of matrix C and shift them in sequence to the fourth row in matrix D, presenting as $(21, 2, 18, 9, 5)$.
5) *Step 5:* For the fifth row elements $(4, 3, 2, 5, 3)$ of matrix T, select the corresponding elements $(p_{41}, p_{32}, p_{23}, p_{54}, p_{35})$ from each column of matrix C and shift them in sequence to the fifth row in matrix D, presenting as $(16, 12, 8, 24, 15)$.

The actual scrambling process follows a similar procedure, and the final scrambled image D is obtained.

It should be noted that Logistic chaotic system is highly sensitive to initial values and parameters. Here, we, respectively, set the initial value and parameter in (1) to $x_0 = 0.5$ and $r = 3.58$ to ensure its stability. Moreover, in order to prevent its transient response errors, we discard the data from the first 500 iterations of the chaotic system, and select a relatively stable set of data for the next encryption analysis.

The encryption and decryption of the proposed NDHC is presented in Fig. 3, and its detailed steps are presented below.

2) Encryption of NDHC: The encryption of the proposed NDHC:

1) *Step 1:* Transform and store the original medical image in the plaintext pixel matrix $C \in R^{n\times n}$.
2) *Step 2:* Use the above Logistic Chaos-based scrambling encryption algorithm to rearrange the pixel positions of the plaintext pixel matrix $C \in R^{n\times n}$, and the first scrambled pixel encrypted matrix $D \in R^{n\times n}$ is obtained.
3) *Step 3:* Design an n-dimensional reversible TVDKM $K(t) \in R^{n\times n}$ as the key for the proposed NDHC.
4) *Step 4:* By multiplying the TVDKM $K(t) \in R^{n\times n}$ with the first scrambled pixel encrypted matrix $D \in R^{n\times n}$, and the second encrypted pixel matrix $S(t) = K(t) * D$ with both pixel position arranged and pixel values changed with time t is obtained.

Unlike the CHC encryption, the TVDKM $K(t)$ is dynamic, and the second ciphertext matrix $S(t) = K(t) * D$ is also dynamic and changes with time t, which greatly enhances its security for medical image transmission.

3) Decryption of NDHC: The decryption of the proposed NDHC:

1) *Step 1:* Calculate the DIKM of the TVDKM, denoted as $K^{-1}(t) \in R^{n\times n}$.
2) *Step 2:* Multiply the DIKM $K^{-1}(t)$ with the second ciphertext matrix $S(t) = K(t) \times D$ to obtain the first decrypted plaintext matrix D, which is $D = K^{-1}(t) * S(t)$.
3) *Step 3:* Perform the inverse Logistic Chaos-based scrambling algorithm on the above obtained first scrambled ciphertext matrices D, and the image pixel plaintext matrix C is recovered.
4) *Step 4:* Transform the plaintext matrix C to the original medical image.

The above describes the entire process of NDHC encryption/decryption. It is evident that the NDHC structure is similar to the CHC. The difference lies in using a more secure dynamic key instead of a static key, resulting in element values in the pixel ciphertext matrix that continuously change with time t. In addition, a chaotic algorithm is used to change the pixel positions of the plaintext matrix. The two encryption methods in the proposed NDHC are independent, causing no complications for its decryption process.

It should be noted that the usage of the TVDKM $K(t)$ increases the security of the proposed NDHC, but how to quickly and effectively find DIKM $K^{-1}(t)$ of the TVDKM $K(t)$ becomes an urgent issue in the NDHC decryption.

Due to its effectiveness for time-varying problems solving, the ZNN method is adopted in this work for effectively finding the DIKM $K^{-1}(t)$. To further enhance its convergence and robustness for the above DIKM $K^{-1}(t)$ solving, an FTCF-ZNN model is constructed in the next section.

III. Traditional ZNN Model and Constructed FTCF-ZNN Model

This section first introduces the construction process of traditional ZNN model, then the FTCF-ZNN model with superior convergence and robustness for the above DIKM $K^{-1}(t)$ solving is constructed.

A. Traditional ZNN Model

The above DIKM of the TVDKM for the NDHC decryption can be depicted in

$$A(t)K(t) = I \in R^{n\times n} \tag{2}$$

where $K(t)$ is the known TVDKM for the NDCH encryption, I is the identity matrix, and $A(t)$ is the unknown DIKM for the NDCH decryption to be solved, denoted as $A(t) = K^{-1}(t)$.

Next, we will detail the construction process of the ZNN model for solving the above DIKM $A(t) = K^{-1}(t)$.

Define the following dynamic error function monitoring the process of DIKM solving:

$$E(t) = A(t)K(t) - I. \tag{3}$$

Obviously, when the error function $E(t)$ converges to 0, we can easily obtain the solution $A(t) = K^{-1}(t)$, and the ijth element of $E(t)$ is denoted as $e_{ij}(t)$.

Here, we use the following evolutionary formula for the convergence of $E(t)$:

$$\dot{E(t)} = -r\beta(E(t)) \tag{4}$$

where $r > 0$ is an adjustable convergence factor, $\beta(\cdot)$ is the activation function array, and $\dot{E(t)}$ is the derivative of the error function $E(t)$.

Finally, by substituting (3) into (4), the traditional ZNN model can be obtained as

$$A(t)\dot{K}(t) = -\dot{A}(t)K(t) - r\beta(E(t)) \tag{5}$$

where $\dot{A}(t)$ and $\dot{K}(t)$ are the time derivatives of $A(t)$ and $K(t)$, respectively.

Typically, information is inevitably subject to noise interference during its transmission process. Therefore, in order to expand the applicability and satisfy the practical requirements of the model, having a certain noise resistance capability is essential for the model. Hence, the ZNN model with noise can be presented as follows:

$$A(t)\dot{K(t)} = -\dot{A(t)}K(t) - r\beta(E(t)) + N(t) \tag{6}$$

where $N(t)$ represents the additive noise.

It should be noted that the choice of activation function $\beta(\cdot)$ significantly impacts model performance. Table II introduces several common forms of activation functions and their corresponding models, and the recently reported models presented in Table II will be used for the purpose of comparison with our newly constructed FTCF-ZNN model for solving the DIKM of the TVDKM for the NDHC decryption.

B. Constructed FTCF-ZNN Model

As the choice of activation function $\beta(\cdot)$ significantly impacts model performance, we will introduce the fuzzy-logic system (FLS) theory to design a fuzzy activation function, then, we will construct a new FTCF-ZNN model with superior convergence and robustness for solving the DIKM of the TVDKM for the NDHC decryption.

Here, the process to generate the fuzzy parameter $v > 1$ is introduced in advance.

1) Fuzzy-Logic System: Given that fuzzy-logic theory performs excellently in handling uncertainty issues, enhancing system flexibility, and adaptability, it is commonly used in the control of nonlinear systems. However, noise is inevitable and unpredictable in the transmission of image information, which increases the model's uncertainty. Therefore, introducing the fuzzy-logic theory in the newly constructed FTCF-ZNN model helps reduce the complexity of system modeling and design, address time-varying issues in noisy environments.

Mamdani fuzzy reasoning is one of the most common fuzzy reasoning methods, with its primary form being IF-THEN, and the Mamdani rule is adopted in this work. The Mamdani rule involves three main steps: 1) fuzzification; 2) selection of fuzzy rules and fuzzy mechanism reasoning; 3) defuzzification; and 4) its specific structure is shown in Fig. 4. In Fig. 4,

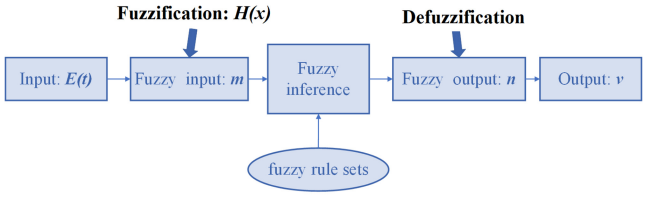

Fig. 4. Structure of FLS.

$E(t)$ serves as the input to the FLS, and it may be affected by noise during transmission. m and n act as the fuzzy input and fuzzy output, respectively. Finally, the fuzzy parameter v is obtained. The specific process of the FLS is presented as follows.

1) *Fuzzification:* First, identify the input $E(t)$ in the problem. Then, convert it into fuzzy input m and select an appropriate membership function to describe the variable membership degree. For a given precise input, calculate its membership degree in each fuzzy set using the membership function. In this article, the Gaussian membership function (GMF) is used to obtain the fuzzy output n

$$H(x) = \exp\left[-\frac{(x-d)^2}{2\delta^2}\right]. \tag{7}$$

2) *Selection of Fuzzy Rules and Fuzzy Mechanism Reasoning:* The main purpose is to establish a connection between the fuzzy input $E(t)$ and the fuzzy output n by selecting appropriate fuzzy rules. This work adopts the Mamdani rule, which is one of the most common fuzzy reasoning methods. The Mamdani fuzzy inference rule has a rule form of IF-THEN, defined as follows:

$$\begin{aligned}
&\text{Rule1}: \text{if } E(t) = ZO \text{ then } n = ZO\\
&\text{Rule2}: \text{if } E(t) = PS \text{ then } n = PS\\
&\text{Rule3}: \text{if } E(t) = PM \text{ then } n = PM\\
&\text{Rule4}: \text{if } E(t) = PB \text{ then } n = PB
\end{aligned} \tag{8}$$

where ZO, PS, PM, and PB represent error values of zero, small error, medium error, and large error, respectively. Additionally, let $\text{Rule}K = \text{Rule1} \cup \text{Rule2} \cup \text{Rule3} \cup \text{Rule4}$, where $k = 1, 2, 3, 4$. From this, we can derive the formula $n = E(t) \diamond \text{Rule}K$, where $\diamond$ represents a fuzzy operation.

3) *Defuzzification:* By defuzzifying the obtained parameter n, the fuzzy parameters v can be obtained. The specific defuzzification method is as follows:

$$v = \text{argmax}\text{M}_{E(t)} \diamond \text{Rule}k(n) \tag{9}$$

where $M_{E(t)\diamond\text{Rule}}(n) = M_{E(t)\diamond\text{Rule1}} \vee M_{E(t)\diamond\text{Rule2}} \vee M_{E(t)\vee\text{Rule3}} \vee M_{E(t)\diamond\text{Rule4}}$, $M_{E(t)\diamond\text{Rule}_k} = \sup(M_{E(t)^k} \wedge M_{n^k})$, $K = 1, 2, 3, 4$, $\vee$ and $\wedge$ stand for the maximum and minimum value operations.

Based on the fuzzy parameter v generated by the above FLS, the following fuzzy activation function FTCF-AF is designed:

TABLE II
RECENTLY REPORTED MODELS AND ACTIVATION FUNCTIONS

NO.	Model names	Formula of AFs
1	LAF-ZNN	$\beta(x) = x$
2	SBPAF-ZNN	$\beta(x) = \frac{(\lvert x\rvert^p + \lvert x\rvert^{\frac{1}{p}})sgn(x)}{2}, \quad 0 < p < 1$
3	NLAF-ZNN	$\beta(x) = \omega_1 \exp(\lvert x\rvert^c)\lvert x\rvert^{1-c} sgn(x)/c + \omega_2 s + \omega_3 sgn(x), \quad 0 < c < 1, \quad 0 < \omega_1, \quad 0 \le \omega_2, \quad 0 \le \omega_3$

$$\beta(x) = \left(a_1|x|^v + a_2|x|^{v+1} + a_3|x| - a_4\right)\mathrm{sgn}(x). \tag{10}$$

Here, v is the fuzzy parameter obtained from the aforementioned FLS.

By replacing the activation function $\beta(\cdot)$ in the traditional ZNN model (6), the newly constructed FTCF-ZNN model with noise matrix $N(t)$ for solving the DIKM of the TVDKM for the NDHC decryption is presented as follows:

$$\begin{aligned} A(t)\dot{K}(t) = &-\dot{A}(t)K(t) \\ &- r\left(a_1|E(t)|^v + a_2|E(t)|^{v+1} + a_3|E(t)| - a_4\right) \\ &+ N(t) \end{aligned} \tag{11}$$

where $N(t)$ is the noise matrix, its ijth element is denoted as $n_{ij}(t)$.

IV. THEORETICAL DISCUSSION ON THE FTCF-ZNN MODEL

In this section, the convergence and robustness of the constructed FTCF-ZNN model for solving the DIKM of the TVDKM will be discussed, and Lemma 1 is provided in advance.

Lemma 1 [48]: If there exists a function that is completely continuous, unbounded, and positive-definite function K: $R^n \longrightarrow R_+ \cup \{0\}$, such that:

1) $K(m) = 0 \Longleftrightarrow m = 0$;
2) any solution $m(t)$ satisfying the following formula:

$$\dot{K}(m(t)) \le -aK^{\varphi}(m(t)) - bK^{\psi}(m(t)) + c \tag{12}$$

for $a > 0, b > 0, 0 < \varphi < \psi, a > c$, then the system (12) is fixed-time stable.

Then, the following estimate holds: $K(t) \equiv 0, t \le T(m_0)$, with the setting time bounded to

$$\begin{aligned} T(m(0)) \le T_{\max} = &\frac{1}{a(1-\varphi)} \\ &+ \frac{2^{\psi-1}}{b^{\frac{1}{\phi}}(\psi-1)}\left(b^{\frac{1}{\phi}} + (a-c)^{\frac{1}{\phi}}\right)^{1-\psi} \end{aligned} \tag{13}$$

in which $T(m_0) = T(m(0))$.

A. Convergence Analysis of the FTCF-ZNN Model

Theorem 1: Assuming the existence of a solution to the DIKM in (2), and the noise in the FTCF-ZNN model (10) satisfies $N(t) = 0$, the FTCF-ZNN model (11) can accurately and rapidly converge to the DIKM $A(t) = K^{-1}(t)$ for the NDCH decryption in a fixed time $T(m)$. The upper bound expression of $T(m)$ is given by

$$\begin{aligned} T(m) \le T_{\max} = &\frac{1}{ra_1(1-v)} \\ &+ \frac{2^{n+2}}{v \times (ra_2)^{\frac{2}{2+v}}}\left((2ra_2)^{\frac{v}{2}} + (2ra_1 - \delta)^{\frac{v}{2}}\right)^{-\frac{v}{2}} \end{aligned} \tag{14}$$

where $a_1 > a_4 > 0, a_2 > 0, a_3 > 0, 0 < v < 1$.

Proof: First, if $E(t)$ in evolution (4) converges to 0 in fixed time, it follows that the proposed FTCF-ZNN model (11) also converges to the DIKM $A(t) = K^{-1}(t)$ in fixed time. Considering that evolution (4) is composed of n subsystems, we arbitrarily select one subsystem of the evolution (4) to validate its convergence, as outlined below

$$e_{ij}(t) = -r\beta\left(e_{ij}(t)\right) \tag{15}$$

where $i, j \in \{1, 2, \ldots, n\}$. ■

Next, we select the Lyapunov function $U_{(t)} = |e_{ij}(t)|^2$ to verify the stability of the ij subsystem of evolution (4). The specific proof process is as follows:

$$\begin{aligned} \dot{U}(t) &= 2\left|e_{ij}(t)\right| \cdot \left|\dot{e_{ij}}(t)\right| \\ &= 2\left|e_{ij}(t)\right| \cdot \left(-r\left(\left(a_1\left|e_{ij}(t)\right|^n + a_2\left|e_{ij}(t)\right|^{n+1}\right)\right)\mathrm{sgn}\left(\left|e_{ij}(t)\right|\right) \\ &\quad + 2\left|e_{ij}(t)\right| \cdot \left(-r\left(\left(a_3\left|e_{ij}(t)\right| - a_4\right)\right)\right)\mathrm{sgn}\left(\left|e_{ij}(t)\right|\right) \\ &= -2r \cdot a_1\left|e_{ij}(t)\right|^{n+1} - 2r \cdot a_2\left|e_{ij}(t)\right|^{n+2} \\ &\quad - 2r \cdot a_3\left|e_{ij}(t)\right|^2 + 2r \cdot a_4\left|e_{ij}(t)\right|. \end{aligned} \tag{16}$$

Let $F(x) = -2g \cdot a_3x^2 + 2g \cdot a_4x$, where $x = |e_{ij}(t)| > 0$, it is clear that $F(x)$ has a maximum value, taking the derivative of $F(x)$ and we obtain

$$\dot{F}(x) = -4r \cdot a_3x + 2r \cdot a_4. \tag{17}$$

When $x = (a_4/2a_3)$, $F(x)$ attains its maximum value δ

$$F(x)_{\max} = \delta = \frac{ra_4^2}{2a_3}. \tag{18}$$

Then

$$\dot{U}(t) \le -2r \cdot a_1\left|e_{ij}(t)\right|^{n+1} - 2r \cdot a_2\left|e_{ij}(t)\right|^{n+2} + \delta. \tag{19}$$

Since the Lyapunov function $U(t) = |e_{ij}(t)|^2$, (19) can be simplified as

$$\dot{U}(t) \le -2r \cdot a_1\left|U_{(t)}\right|^{\frac{n+1}{2}} - 2r \cdot a_2\left|U_{(t)}\right|^{\frac{n+2}{2}} + \delta. \tag{20}$$

Finally, according to Lemma 1, it is easy to deduce that the convergence time $T(m)$ of the ijth subsystem of the evolution equation (4) and the upper bound of the fixed convergence time $T_{\max}$ of the FTCF-ZNN model (11) to converge to the DIKM $A(t) = K^{-1}(t)$ satisfy

$$\begin{aligned} T(m) \le T_{\max} = &\frac{1}{ra_1(1-v)} + \frac{2^{n+2}}{v \times (ra_2)^{\frac{2}{2+v}}} \\ &\left((2ra_2)^{\frac{v}{2}} + (2ra_1 - \delta)^{\frac{v}{2}}\right)^{-\frac{v}{2}}. \end{aligned}$$

The proof of Theorem 1 is completed. ■

B. Robustness Analysis of the FTCF-ZNN Model

To address the inevitable noise interference in practical applications, this section discusses the robustness of the constructed FTCF-ZNN model (11).

Theorem 2: When the TVDKM $K(t)$ in (2) is reversible, and the absolute value of the ijth element of the noise matrix $N(t)$ in (11) satisfies $|n_{ij}(t)| \leq \lambda|e_{ij}(t)|$, $ra_3 > \lambda$, the FTCF-ZNN model (11) can rapidly and accurately obtain the inversion matrix of the dynamic time-varying key $D(t)$ within a fixed time $T_{(m)}$. Furthermore, the expression for the upper bound of the fixed convergence time $T_{(m)}$ is as follows:

$$T(m) \leq T_{\max} = \frac{1}{ra_1(1-v)} + \frac{2^{n+2}}{v \times (ra_2)^{\frac{2}{2+v}}} \left((2ra_2)^{\frac{v}{2}} + (2ra_1 - \mu)^{\frac{v}{2}}\right)^{-\frac{v}{2}}.$$

Similarly, selecting the Lyapunov function $U(t) = |e_{ij}(t)|^2$ to verify the stability of the ij subsystems in evolution equation (4). At this moment, $e_{ij}(t) = -r\beta(e_{ij}(t)) + n_{ij}(t)$, the specific proof process is as follows:

$$\begin{aligned}\dot{U}(t) &= 2\left|e_{ij}(t)\right| \cdot \left|\dot{e_{ij}}(t)\right| \\ &= 2|e_{ij}(t)| \cdot \Big(-ra_1|e_{ij}(t)|^n + a_2|e_{ij}(t)|^{n+1} \\ &\quad + a_3|e_{ij}(t)| - a_4\,\mathrm{sgn}(|e_{ij}(t)|) + n_{ij}(t)\Big) \end{aligned} \tag{21}$$

since $|n_{ij}(t)| \leq \lambda|E_{ij}(t)|$, thus, we obtain

$$\begin{aligned}\dot{U}_{(t)} &= -2r \cdot a_1|e_{ij}(t)|^{n+1} - 2r \cdot a_2|e_{ij}(t)|^{n+2} \\ &\quad + 2(\lambda - r \cdot a_3)|e_{ij}(t)|^2 + 2r \cdot a_4|e_{ij}(t)|. \end{aligned} \tag{22}$$

Let $G(x) = 2(\lambda - r \cdot a_3)x^2 + 2r \cdot a_4 x$, because of $ra_3 > \lambda$, $G(x)$ has a maximum value, which can be determined by taking its derivative. When $x = (ra_4/2(\lambda - r \cdot a_3))$, $G(x)_{\max}$ achieves its maximum value μ

$$G(x)_{\max} = \mu = \frac{3r^2a_4^2}{2(\lambda - r \cdot a_3)}. \tag{23}$$

Then

$$\dot{U}(t) \leq -2r \cdot a_1|e_{ij}(t)|^{n+1} - 2r \cdot a_2|e_{ij}(t)|^{n+2} + \mu. \tag{24}$$

Since the Lyapunov function $U(t) = |e_{ij}(t)|^2$, (24) can be simplified as

$$\dot{U}(t) \leq -2r \cdot a_1\left|U_{(t)}\right|^{\frac{n+1}{2}} - 2r \cdot a_2\left|U_{(t)}\right|^{\frac{n+2}{2}} + \mu. \tag{25}$$

Finally, according to Lemma 1, the convergence time $T(m)$ of the ijth subsystem of the evolution equation (4) and the upper bound of the fixed convergence time $T_{\max}$ of the FTCF-ZNN model (11) with noise to converge to the DIKM $A(t) = K^{-1}(t)$ satisfy

$$T(m) \leq T_{\max} = \frac{1}{ra_1(1-v)} + \frac{2^{n+2}}{v \times (ra_2)^{\frac{2}{2+v}}} \left((2ra_2)^{\frac{v}{2}} + (2ra_1 - \mu)^{\frac{v}{2}}\right)^{-\frac{v}{2}}.$$

The proof of Theorem 2 is completed.

Theorem 1 ensures the convergence of the constructed FTCF-ZNN model, while Theorem 2 guarantees the robustness of the constructed FTCF-ZNN model for solving the DIKM of the TVDKM.

V. Comparative Experiments

In order to validate the advantages of the constructed FTCF-ZNN model for solving the DIKM of the TVDKM for the NDHC decryption at the receiver, comparative simulation results of the constructed FTCF-ZNN model with other recently reported models in Table II for solving the DIKM of the TVDKM for the NDHC decryption at the receiver is presented. Moreover, the proposed NDHC is also applied to encrypt and decrypt the grayscale and RGB medical images to validate its effectiveness in medical images encryption.

A. Comparative Simulation Experiments of the FTCF-ZNN Model With Other Models for Solving the DIKM of the TVDKM for the NDHC Decryption

As mentioned above, replacing the static key matrix K of the CHC with a TVDKM $K(t)$ enhances the proposed NDHC for information transmission security. However, its time-varying nature poses challenges for the receiver to effectively obtain the DIKM $K^{-1}(t)$ of the TVDKM $K(t)$ to decrypt the ciphertext.

In order to effectively address the issue of obtaining the DIKM $K^{-1}(t)$ of the TVDKM for the proposed NDHC decryption, the FTCF-ZNN model is constructed. The following discussion will focus on the simulation results of the constructed FTCF-ZNN model and other recently reported models for solving the DIKM of the TVDKM in various environments.

Here, the TVDKM $K(t)$ in (2) is randomly chosen in (26), and the constructed FTCF-ZNN model and other recently reported models in Table II are all used for solving the DIKM $A(t) = K^{-1}(t)$ with the matrix coefficient TVDKM $K(t)$ in (26) for the purpose of comparison

$$K(t) = \begin{bmatrix} 1 + 2\cos 2t & -3\sin t \\ 2\sin 2t & 1 + 2\cos 2t \end{bmatrix}. \tag{26}$$

In the ideal noise-free environment, the simulation results of the FTCF-ZNN model and other models for solving the DIKM $K^{-1}(t)$ of the TVDKM are shown in Fig. 5.

Based on Fig. 5(a), it can be observed that the neural state solutions of all models converge to the theoretical solution (red dashed curves) of the DIKM $K^{-1}(t)$, indicating that all models are capable of obtaining the solution for (2). The FTCF-ZNN model, however, exhibits the shortest convergence time, approximately around 0.2 s, while the remaining models converge with the state solution at around 1.2 s. In order to observe the performances of all the models clearly, the residual errors $\|A(t)K(t) - I\|$ of all models are displayed in Fig. 5(b). It is evident that the curve representing the FTCF-ZNN model (red solid line) converges to 0 in the shortest time, which indicates that the constructed FTCF-ZNN model has superior performance in solving the DIKM of the TVDKM for the NDHC decryption in noise-free situation.

It is worth noting that noises are inevitable, which raises the question of whether the constructed FTCF-ZNN model also exhibits excellent convergence and robustness in noisy environments. The subsequent simulation experiments will verify the noise suppression capability of the FTCF-ZNN model.

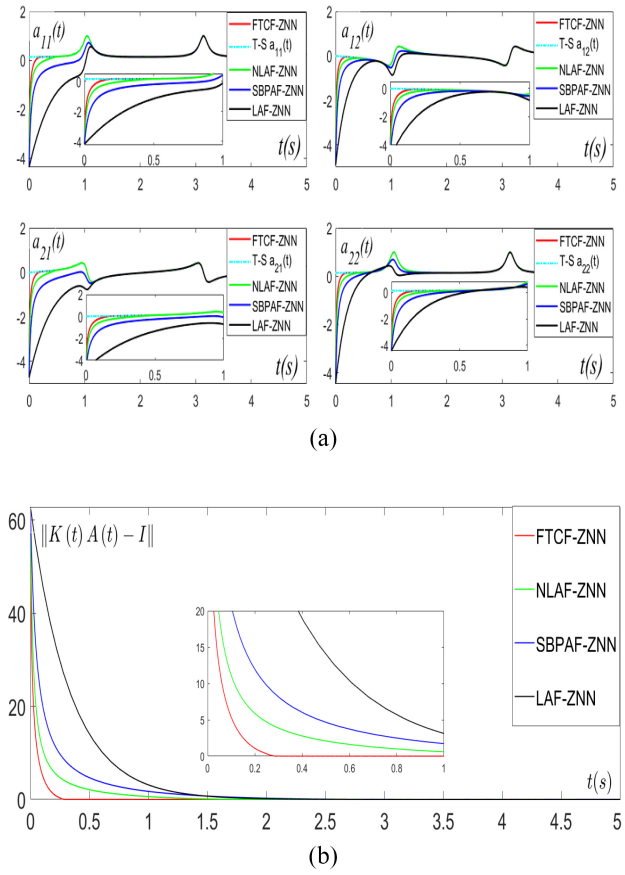

Fig. 5. Constructed FTCF-ZNN and other models for solving DIKM $A(t) = K^{-1}(t)$ without noise. (a) Neural state solutions of the models [T-S are the theoretical solutions of $A(t)$]. (b) Residual errors $\|A(t)K(t)-I\|$ of the models.

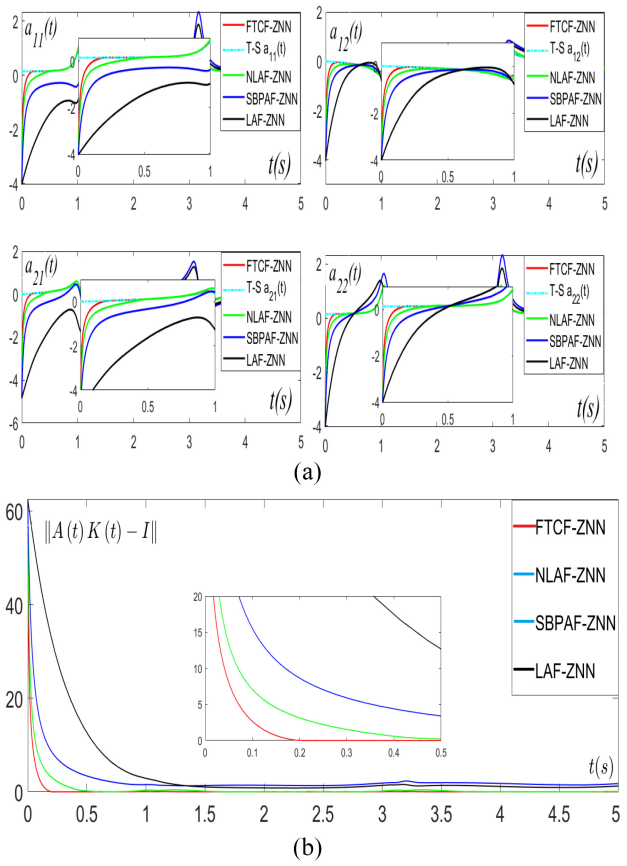

Fig. 6. Constructed FTCF-ZNN and other models for solving DIKM $A(t) = K^{-1}(t)$ with noise $N(t) = 2\sin 3t + 0.3e(-0.2t) + 3t$. (a) Neural state solutions of the models [T-S are the theoretical solutions of $A(t)$]. (b) Residual errors $\|A(t)K(t) - I\|$ of the models.

Fig. 6 is the neural state solutions and residual errors $\|A(t)K(t) - I\|$ of the FTCF-ZNN model and other models for solving the DIKM $A(t) = K^{-1}(t)$ of the TVDKM for the NDHC decryption under combination noise $N(t) = 2\sin 3t + 0.3e(-0.2t) + 3t$.

Based on Fig. 6(a), it is evident that under the interference of combination noise $N(t)$, the state solutions generated by other models (black, green, and blue solid curves) do not align well with the theoretical solution of the DIKM $A(t)$ (red dotted curves), only the neural state solutions (red solid line) generated by the constructed FTCF-ZNN model in this article exhibits a excellent alignment with the theoretical solution (red dotted curves).

In order to observe the performances of all the models clearly, the residual errors $\|A(t)K(t) - I\|$ of all models for solving the DIKM $A(t)$ of the TVDKM under the above combination noise is displayed in Fig. 6(b). It is apparent that other models struggle to reduce their residual errors $\|A(t)K(t) - I\|$ to zero, and they exhibit significant errors, whereas the constructed NLS-ZNN can still converge to zero. Consequently, it can be argued that the proposed FTCF-ZNN model demonstrates excellent robustness and convergence.

Based on the aforementioned experiments, we can conclude that the constructed FTCF-ZNN model (11) in this article possesses efficient and accurate capabilities in solving the DIKM $A(t)$ of the TVDKM for the NDHC decryption, and it fully satisfies the practical requirements.

B. Experimental Application of the Proposed NDHC in Medical Images Encryption and Decryption

In medical imaging, the X-ray images are usually used for diagnosing fractures and lung diseases, the CT images, MRI, ultrasound images, and PET scans are used for diagnosing brain and other diseases. The medical Images encountered in daily life are typically categorized as grayscale images and RGB color images, and the two kinds of medical images will be used for the validation of the proposed NDHC algorithm.

Grayscale images contain only black and white, and they are commonly used to represent the brightness and grayscale levels of objects without considering color information. Each pixel value represents the brightness at that point, with 0 typically representing black and 255 representing white. Color images, on the other hand, are based on grayscale images but are transformed into three dimensions. For example, an RGB color image of 528 × 528 can be represented as (528, 528, 3), where the first two terms represent the rows and columns of the matrix, and 3 represents three basic color channels: red (R), green (G), and blue (B). Therefore, color images are also known as RGB images, where any color can be obtained through combinations of these three primary colors.

According to Fig. 3, the NDHC encryption process for color images is as follows.

1) Extract the pixel matrices of the R, G, and B channels of the image, respectively, as the first layer (C_1), the second layer (C_2), and the third layer (C_3) plaintext matrices.
2) Scramble the plaintext matrices C_1, C_2, and C_3, and the pixel positions scrambled ciphertext matrices D_1, D_2, and D_3 are obtained.
3) Use (27) to generate three TVDKM $K_1(t)$, $K_2(t)$, and $K_3(t)$.
4) Then, multiply the above scrambled ciphertext matrices D_1, D_2, and D_3 with the TVDKM $K_1(t)$, $K_2(t)$, and $K_3(t)$ to obtain the pixel values changed ciphertext matrices $S_1(t) = K_1(t) * D_1$, $S_2(t) = K_2(t) * D_2$, $S_3(t) = K_3(t) * D_3$

$$K_1^{ij}(t) = K_2^{ij}(t) = K_3^{ij}(t) = \begin{cases} 10 \times (9 + \sin(t)), & \text{if } i = j \\ 10 \times (\cos 4t/(i-j)), & \text{if } i > j \\ 10 \times (\sin 4t/(j-i)), & \text{if } i < j. \end{cases} \quad (27)$$

The above is the proposed NDHC encryption process for the RGB color images in the transmitter.

The NDHC decryption process involves multiplying the ciphertext matrices $S_1(t), S_2(t), S_3(t)$ by the DIKMs $K_1^{-1}(t)$, $K_2^{-1}(t)$, $K_3^{-1}(t)$ of the TVDKM $K_1(t)$, $K_2(t)$, and $K_3(t)$ to obtain the scrambled ciphertext matrices $D_1 = K_1^{-1}(t) * S_1(t)$, $D_2 = K_2^{-1}(t) * S_2(t)$, and $D_3 = K_3^{-1}(t) * S_3(t)$.

It is worthy to mention that how to quickly and effectively obtain the DIKMs $K_1^{-1}(t)$, $K_2^{-1}(t)$, and $K_3^{-1}(t)$ of the TVDKM $K_1(t)$, $K_2(t)$, and $K_3(t)$ is very crucial for the proposed NDHC encryption, and the FTCF-ZNN model with superior convergence and robustness constructed in Section III-B and validated in Section IV, and Section V-A is used for the above thorny DIKM problem solving.

Similarly, the detailed NDHC decryption process for color images is as follows.

1) Multiplying the ciphertext matrices $S_1(t), S_2(t), S_3(t)$ by the DIKM $K_1^{-1}(t)$, $K_2^{-1}(t)$, $K_3^{-1}(t)$ to obtain the scrambled ciphertext matrices $D_1 = K_1^{-1}(t) * S_1(t) = K_1^{-1}(t) * K_1(t) * D_1$, $D_2 = K_2^{-1}(t) * S_2(t) = K_2^{-1}(t) * K_2(t) * D_2$ and $D_3 = K_3^{-1}(t) * S_3(t) = K_3^{-1}(t) * K_3(t) * D_3$.
2) Perform the inverse Logistic Chaos-based scrambling algorithm on the obtained scrambled ciphertext matrices D_1, D_2, and D_3 in step 2, and the plaintext matrices C_1, C_2, and C_3 are recovered.
3) Transform the plaintext matrices C_1, C_2, and C_3 into R, G, and B channels of the image, the original RGB color image is restored.

The above is the proposed NDHC decryption process for the RGB color images in the receiver. It is important to note that the decryption order must not be disrupted, or the original image cannot be correctly recovered.

This describes the encryption and decryption of the proposed NDHC for RGB color images. The NDHC encryption and decryption for grayscale images is easier than the color images, and it only need to carry out on a single channel. In simple terms, NDHC encryption and decryption operations of grayscale images are performed on a single matrix, following the same NDHC color image process as described above.

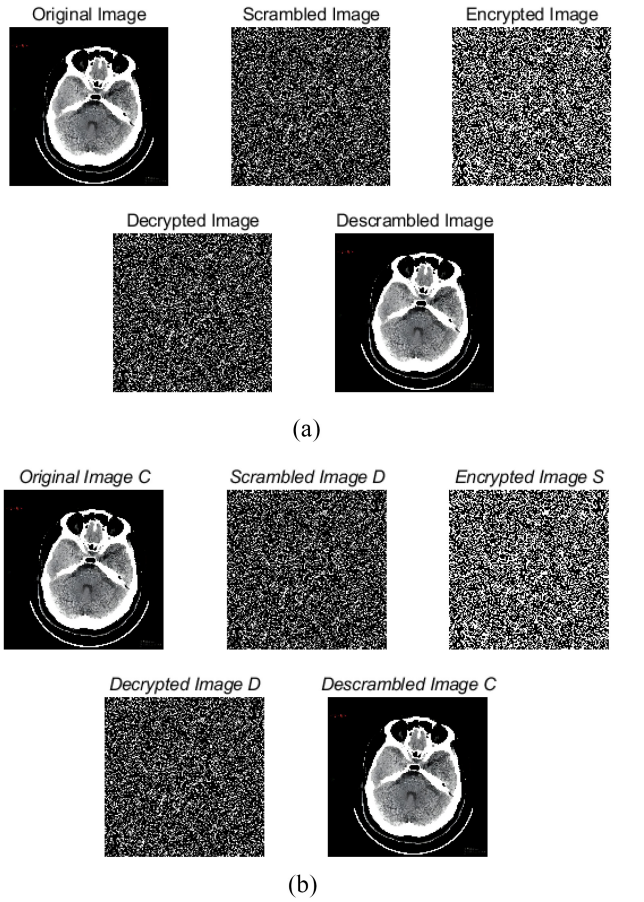

Fig. 7. NDHC encryption and decryption results of MRI grayscale image (528 × 528 × 1). (a) Key time $t = 5.3$ s. (b) Key time $t = 11.8$ s.

The MRI grayscale images in Fig. 7 and the CT color images in Fig. 8 are used to test the proposed NDHC encryption and decryption processes. The time points of the TVDKM $K_1(t)$, $K_2(t)$, and $K_3(t)$ in experiments are set to be $t = 5.3$ s and $t = 11.8$ s, respectively.

It is evident that the human eye cannot observe any connection between the ciphertext image and the original image, and the original image can be restored after decryption, which demonstrates that the proposed NDHC can effectively encrypt and decrypt both grayscale and color images. Moreover, it can be clearly observed that there is a significant difference between the encrypted ciphertext image in Fig. 8(a3) and (b3), the reason leading to this significant difference is the different time points ($t = 5.3$ s and $t = 11.8$ s) of the TVDKM $K_1(t)$, $K_2(t)$, and $K_3(t)$ used in the experiments.

In order to intuitively observe the security of the NDHC proposed in this work, the histograms analysis of the "CT" image is shown in Fig. 9. Fig. 9(a) shows the RGB histograms of the original CT image, and it can be seen that the distribution of pixel values of the original image in each channel is uneven. However, the pixel positions and values of the encrypted image in Fig. 9(b) obtained after the NDHC encryption operation are completely disrupted, and the

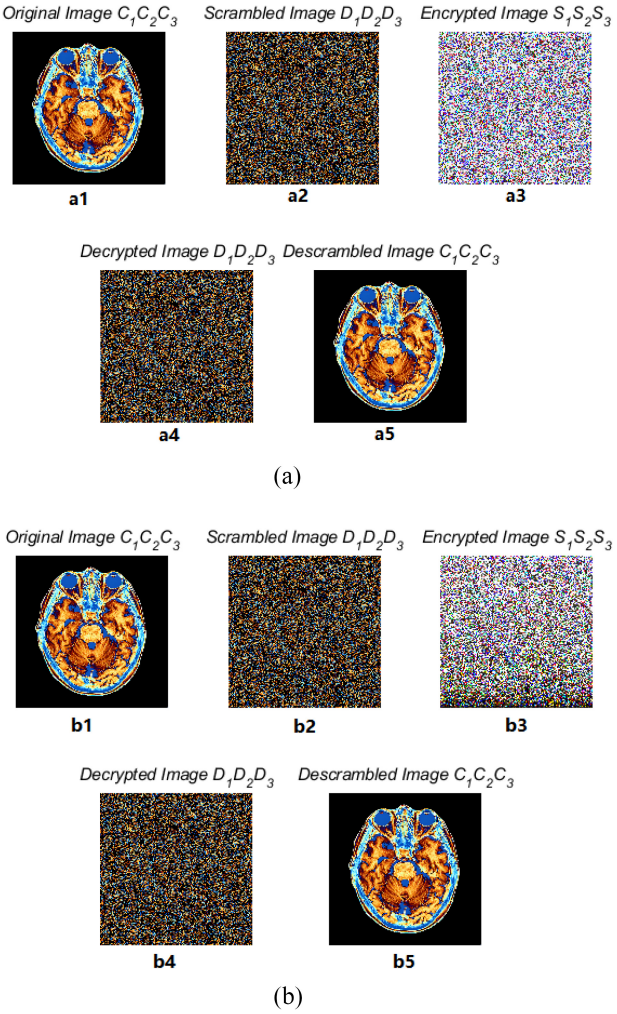

Fig. 8. NDHC encryption and decryption results of CT color image (528 × 528 × 3). (a) Key time $t = 5.3$ s. (b) Key time $t = 11.8$ s.

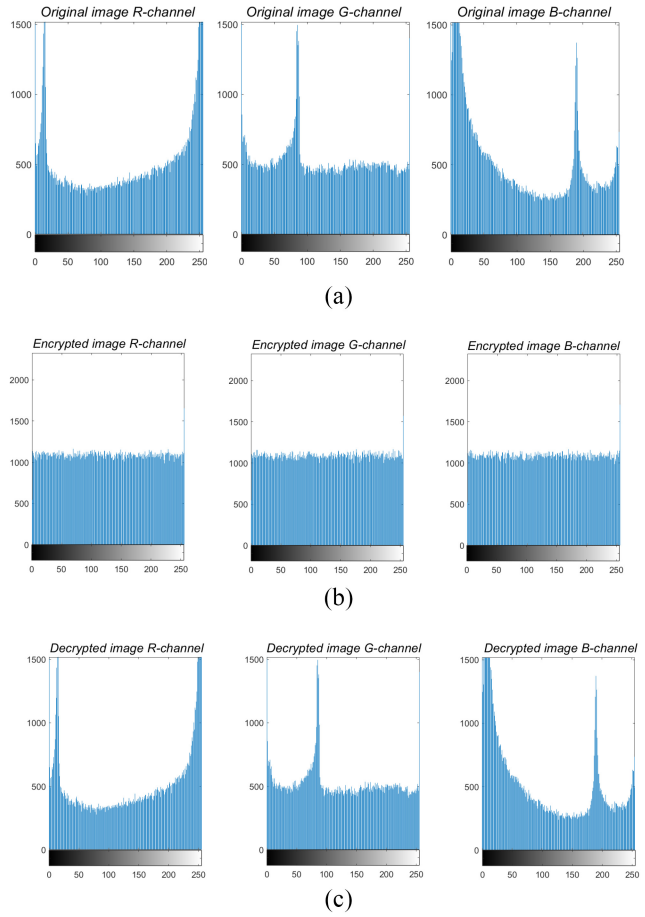

Fig. 9. At key time $t = 11.8$ s, the histograms of the CT RGB color image before and after the NDHC encryption and decryption. (a) Histograms of the original image. (b) Histograms of the NDHC encrypted image. (c) Histograms of the NDHC decrypted image.

histogram of each channel of the NDHC encrypted CT image is smooth and even, which means the image information is completely covered after the NDHC encryption. Finally, it can be observed in Fig. 9(c) that the original image can be well restored after the NDHC decryption operation, which further verifies the feasibility of the proposed NDHC method in this work.

The above experimental results indicate that the proposed NDHC encrypts and decrypts grayscale and RGB color medical images perfectly and enable the recipient to quickly and accurately obtain the desired information upon reception. In addition, the security of the NDHC encrypted images are greatly enhanced due to the adoption of the dynamic time-varying key matrix.

VI. Conclusion

Cryptography is a hot topic in the information age of the Internet. The rapid development of the Internet has led to a plethora of security issues such as information leakage. As a result, cryptography has gained favor among a wide range of researchers. This work takes the CHC as an example and proposes an NDHC not only replaces the static matrix key of the CHC with a TVDKM to change the medical image pixel values with time t but also uses the Logistic chaos sequence scrambling algorithm to rearrange the medical image pixel positions, which greatly enhances the security of medical images transmission.

In the decryption process, the main focus is on how to quickly restore the original image. It is evident that the difficulty in the proposed NDHC decryption process lies in quickly finding the DIKM of the TVDKM. This article adopts the ZNN neural network method to solve the dynamic inversion matrix of the TVDKM, constructs a new FTCF-ZNN model based on fuzzy theory to solve it. Comparisons of the FTCF-ZNN model with several existing models separately in noise-free and noisy conditions are presented to fully demonstrate its superiority. The superior performance of the constructed FTCF-ZNN model for solving the DIKM of the TVDKM are validated by both theoretical analysis and comparative simulation experiments. The consistency between theoretical proofs and experimental results validates the effectiveness of the constructed FTCF-ZNN in addressing DIKM problem. Additionally, appropriate grayscale and RGB color medical images are selected for the proposed NDHC encryption and decryption experiments, with the experimental results meeting the expected outcomes.

REFERENCES

[1] H. Jadvar, R. W. Henderson, and P. S. Conti, "[F-18] fluorodeoxyglucose positron emission tomography and positron emission tomography: Computed tomography in recurrent and metastatic cholangiocarcinoma," *J. Comput. Assist. Tomogr.*, vol. 31, no. 2, pp. 223–228, 2007.

[2] M. Subbarao, "High-sensitivity Single-Photon Emission Computed Tomography (SPECT): Safer, faster, and more accurate SPECT," in *Proc. 8th Int. Conf. Expo Emerg. Technol. Smarter World*, 2011, pp. 1–2.

[3] K. An et al., "A novel micro-multifocus X-ray source based on electron beam scanning for multi-view stationary micro computed tomography," *IEEE Electron Device Lett.*, vol. 41, no. 1, pp. 167–170, Jan. 2020.

[4] N. Li et al., "Simultaneous head and spine MR imaging in children using a dedicated multichannel receiver system at 3T," *IEEE Trans. Biomed. Eng.*, vol. 68, no. 12, pp. 3659–3670, Dec. 2021.

[5] S. A. Soleymani, S. Goudarzi, M. H. Anisi, M. Zareei, A. H. Abdullah, and N. Kama, "A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET," *Veh. Commun.*, vol. 29, Jun. 2021, Art. no. 100335.

[6] C. Cachin, S. Micali, and M. Stadler, "Computationally private information retrieval with polylogarithmic communication," in *Proc. Int. Conf. Theory Appl. Cryptogr. Techn.*, 1999, pp. 402–414.

[7] H. Xiong, H. Wang, W. Meng, and K.-H. Yeh, "Attribute-based data sharing scheme with flexible search functionality for cloud-assisted autonomous transportation system," *IEEE Trans. Ind. Informat.*, vol. 19, no. 11, pp. 10977–10986, Nov. 2023.

[8] J. Wang and T. Yang, "Subliminal channel and digital currency pay security," in *Proc. Int. Conf. Intell. Transp., Big Data Smart City (ICITBS)*, 2018, pp. 129–132.

[9] H. Xiong, J. Chen, Q. Mei, and Y. Zhao, "Conditional privacy-preserving authentication protocol with dynamic membership updating for VANETs," *IEEE Trans. Depend. Secure Comput.*, vol. 19, no. 3, pp. 2089–2104, May/Jun. 2020.

[10] G. Singh and Supriya, "Modified vigenere encryption algorithm and its hybrid implementation with Base64 and AES," in *Proc. 2nd Int. Conf. Adv. Comput., Netw. Security*, 2013, pp. 232–237.

[11] A. Bhateja and S. Kumar, "Genetic algorithm with elitism for cryptanalysis of Vigenere cipher," in *Proc. Int. Conf. Issues Challenges Intell. Comput. Techn. (ICICT)*, 2014, pp. 373–377.

[12] A. K. Bhateja, A. Bhateja, S. Chaudhury, and P. Saxena, "Cryptanalysis of Vigenere cipher using cuckoo search," *Appl. Soft Comput.*, vol. 26, pp. 315–324, Jan. 2015.

[13] S. Dey, J. Nath, and A. Nath, "An integrated symmetric key cryptographic method-amalgamation of TTJSA algorithm, advanced Caesar cipher algorithm, bit rotation and reversal method: SJA algorithm," *Int. J. Modern Educ. Comput. Sci.*, vol. 4, no. 5, p. 1, 2012.

[14] S. Dey, J. Nath, and A. Nath, "An advanced combined symmetric key cryptographic method using bit manipulation, bit reversal, modified Caesar cipher (SD-REE), DJSA method, TTJSA method: SJA-I algorithm," *Int. J. Comput. Appl.*, vol. 46, no. 20, pp. 46–53, 2012.

[15] S. Srikantaswamy and D. H. Phaneendra, "Improved Caesar cipher with random number generation technique and multistage encryption," *Int. J. Cryptogr. Inf. Secur.*, vol. 2, no. 4, pp. 39–49, 2012.

[16] M. A. Taha, S. E. Assad, A. Queudet, and O. Deforges, "Design and efficient implementation of a chaos-based stream cipher," *Int. J. Internet Technol. Secured Trans.*, vol. 7, no. 2, pp. 89–114, 2017.

[17] W. J. Sun, "Research on stream cipher model based on chaos theory," *Appl. Mech. Mater.*, vol. 539, pp. 321–325, Jun. 2014.

[18] J. Feng, J. Wang, Y. Zhu, and K. Han, "A hybrid chaotic encryption ASIC with dynamic precision for Internet of Things," *IEEE Internet Things J.*, vol. 11, no. 1, pp. 1148–1163, Jan. 2024.

[19] H. Lin, X. Deng, F. Yu, and Y. Sun, "Grid multibutterfly memristive neural network with three memristive systems: Modeling, dynamic analysis, and application in police IoT," *IEEE Internet Things J.*, vol. 11, no. 18, pp. 29878–29889, Sep. 2024.

[20] S. Mandowen et al., "Advanced Hill cipher algorithm for security image data with the involutory key matrix," *J. Phys., Conf. Ser.*, vol. 1899, no. 1, 2021, Art. no. 12116.

[21] U. Indriani, H. Gunawan, A. Y. N. Harahap, and H. Zaharani, "Chat message security enhancement on WLAN network using Hill cipher method," in *Proc. 8th Int. Conf. Cyber IT Service Manag. (CITSM)*, 2020, pp. 1–5.

[22] F. Chen, Y. Yuan, H. He, M. Tian, and H.-M. Tai, "Multi-MSB compression based reversible data hiding scheme in encrypted images," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 31, no. 3, pp. 905–916, Mar. 2021.

[23] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of image ciphers with permutation-substitution network and chaos," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 31, no. 6, pp. 2494–2508, Jun. 2021.

[24] Z. Hua, Y. Wang, S. Yi, Y. Zhou, and X. Jia, "Reversible data hiding in encrypted images using cipher-feedback secret sharing," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 8, pp. 4968–4982, Aug. 2022.

[25] M. Yu, H. Yao, C. Qin, and X. Zhang, "A comprehensive analysis method for reversible data hiding in stream-cipher-encrypted images," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 10, pp. 7241–7254, Oct. 2022.

[26] Q. Zhang and J.-a. Lu, "Chaos synchronization of a new chaotic system via nonlinear control," *Chaos, Solitons Fractals*, vol. 37, no. 1, pp. 175–179, 2008.

[27] H. Zhang, D. Liu, and Z. Wang, *Controlling Chaos: Suppression, Synchronization and Chaotification*. London, U.K.: Springer, 2009.

[28] J. Jin, W. Chen, A. Ouyang, F. Yu, and H. Liu, "A time-varying fuzzy parameter zeroing neural network for the synchronization of chaotic systems," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 8, no. 1, pp. 364–376, Feb. 2024.

[29] W. Chen, J. Jin, C. Chen, F. Yu, and C. Wang, "A disturbance suppression zeroing neural network for robust synchronization of chaotic systems and its FPGA implementation," *Int. J. Bifurcation Chaos*, vol. 32, no. 14, 2022, Art. no. 2250210.

[30] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6–21, Aug. 2002.

[31] J. Amigo, L. Kocarev, and J. Szczepanski, "Theory and practice of chaotic cryptography," *Phys. Lett. A*, vol. 366, no. 3, pp. 211–216, 2007.

[32] L. Kocarev and S. Lian, *Chaos-Based Cryptography: Theory, Algorithms and Applications*, vol. 354. Berlin, Germany: Springer, 2011.

[33] A. Potapov and M. K. Ali, "Robust chaos in neural networks," *Phys. Lett. A*, vol. 277, no. 6, pp. 310–322, 2000.

[34] D. Sussillo and L. F. Abbott, "Generating coherent patterns of activity from chaotic neural networks," *Neuron*, vol. 63, no. 4, pp. 544–557, 2009.

[35] H. N. Balakrishnan, A. Kathpalia, S. Saha, and N. Nagaraj, "ChaosNet: A chaos based artificial neural network architecture for classification," *Chaos Interdiscipl. J. Nonlin. Sci.*, vol. 29, no. 11, 2019, Art. no. 113125.

[36] X. Kong, F. Yu, W. Yao, S. Cai, J. Zhang, and H. Lin, "Memristor-induced hyperchaos, multiscroll and extreme multistability in fractional-order HNN: Image encryption and FPGA implementation," *Neural Netw.*, vol. 171, pp. 85–103, Mar. 2024.

[37] Z. Hua, Y. Zhou, C.-M. Pun, and C. P. Chen, "2D sine logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, pp. 80–94, Mar. 2015.

[38] H. Zhu, Y. Zhao, and Y. Song, "2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption," *IEEE Access*, vol. 7, pp. 14081–14098, 2019.

[39] L. Jia, L. Xiao, and J. Dai, "Application of two fuzzy logic systems to complex-type ZNN models for the Drazin inverse of time-dependent complex-value matrix," *IEEE Trans. Fuzzy Syst.*, vol. 30, no. 9, pp. 3685–3694, Sep. 2022.

[40] J. Jin, J. Zhu, L. Zhao, L. Chen, L. Chen, and J. Gong, "A robust predefined-time convergence zeroing neural network for dynamic matrix inversion," *IEEE Trans. Cybern.*, vol. 53, no. 6, pp. 3887–3900, Jun. 2023.

[41] J. Jin, J. Zhu, L. Zhao, and L. Chen, "A fixed-time convergent and noise-tolerant zeroing neural network for online solution of time-varying matrix inversion," *Appl. Soft Comput.*, vol. 130, Nov. 2022, Art. no. 109691.

[42] L. Jia, L. Xiao, J. Dai, Z. Qi, Z. Zhang, and Y. Zhang, "Design and application of an adaptive fuzzy control strategy to zeroing neural network for solving time-variant QP problem," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 6, pp. 1544–1555, Jun. 2021.

[43] L. Xiao, X. Li, W. Huang, and L. Jia, "Finite-time solution of time-varying tensor inversion by a novel dynamic-parameter zeroing neural-network," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4447–4455, Jul. 2022.

[44] L. Xiao, Y. He, Y. Wang, J. Dai, R. Wang, and W. Tang, "A segmented variable-parameter ZNN for dynamic quadratic minimization with improved convergence and robustness," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 5, pp. 2413–2424, May 2023.

[45] L. Jin, J. Zhao, L. Chen, and S. Li, "Collective neural dynamics for sparse motion planning of redundant manipulators without hessian matrix inversion," *IEEE Trans. Neural Netw. Learn. Syst.*, early access, Feb. 16, 2024, doi: 10.1109/TNNLS.2024.3363241.

[46] B. Zhang, S. Li, X. Chen, and Y. Mao, "A novel zeroing neural model for solving dynamic matrix Moore-Penrose inverse and its application to visual Servoing control of manipulator," *IEEE Trans. Instrum. Meas.*, vol. 73, p. 1–13, Feb. 2024.
[47] T. Wang, D. Wang, and K. Wu, "Chaotic adaptive synchronization control and application in chaotic secure communication for Industrial Internet of Things," *IEEE Access*, vol. 6, pp. 8584–8590, 2018.
[48] F. Ren, M. Jiang, H. Xu, and M. Li, "Quasi fixed-time synchronization of memristive Cohen-Grossberg neural networks with reaction-diffusion," *Neurocomputing*, vol. 415, pp. 74–83, Nov. 2020.

Jie Jin received the B.Sc. degree from Shenzhen University, Shenzhen, China, in 2007, and the M.S. degree and the Ph.D. degree in computer science and Technology from Hunan University, Changsha, China, in 2010 and 2015, respectively.

He is currently an Associate Professor with the School of Information and Electrical Engineering, Hunan University of Science and Technology, Xiangtan, China. His main research interests include neural networks, robotics, and integrated circuits design.

Mengfan Wu received the B.S. degree in electronic information engineering from Changsha Normal University, Changsha, China, in 2023. He is currently pursuing the master's degree with the School of Information and Electrical Engineering, Hunan University of Science and Technology, Xiangtan, China.

His current research interests include neural networks, chaotic systems, and image encryption.

Aijia Ouyang received the Ph.D. degree in computer science from Hunan University, Changsha, China, in 2015.

He has published more than 60 research papers in international conference and journals of intelligence algorithm and parallel computing. His research interests include intelligence computing, parallel computing, cloud computing, and data mining.

Keqin Li (Fellow, IEEE) received the Ph.D. degree in computer science from the University of Houston, Houston, Texas, USA, in 1990.

He is currently a SUNY Distinguished Professor of Computer Science with the State University of New York, New Paltz, NY, USA. He has published over 620 journal articles, book chapters, and refereed conference papers. His current research interests include cloud computing, fog computing, mobile-edge computing, energy-efficient computing and communication, embedded systems, cyber–physical systems, heterogeneous computing systems, big data computing, high-performance computing, CPU–GPU hybrid and cooperative computing, computer architectures and systems, computer networking, machine learning, and intelligent and soft computing.

Prof. Li received several best paper awards. He currently serves or has served on the editorial boards of IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE TRANSACTIONS ON COMPUTERS, IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE TRANSACTIONS ON SERVICES COMPUTING, and IEEE TRANSACTIONS ON SUSTAINABLE COMPUTING.

Chaoyang Chen (Senior Member, IEEE) received the Ph.D. degree in control science and engineering from Huazhong University of Science and Technology, Wuhan, China, in 2014.

He was a Postdoctoral Fellow with the School of Information Science and Engineering, Central South University, Changsha, China, from 2015 to 2017. He was a Visiting Researcher with the Center for Polymer Studies and the Department of Physics, Boston University, Boston, MA, USA, from 2018 to 2019. He is currently the Director of the Institute of Complex Systems Analysis and Control and an Associate Professor with the School of Information and Electrical Engineering, Hunan University of Science and Technology, Xiangtan, China. His current research interests include networked control systems, complex networks, multiagent systems, robust control, and their related applications.