Medical Image Encryption by Content-Aware DNA Computing for Secure Healthcare

Yirui Wu, *Member, IEEE*, Lilai Zhang, Stefano Berretti, *Senior Member, IEEE*, and Shaohua Wan, *Senior Member, IEEE*

***Abstract*—There exists a rising concern on security of healthcare data and service. Even small lost, stolen, displaced, hacked, or communicated in personal health data could bring huge damage to patients. Therefore, we propose a novel content-aware deoxyribonucleic acid (DNA) computing system to encrypt medical images, thus guaranteeing privacy and promoting secure healthcare environment. The proposed system consists of sender and receiver to perform tasks of encryption and decryption, respectively, where both contain the same structure design, but perform opposite operations. In either sender or receiver, we design a randomly DNA encoding and a content-aware permutation and diffusion module. Considering introducing random mechanism to increase difficulty of cracking, the former module builds a random encryption rule selector in DNA encoding process by randomly mapping quantity of medical image pixels to outputs. Meanwhile, the latter module constructs a permutation sequence, which not only encodes information of pixel values, but also involves redundant correlation between adjacent pixels located in a patch. Such design brings awareness property of medical image content to greatly increase complexity in cracking by embedding semantical information for encryption. We demonstrate that the proposed system successfully improve cybersecurity of medical images against various attacks in robustness and effectiveness when transmitting data in wireless broadcasting scenarios.**

***Index Terms*—Context-aware DNA permutation and diffusion, cybersecurity for healthcare system, DNA computing, medical image encryption.**

Manuscript received 28 March 2022; revised 20 June 2022; accepted 21 July 2022. Date of publication 28 July 2022; date of current version 13 December 2022. This work was supported in part by the National Key R&D Program of China under Grant 2021YFB3900601, in part by the National Natural Science Foundation of China under Grant 62172438, and in part by the Fundamental Research Funds for the Central Universities under Grant B220202074. Paper no. TII-22-1295. *(Yirui Wu and Lilai Zhang contributed equally to this work.) (Corresponding author: Shaohua Wan.)*

Yirui Wu and Lilai Zhang are with the Key Laboratory of Water Big Data Technology of Ministry of Water Resources, Hohai University, Nanjing 210096, China, and also with the College of Computer and Information, Hohai University, Nanjing 210096, China (e-mail: wuyirui@hhu.edu.cn; zhanglilai1999@gmail.com).

Stefano Berretti is with the Department of Information Engineering (DINFO), University of Florence, 50139 Florence, Italy (e-mail: stefano.berretti@unifi.it).

Shaohua Wan is with the Shenzhen Institute for Advanced Study, University of Electronic Science and Technology of China, Shenzhen 518110, China (e-mail: shaohua.wan@uestc.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2022.3194590.

Digital Object Identifier 10.1109/TII.2022.3194590

I. Introduction

With the involvement of cloud computing and Internet of Medical Things, the healthcare system has been greatly progressed by improving clinical treatment experiment and reducing patients' cost. However, healthcare is an attractive target for cybercrime, due to its high value and weak defences. Researchers generally define information lost, stolen, displaced, hacked, or communicated without unofficial recipients as a cybersecurity breach of healthcare information. It was reported in [1] that about 94% of healthcare organizations have experienced at least one cyberattack and 150 million patient health records have been breached between 2009 and 2014.

Among cybersecure solutions for different kinds of cyber threats, we aim to improve security under cryptographic attack, which is carried out with the intention of revealing information that has been encrypted. Cloud-based healthcare systems could transmit patients' large size medical images at an ease of expendability and mobility. However, problems of privacy disclosure, copyright flouting, illegal redistribution, and identity theft arise even with the encryption process, since healthcare data are substantially valuable estimated as over 1000 dollars per patient [2]. Aiming to guarantee the security of medical images in the transfer process, an efficient and reliable image encryption system is required. Famous methods, such as rivest, shamir, adleman (RSA), data encryption standard (DES), advanced encryption standard (AES), and international data encryption algorithm (IDEA), are widely used to protect text structure data by regarding images as common high-dimensional data. Since medical images own unique characteristics of strong correlation between adjacent pixels with high redundancy, we prefer special designed image encryption methods. Due to the promising properties of high speed, parallelism computation, minimal storage, and unbreakable cryptosystms, deoxyribonucleic acid (DNA) computing is adopted to encrypt medical images in the transfer process other than common methods, such as chaos [3], elliptic curve cryptography (ECC) [4]–[6], etc.

Following the idea of DNA computing for encryption, a content-aware DNA computing for medical image encryption is put forward in this article, designed with the following three goals for realization.

1) *Consistent and High-Capacity Workflow for Medical Image Encryption:* Generally, healthcare professionals prefer smooth workflow with real-time and consistent response to reach the final conclusion in clinical diagnosis. If adopting complicated and annoying image encryption

workflow, professionals might resist encryption in transfer process to improve security.

2) *Secure Ability Using Random Mechanism and Image Data for High Complexity:* Random mechanism is widely recognized as a means to increase difficulty of cracking. Meanwhile, images themselves recognized as high-dimensional data can be a natural source to bring high complexity. How to encode both source of complexity still remains an open question.
3) *Content-Aware Encryption for Medical Images:* Due to properties of taken devices, medical images generally own strong correlation between adjacent pixels with high redundancy. In other words, local and neighboring pixels share the characteristics of naturally and smoothly varying. How to link image content and encryption process for higher complexity becomes our focus in this article.

Inspired by these ideas, highlights of the proposed work are listed as follows:

1) Building on DNA encoding and permutation, the proposed method not only involves its high-speed and parallelism computation for real-time performance, but also utilizes the minimal storage property to guarantee high-capacity ability with small cost.
2) We introduce a randomly DNA encoding module to build random mappings between image pixels and computing and a content-aware permutation and diffusion module to construct a content-related permutation sequence, where both modules greatly improve secure ability.
3) Inspired by neighboring characteristics of medical image pixels, the content-aware DNA permutation and diffusion module reorganizes the transmitting data structure by highly nonlinear functions for higher difficulty in cracking, which originate from the correlation relationship of pixels and patches in medical images.

II. Related Work

A. Cybersecurity for the Healthcare System

Facing serious crime in cybersecurity, it is crucial to develop technologies for protection of patients' safety. To offer background knowledge, Bhuyan et al. [1] systematically examined cybersecurity threats in healthcare, and classified cyberattacks to different types. They laid a firm foundation for healthcare organizations and policymakers in better understanding cybersecurity.

Focusing on a special category of cyber threats to the healthcare system, researchers have proposed quantity of solutions. For example, to place real-time, affordable, and consistent cyber-physical systems (CPS) in healthcare applications, Rajhans et al. [7] deployed a structural approach for CPS by applying semantic mappings to assure reliability and activate scheme-level validation. Regarding cyber defence as a collaborative effort between employees and the administrative members of the healthcare organization, Singh and Sittig [8] presented recommendations aiding healthcare professionals, which successfully identify phishing email attacks in practice. Considering the purpose of reducing the load of terminal equipment, Wang et al. [9] introduced an edge computing framework into the encryption algorithm where the plain image is encoded to generate redundant data, and then divided into three parts. Each part cannot reconstruct plaintext and is stored in terminal, edge device, and cloud server, respectively. Although this method reasonably distributes the load, it still needs to transmit partially redundant plain image data, making it vulnerable to differential attack.

Recently, Kessler et al. [10] argued that the majority of data breaches lies with employee negligence and/or carelessness on information security. They thus built a cybersecurity risk method to model employee behavior surrounding information security where they introduced the information security climate index as a parsimonious tool to represent an extensive validation effort. Using cognitive computing, Ogiela and Ogiela [11] proposed a linguistic biometric threshold scheme for data sharing where the biometric stage was designed to allocate secret data to their respective owners with biometric labeling. Such process can facilitate the management of healthcare data at basic, fog, and cloud levels, providing high efficiency and security for sharing and distribution processes [12], [13]. By utilizing latest technologies, Nguyen et al. [14] proposed a secure intrusion detection with blockchain-based data transmission and artificial intelligence-based classification model for a cyberphysical system in healthcare sector, which involve blockchain and artificial intelligence (AI) for better security in healthcare. Last but not least, Nifakos et al. [15] offered a systematic review, which first identifies commonly encountered solutions that mitigate the cyber defence strategy, and then reviews organizational risk assessment methodologies to strengthen cybersecurity.

Security risks increase with more users connecting their devices to different application servers over the internet. Acar et al. [16] introduced a biometric template with wearable assisted keystroke dynamic privacy-aware continuous authentication protocol to capture the users' behavioral features to continuously monitor user behaviors to adjust their access based on the activity they have performed. Soni et al. [17] proposed a secure scheme for medical data transmission through continuous real-time monitoring of the user in the background. It collects five body positions of the user while performing six activities as behavioral features in the background of the current session.

In consideration of the suddenness, randomness, and urgency of healthcare events, it is a necessity to minimize the latency and the energy consumption of the users. How to process data at the minimum cost while under the ensurance of data security has become a thorny problem. Medical data have relatively low tolerance to risk, so it should be considered more from the perspective of data security. Apostolopoulos et al. [18] presented a risk-based distributed framework, which allow the users to determine the computation load to be offloaded at each multi-access edge computing (MEC) server under risk. It properly captures users' behavior under losses and gains, and strike a balance between safety and efficiency.

B. Image Encryption Methods

Unlike text structure data cryptography with quantity of mature algorithms, image cryptography is an emerging and developing field, due to its high-dimensional and unstructured

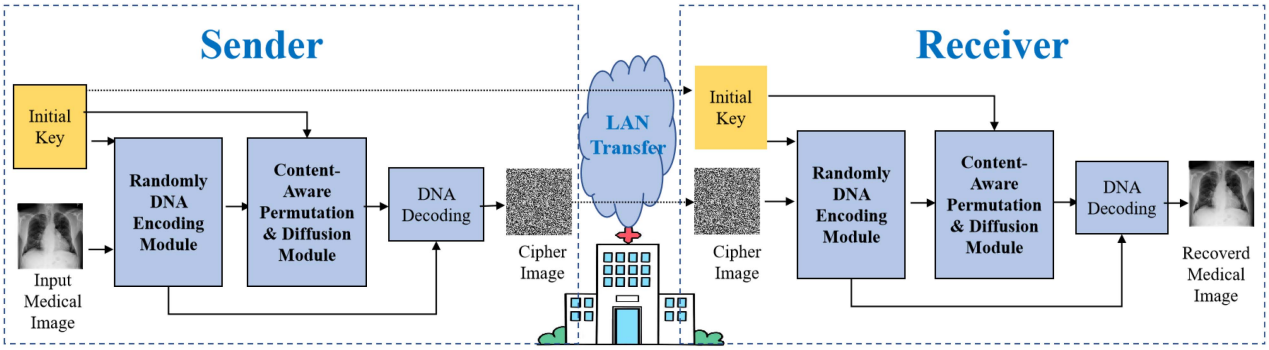

Fig. 1. General workflow of a sender, local area network (LAN) transfer, and a receiver in healthcare organization where sender and receiver correspond to the encryption process and decryption process, respectively.

data arrangement. For example, Shankar et al. [19] proposed a new red, green, blue (RGB)-based share creation model using an ECC method, which first generates a set of shares for an individual image, and then undergoes encryption and decryption using ECC to attain both privacy and safety. However, as an asymmetric encryption, ECC has high security, complex structure, and large amount of computation, and is not suitable for occasions with high urgency, such as healthcare events. Later, Anand and Singh [20] proposed a secure data hiding in fused medical image for smart healthcare where they first created a fused medical image as a cover by nonsubsampled contourlet transform, then the method could be applied to conceal the image and electronic patient records mark into the fused image. They claimed their methods have achieved a balanced compromise with the privacy and security of medical images.

Recently, Li et al. [21] proposed a novel chaos-based image encryption scheme by using randomly DNA encode and plaintext-related permutation, where they randomly encoded plain image into a nucleotide sequence with piecewise linear chaotic map (PWLCM). Most relevant to our work, Chen et al. [22] proposed a secure and efficient image encryption method, where self-adaptive permutation–diffusion model utilized the reusability of the random variables to promote efficiency of the cryptosystem. Later, Zhang et al. [23] proposed a multi-image encryption algorithm, which protects the content security of multiple images and improve the transmission speed based on technologies of image hash, bit-plane decomposition, and dynamic DNA coding.

III. Proposed Method

The generic framework of our proposed work is shown in Fig. 1, where the algorithm descriptions for sender and receiver are represented as encryption and decryption process in Algorithm 1 and 2, respectively. It is noted that DNA decoding procedures can be seen as the inverse process of the previous DNA encoding procedures. Therefore, we can notice that both sender and receiver share the same modules, i.e., randomly DNA encoding module and content-aware permutation and diffusion module. We then goes into the following two modules for algorithm explanation.

Algorithm 1: Encryption process.

Data: Initial key K, plain image I
Result: Cipher image C
1: Input a $m \times n$ plain image I and an initial key K into the random DNA encoding module, and generate a DNA rule select sequence S_{rule} and a DNA image-encoded sequence S_1;
2: Input S_1 and K into the content aware permutation and diffusion module, and generate a permutated–diffused DNA sequence S_2;
3: Input S_2 and S_{rule} into the content aware permutation and diffusion module, use the S_{rule} as the rule selector to decode S_2 and generate the cipher image C;
4: Transmit C to the receiver

Algorithm 2: Decryption process.

Data: Initial key K, cipher image C
Result: Plain image I
1: Receive and input the cipher image C with an initial key K into the random DNA encoding module, and generate the DNA rule select sequence S_{rule} and a reverse DNA image encoded sequence S_1^r.
2: Input S_1^c and K into the content-aware permutation and diffusion module, and generate a reverse permutated diffused DNA sequence S_2^r.
3: Input S_2^r and S_{rule} into the content-aware permutation and diffusion module, use the S_{rule} as the rule selector to decode S_2^r and generate the plain image I.

A. Randomly DNA Encoding Module

The DNA encoding process reconstructs the image data into DNA format for later calculation. The advantage of DNA encoding is that there are several different rules to choose, and we introduce chaotic system, which makes the variety of rules more diverse and elusive.

There are four kinds of DNA bases: 1) adenine (A); 2) guanine (G); 3) cytosine (C); and 4) thymine (T). Aadenine and thymine is a complementary pair, while cytosine and guanine is

TABLE I
DNA ENCODING RULES

DNA base	A	C	G	T
Rule 1	00	01	01	11
Rule 2	00	10	10	11
Rule 3	01	11	00	10
Rule 4	01	00	11	10
Rule 5	10	11	00	01
Rule 6	10	00	11	01
Rule 7	11	01	01	00
Rule 8	11	10	10	00

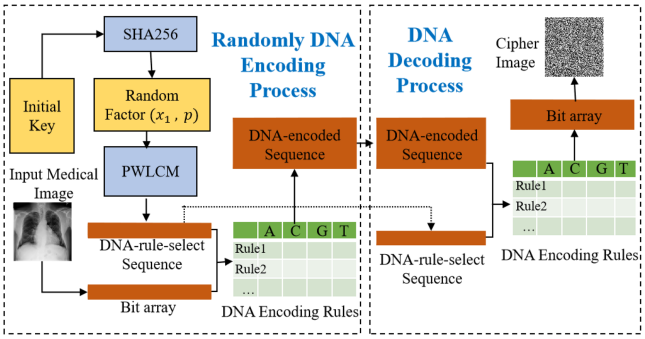

Fig. 2. Workflow of the randomly DNA encoding process and DNA decoding process inside encryption.

a complementary pair in human genome. In this case, there are totally eight kinds of encoding rules, as given in Table I.

The module proposed in this section needs to randomly select different rules for encoding each pixel in the image. As shown in Fig. 2, the SHA256 algorithm is used to calculate the hash value of the initial key and generate a random factor, which is a necessary initialization parameter for the PWLCM to generate a pesudo random DNA-rule-select sequence. By using this chaotic map, a small change in the initial random factor will lead to huge variation in the generated sequence, which can significant improve the key sensitivity of the cryptosystem. Finally, this sequence is used to establish the mapping between each byte in the image data and the eight different DNA encoding rules. The PWLCM is defined as

$$x_{n+1} = \begin{cases} \frac{x_n}{p}, & 0 \le x < p \\ \frac{x_n - p}{0.5 - p}, & p < x \le 0.5 \\ F(1 - x_n, p), & 0.5 < x \le 1 \end{cases} \quad (1)$$

where the initial input x_1 is abovementioned the random factor and the $p \in (0, 0.5]$ is a parameter of PWLCM. The whole encoding process is explained in detail in the following pesudo code Algorithm 3.

B. Content-Aware Permutation and Diffusion Module

Permutation and diffusion are two basic methods of symmetric encryption. However, traditional methods either only generate the permutation sequence by the key, where the sensitivity to content is weak [24], or need to transfer the hash value of the original graph to the encryption part that pose a threat to the security [25]. In contrast, our method take advantage of the reversibility of permutation operation and the commutative law of DNA operation, and cleverly realize the reversible content-related permutation and diffusion without transmitting any data other than the cipher image. It overcomes the shortcomings of both the abovementioned two methods.

Algorithm 3: Randomly DNA encoding process.

Data: Initial key K, plain image I
Result: DNA rule-select sequence S_{rule}, DNA image-encoded sequence S_1
1: Change the plain image I into bit array I_{bit};
2: len $\leftarrow$ Length(I_{bit});
3: HASH$_K$ $\leftarrow$ SHA256(K);
4: $H_1, H_2 \leftarrow$ HASH$_K$;
5: $x_1 = \text{mod}(H_1/10^{15}, 1)$, $p = \text{mod}(H_2/10^{15}, 1)$;
6: Put x_1, p into PWLCM to generate a sequence $X = [x_1, x_2, \ldots, x_n]$ by iterating;
7: $S_{\text{rule}} = \text{mod}(\text{floor}(\boldsymbol{X} \times 10^{15}), 8)$;
8: Introduce the DNA encoding Table T;
9: **For**(i = 0 **to** 2 $\times$ len);
10: $S_1(i) \leftarrow T(S_{\text{rule}}(i), I_{\text{bit}}(2i, 2i+1))$;

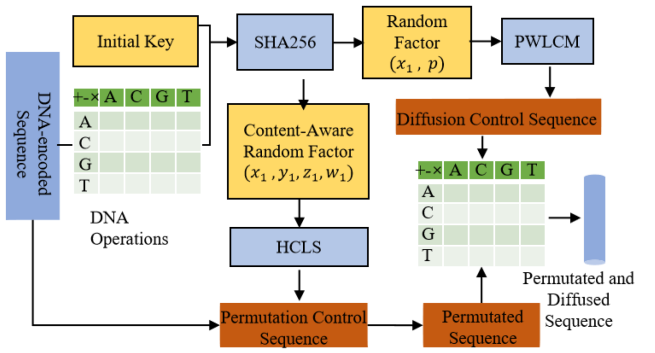

Fig. 3. Structure design of the proposed content-aware permutation and diffusion module.

The content-aware permutation and diffusion module, as shown in Fig. 3, contains the reversible plaintext-related permutation algorithm and the diffusion algorithm that the information of plain image can directly calculated in the decryption part without transmitting from the encryption part. These two algorithms take advantage of three types of DNA operations: 1) ADD; 2) SUB; and 3) XOR.

Compared with traditional mathematical and logical operations, these DNA operations contain more diversified forms, which improve the variability of encrypted sequences. Meanwhile, as the DNA encoding itself may involve redundant correlation between adjacent pixels in the image, the DNA operation based on that will be more sensitive to the correlation information.

In particular, it can be seen that the abovementioned ADD and XOR operations satisfy the commutative law, which means that the result of these operations is exactly the same for the DNA sequence before and after permutation. So, the

Algorithm 4: Permutation process.

Data: Initial key K, DNA image-encoded sequence S_1
Result: Permutated Sequence S_1^p
TA :DNA ADD table);
TX :DNA XOR table);
len $\leftarrow \text{Length}(S_1)$;
$AR \leftarrow S_1(0); XR \leftarrow S_1(0)$;
For(i $= 1$ **to** len);
    $AR \leftarrow TA(AR, S_1(i))$;
    $XR \leftarrow TX(XR, S_1(i))$;
$\text{HASH}_D \leftarrow \text{SHA256}([AR, XR])$;
$\text{HASH}_K \leftarrow \text{SHA256}(K)$;
$\text{HASH}_{DK} \leftarrow \text{HASH}_D \oplus \text{HASH}_K$;
$A_1, A_2, A_3, A_4 \leftarrow \text{HASH}_{DK}$;
$x_1 \leftarrow (\text{mod}(\text{fix}(A_1/10^8), 80) - 40) + (A_1/10^{14} - \text{fix}(A_1/10^{14}))$;
$y_1 \leftarrow (\text{mod}(\text{fix}(A_2/10^8), 80) - 40) + (A_2/10^{14} - \text{fix}(A_2/10^{14}))$;
$z_1 \leftarrow (\text{mod}(\text{fix}(A_3/10^8), 80) + 1) + (A_3/10^{14} - \text{fix}(A_3/10^{14}))$;
$w_1 \leftarrow (\text{mod}(\text{fix}(A_4/10^8), 500) - 250) + (A_4/10^{14} - \text{fix}(A_4/10^{14}))$;
For($i = 0$ **to** length(S_1));
    $x_{i+1}, y_{i+1}, zi + 1, w_{i+1} = \text{HCLS}(x_i, y_i, zi, w_i)$;
X=[$x_1, x_2, \ldots$];
$S_p = \text{mod}(\text{floor}(\boldsymbol{X} \times 10^{15}), \text{len})$;
If(This is encryption process);
    $m = 0, n = \text{len}/2$;
Else;
    $m = \text{len}/2, n = 0$;
For($k = m$ **to** n);
    $S_1(S_p(k)) \leftrightarrow S_1(S_p(\text{len} - k))$;
$S_1^p \leftarrow S_1$

permutation procedures of the encryption and decryption processes can be realized with the same algorithm and parameters, without transmitting additional data in the LAN.

In the permutation procedure, the proposed module first uses XOR and ADD operations to calculate a result (x_1, y_1, z_1, w_1) based on initial key K and DNA-encoded sequence S_1, the detailed process is shown in the pesudo code Algorithm 3. Then, input this result into the hyperchaotic Lorenz system (HCLS) to generate a content-aware permutation control sequence S_p. The HCLS is given by

$$\begin{cases} x_{n+1} = a(y_n - x_n) + w_n \\ y_{n+1} = cx_n - y_n - x_n z_n \\ z_{n+1} = x_n y_n - b_n z_n \\ w_{n+1} = -y_n z_n + \gamma w_n \end{cases} \tag{2}$$

where a, b, c, and γ are the parameters of HCLS, and the system is chaotic when $a = 10, b = 8/3, c = 28$, and $\gamma \in [-1.52, -0.06]$. Then, the permutation process is shown in detail in Algorithm 4.

Then, we make the permutation control sequence the rule perform content-aware permutation, and get a permutated sequence. After this, the permutated sequence is input into the

Algorithm 5: Diffusion process (encryption).

Data: Initial key K, DNA rule-select sequence S_r, permutated sequence S_1^p
Result: Permutated and diffused sequence S_2
Change the plain image I into bit array I_{bit};
len $\leftarrow \text{Length}(S_p)$;
$\text{HASH}_K \leftarrow \text{SHA256}(K)$;
$H_1 \leftarrow \text{HASH}_K(128:191); H_2 \leftarrow \text{HASH}_K(192:255)$;
$x_1 = \text{mod}(H_1/10^{15}, 1)$;
$p = \text{mod}(H_2/10^{15}, 1)$;
Put x_1, p into PWLCM to generate a sequence $X = [x_1, x_2, \ldots, x_n]$ by iterating;
$Y = \text{mod}(\text{floor}(\boldsymbol{X} \times 10^{15}), 256)$;
Introduce the DNA encoding table T;
For(i $= 0$ **to** $2 \times$ len);
    $S_{\text{key}}(i) \leftarrow T(S_{\text{rule}}(i), Y(2i, 2i+1))$;
Introduce the DNA ADD table TA; introduce the DNA SUB table TS; Introduce the DNA XOR table TX;
If(encrypting)
  $D(0) \leftarrow TA(S_p(0), S_{\text{key}}(0))$;
  $D(0) \leftarrow TX(D(0), S_{\text{key}}(0))$;
  For $i = 1$ **to** len $- 1$;
    If $\text{mod}(i, 2) = 1$ then;
      $D(i) \leftarrow TX(S_p(i), S_{\text{key}}(i))$;
      $D(i) \leftarrow TX(D(i), D(i-1))$;
    Else;
      $D(i) \leftarrow TA(S_p(i), S_{\text{key}}(i))$;
      $D(i) \leftarrow TX(D(i), D(i-1))$;
Else;
  For $i =$ len $- 1$ **to** 1;
    If $\text{mod}(i, 2) = 1$ then;
      $D(i) \leftarrow TX(S_p(i), S_{\text{key}}(i))$;
      $D(i) \leftarrow TX(D(i), S_p(i-1))$;
    Else;
      $D(i) \leftarrow TA(S_p(i), S_p(i))$;
      $D(i) \leftarrow TX(D(i), S_{\text{key}}(i-1))$;
  $D(0) \leftarrow TA(S_p(0), S_{\text{key}}(0))$;
  $D(0) \leftarrow TX(D(0), S_{\text{key}}(0))$

DNA diffusion process. During this procedure, the initial key K is utilized again to generate a diffusion control sequence. Finally, DNA operations are used to calculate between the permutated sequence and diffusion control sequence, then generate the permutated and diffused sequence. Detailed processes are shown in the pesudo code Algorithm 5.

IV. Experiment

A. Datasets

We selected ChestXray-14, COVID-CT, and fcon_1000 as our datasets. ChestX-ray14 is a medical imaging dataset, which comprises 112 120 1024 $\times$ 1024 $\times$ 8 b single-channel frontal-view X-ray images of 30 805 unique patients. The COVID-CT dataset has 349 CT images containing clinical findings of COVID-19 from 216 patients. These CT images have no specific

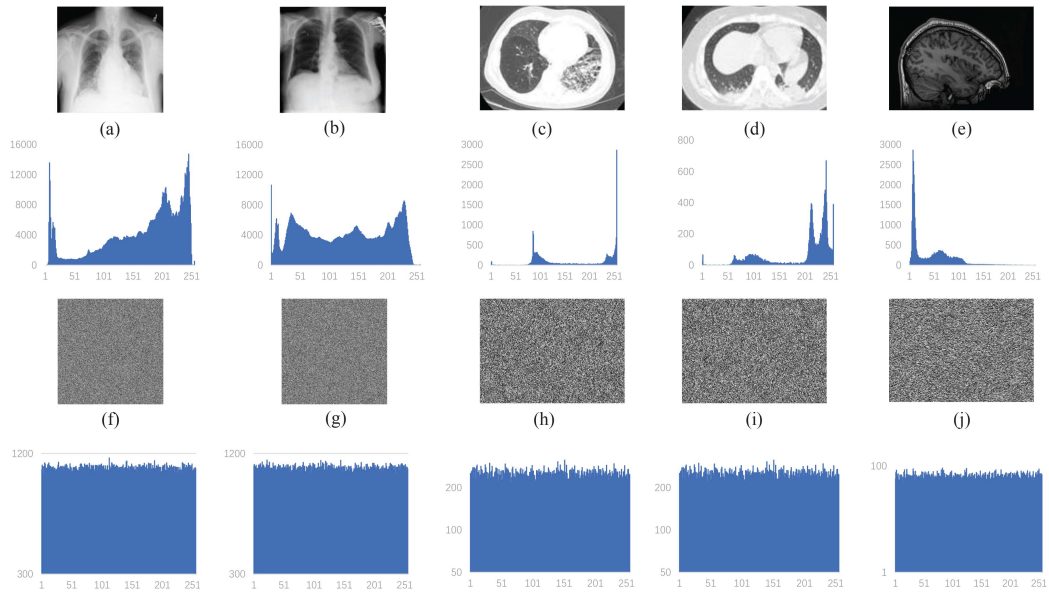

Fig. 4. Histograms of images before and after encryption. (a) and (b) Images of representative chest X-ray images. (c) and (d) Chest CT images from the COVID-CT dataset. (e) Brain magnetic resonance image from the fcon1000 dataset. (f)–(j) Their corresponding cipher image. The graphs under them are the histograms.

size, but are also 8-b single-channel gray images. Fcon_1000 contains a large number of nii format brain magnetic resonance imaging (MRI) images. In our experiment, they are converted into 8-b gray images for processing.

B. Implement Details

The experiment is conducted on the proposed random computing deoxyribonucleic acid (RC-DNA) based on Python 3.8, with an HP personal laptop with Intel(R) Core(TM) i7-9750H CPU 2.60 GHz and 8 G Memory. And, the process runs on the system of Win10. Initial key is set as "HELLO-WORLD" in hexadecimal. The parameters of HCLS are set as $a = 10$, $b = 8/3$, $c = 28$, and $\gamma = -0.5$. Moreover, to verify effectiveness and feasibility of proposed cryptosystem on the transmission control protocol/internet protocol (TCP/IP)-based internet of things (IoT) environment, we test it on the LAN with a router Tenda-AC7 1200 M, and the image is transmitted via IP messenger.

C. Keyspace Analysis

Keyspace is the set of all valid, possible, and distinct keys of a given cryptosystem. Different cipher algorithms usually have different limit to the number of keys by their encryption rules. To resist a brute-force attack, the keyspace requires be large enough, no less than 2^{100}. There are the following two circumstances for the keyspace.

1) The internal keys of our cryptosystem are two parameters $p \in (0, 0.5)$ and two initial values $x_1 \in (0, 1)$ of two PWLCM and four initial values: a) $x_1 \in (-40, 40)$; b) $y_1 \in (-40, 40)$; c) $z_1 \in (1, 81)$; and d) $w_1 \in (-250, 250)$, of the HCLS system. Finally, the keyspace of RC-DNA can be calculated as $S = (0.5 \times 10^{15})^2 \times (1 \times 10^{15})^2 \times (80 \times 10^{14})^3 \times (500 \times 10^{14}) = 6.4 \times 10^{127} \approx 2^{418}$.
2) If the attacker gets the cipher image and expects to use brute force to get the initial key, the keyspace can be 2^{256} as the SHA256 algorithm has 2^{256} different outputs. These results show that our keyspace is far large enough for security.

D. Histogram Analysis

A histogram at each gray level reflects statistical indiscernibility of a cipher image. Its analysis results are shown in Fig. 4. The test plain images are shown in Fig. 4(a)–(e), and the corresponding cipher images in Fig. 4(f)–(j). It can be seen that the noise-like cipher image greatly hides the information of the image, making it difficult for attackers to obtain valid information through cipher images. Therefore, the proposed RC-DNA can resist statistical analysis attacks.

E. Pixel Correlation Analysis

In the field of image encryption, pixel correlation usually refers to the similarity between adjacent pixels. Images tend to have unique characteristics of strong correlation between adjacent pixels. And, encryption methods need to break the correlation to improves security. The correlation coefficient is given as

$$\begin{cases} r_{ab} = \frac{\operatorname{cov}(a,b)}{\sqrt{D(a)}\sqrt{D(b)}} \\ \operatorname{cov}(a,b) = \frac{1}{N}\sum_{i=1}^{N}(a_i - E(a))(b_i - E(b)) \\ D(a) = \frac{1}{N}\sum_{i=1}^{N}(a_i - E(a))^2 \\ E(a) = \frac{1}{N}\sum_{i=1}^{N} a_i \end{cases} \tag{3}$$

where $\operatorname{cov}(a, b)$ is the covariance between the image a and b and $E(a)$ and $D(a)$ are the expected and mean square error of image a, respectively.

TABLE II
CORRELATION COEFFICIENTS

Images	Plain Image			Cipher Image		
	V	H	D	V	H	D
X-ray1	0.8922	0.7470	0.7598	0.0021	0.0029	0.0016
X-ray2	0.9554	0.9422	0.9589	−0.0012	0.0023	−0.0009
COVID-CT1	0.9756	0.9583	0.9932	−0.0008	0.0012	−0.0019
COVID-CT2	0.9215	0.9638	0.9516	0.0009	0.0015	0.0023
MRI	0.9323	0.8924	0.9280	−0.0018	−0.0022	0.0014

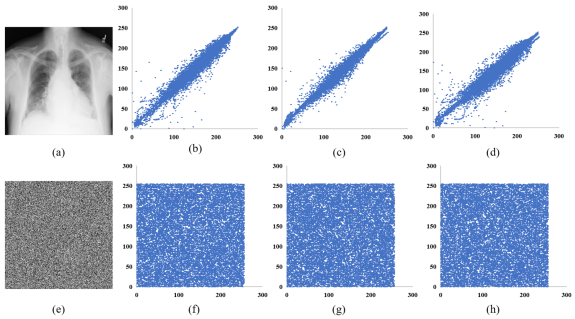

Fig. 5. (a) and (e) Correlation coefficients distributions of chest X-ray image and its cipher image, respectively. In the graph, a point represents a pixel, and the value of its abscissa is its gray value. (b) and (f) Ordinates in these are the gray value of right adjacent pixel. (c) and (g) Ordinates in these are the gray value of lower adjacent pixel. (d) and (h) Ordinates in these are the gray value of lower right adjacent pixel.

TABLE III
INFORMATION ENTROPY

Image	Babbon	Bridge	Chest	Luna	Hohai
Entropy	7.998432	7.999252	7.993527	7.998823	7.994215

The correlation coefficients of some images are given in Table II. The results show that the plain images have strong correlation between adjacent pixels in different directions, while the corresponding cipher image almost has no correlation. Also, Fig. 5 is present to intuitively display the comparison of correlation of the image before and after encryption. Our algorithm successfully breaks the correlation between adjacent pixels. This mainly owe to the randomness of the proposed DNA encoding process and the permutation algorithm.

F. Information Entropy Analysis

Information entropy is a measure of data uncertainty that can reflect the diffusion performance of an image cryptosystem. Generally, the greater the entropy of the cipher image is, the harder it will be for the attacker to crack. As this experiment is conducted on 8-b gray images, the equation of information entropy is

$$H = -\sum_{i=1}^{256} p(e_i) \log_2 p(e_i) \tag{4}$$

where e_i means the event that the current pixel value is i and $P(e_i)$ means the probability of e_i. The experimental results of the proposed method are given in Table III. For the ideal case of a K-b image, the information entropy is $H = K$. The information entropy of the 8-b encrypted images by our proposed cryptosystem is close to 8, indicating that it has good diffusion performance.

TABLE IV
AVERAGE VALUES OF NPCR AND UACI FOR THE SENSITIVITY OF THE PLAIN IMAGE

Images	NPCR	UACI
Baboon	99.6120	33.4824
Bridge	99.6221	33.4817
Chest	99.6132	33.5012
Lena	99.6112	33.4254
Hohai	99.6178	33.4910

TABLE V
VALUES OF NPCR AND UACI FOR THE SENSITIVITY OF THE KEY

Cipher Image	NPCR	UACI
$E_1 \leftrightarrow E_2$	99.6012	33.3712
$E_1 \leftrightarrow E_3$	99.6091	33.4322
$E_2 \leftrightarrow E_3$	99.5223	33.4215

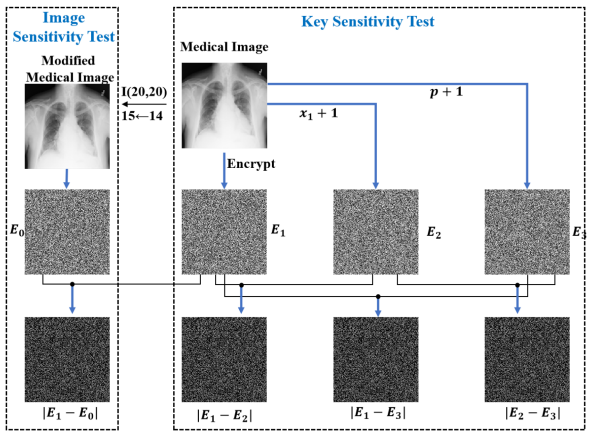

Fig. 6. Differential cipher image. Both image sensitivity and key sensitivity are shown in this figure.

G. Sensitivity Analysis

Differential attack usually used to change the value of a pixel or several pixels in the plain image, and compares the difference between two corresponding cipher images. In that case, the sensitivity of the cryptosystem is very important in resisting the differential attack. There are two indexes to evaluate the sensitivity: 1) number of pixels change rate (NPCR); and 2) unified average changing intensity. They are given as follows:

$$\begin{cases} \text{NPCR} = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} D_{ij} \times 100\% \\ \text{UACI} = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} \left(\frac{I(i,j) - I'(i,j)}{255} \right) \times 100\% \end{cases} \tag{5}$$

where $D_{ij} = \begin{cases} 1, I(i,j) \neq I'(i,j) \\ 0, I(i,j) = I'(i,j) \end{cases}$ and I and I' are the cipher images before and after the plain image changed by 1 pixel, respectively.

The sensitivity of the proposed cryptosystem is estimated in two aspects: 1) plain image sensitivity; and 2) key sensitivity. First, we test the sensitivity of plain images. We conduct this experiment by changing a certain pixel value of a plain image. Fig. 6 shows the effect of changing the value of the pixel (20,

TABLE VI
ABLATION STUDY

Cryptosystems	Correlation			Entropy	Sensitivity	
	V	H	D		NPCR	UACI
Case1	0.0096	–0.0092	–0.0053	7.2894	94.3892	29.4581
Case2	0.0084	0.0102	–0.0024	7.2378	95.2349	30.4258
Case3	–0.0023	0.0024	0.0011	7.6823	98.7118	33.2084
Case4 (The proposed)	0.0014	0.0009	0.0004	7.9992	99.6841	33.5539

TABLE VII
COMPARISON ON SEVERAL SECURITY INDEXES

Cryptosystems	Correlation			Entropy	Sensitivity	
	V	H	D		NPCR	UACI
Zhan et al. [26]	0.0039	0.0052	0.0215	7.9978	76.26	28.30
Chai et al. [27]	–0.0082	–0.0068	0.0036	7.9992	99.62	33.51
Yan et al. [28]	–0.0056	–0.0012	–0.0020	7.9994	99.62	33.55
Aouissaoui et al. [29]	0.0240	0.0014	–0.0014	7.9978	99.6552	33.5871
Chen et al. [22]	–0.0064	0.0003	0.0110	7.9993	99.6218	33.5084
Zhang et al. [23]	0.0000016	–0.000003	–0.0000001	–	99.5009	33.4408
Proposed	0.0014	0.0009	0.0004	7.9992	99.6841	33.5539

20) from 14 to 15 in the chest image. Moreover, we calculate the NPCR and UACI of the five images for 20 times, and the average results are given in Table IV. The values of NPCR and UACI in RC-DNA are both close to their theoretical values, which means our cryptosystem is sensitive to plain images.

Second, we evaluate the sensitivity of the key. We select the image "Bridge" and encrypt it to cipher image E_1 by using initial key "HELLO-WORLD" to get the "random factor" $(x_1 = 0.401894441844344, p = 0.33533929244635197)$, which is explained in Section III-B. Then, make changes as $x_1 = x_1 + 10^{-14}$, to generate the cipher image E_2, and $p = p + 10^{-14}$, to generate E_3. We still use the NPCR and UACI to estimate the difference between the three cipher images, the results are given in Table V and Fig. 6.

H. Computation Cost Analysis

Due to the character of high-speed and parallelism, DNA computing has advantage of encrypting large numbers of image data. In the proposed cryptosystem, the two main time consumption processes are: 1) PWLCM; and 2) HCLS, and the time complexity of both processes is $O(m \times n)$, proportional to the size of the image. Using the software and hardware mentioned in Section IV-A, encryption of a 256×256 image totally costs 2.12 s and that of a 512×512 image costs 9.56 s. The time consumption is satisfactory in the Python 3.8 environment. If it can be large scale applied in IoT in the future, with the support of high-performance software and hardware dedicated to DNA computing, the speed of our algorithm can be higher.

I. Ablation Study

In this section, we performed ablation experiments on the two modules in Section III. The choice between the two modules can be divided into the following four cases and the result is presented in Table VI.

1) There is no randomly DNA encoding for plain image. Permutation and diffusion are performed directly at pixel level and not content related.
2) No randomly DNA encoding for plain images. Content-aware permutation and diffusion are performed directly at pixel level.
3) There is a randomly DNA encoding process, but permutation and diffusion module is not content related.
4) There is a randomly DNA encoding process, and content-aware permutation and diffusion are also performed.

It can conducted from Table VI that the pixel gray-value distribution of medical images is usually concentrated, which can be confirmed from Fig. 4. Pixel-level diffusion and displacement operations cannot solve this problem. Therefore, without random DNA coding, the performance of encryption will be very poor.

The content-aware method increases the sensitivity of the algorithm to plain image, so it achieves good results in NPCR and UACI.

J. Performance Comparisons

The comparison between the proposed RC-DNA and other state-of-the-art algorithms is given in Table VII. Although our method is not optimal in some certain indicators, but our method still achieves excellent results in general. Considering that other methods use RGB images as test samples, and our test samples are single-channel 8-medical images, the low color gamut will slightly affect the performance of our algorithm.

K. Implementation Details

The experiment is conducted on the proposed RC-DNA based on Python 3.8, with an HP personal laptop with Intel(R) Core(TM) i7-9750H CPU 2.60 GHz and 8 G Memory. And, the process runs on the system of Win10. Initial key is set as "HELLO-WORLD" in hexadecimal. The parameters of HCLS are set as $a = 10$, $b = 8/3$, $c = 28$, and $\gamma = -0.5$.

V. Conclusion

To ensure the security of cipher images, this article proposed a novel cryptosystem for secure healthcare with two effective modules: 1) randomly DNA encoding module; and 2) content-aware permutation and diffusion module. The former one builds a random encryption rule selector in DNA encoding process, which increases security by building quantity of random mappings from image pixels to computations and greatly improves key sensitivity. The latter module constructs a permutation sequence, which not only encodes information of pixel values, but also breaks the strong correlation between adjacent pixels located in a patch.

References

[1] S. S. Bhuyan et al., "Transforming healthcare cybersecurity from reactive to proactive: Current status and future recommendations," *J. Med. Syst.*, vol. 44, no. 5, 2020, Art. no. 98.

[2] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, 2018.

[3] M. Alawida, J. S. Teh, A. Samsudin, and W. H. Alshoura, "An image encryption scheme based on hybridizing digital chaos and finite state machine," *Signal Process.*, vol. 164, pp. 249–266, 2019.

[4] A. Abusukhon, Z. Mohammad, and A. Al-Thaher, "An authenticated, secure, and mutable multiple-session-keys protocol based on elliptic curve cryptography and text-to-image encryption algorithm," *Concurrency Comput., Pract. Experience*, vol. 34, no. 4, 2022, Art. no. e6649.

[5] A. Daoui, H. Karmouni, O. E. Ogri, M. Sayyouri, and H. Qjidaa, "Robust image encryption and zero-watermarking scheme using SCA and modified logistic map," *Expert Syst. Appl.*, vol. 190, 2022, Art. no. 116193.

[6] Z. Gu et al., "IEPSBP: A cost-efficient image encryption algorithm based on parallel chaotic system for green IoT," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 1, pp. 89–106, Mar. 2022.

[7] A. Rajhans et al., "Supporting heterogeneity in cyber-physical systems architectures," *IEEE Trans. Autom. Control.*, vol. 59, no. 12, pp. 3178–3193, Dec. 2014.

[8] H. Singh and D. F. Sittig, "A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks," *Appl. Clin. Inform.*, vol. 7, no. 2, pp. 624–632, 2016.

[9] T. Wang, Y. Mei, W. Jia, X. Zheng, G. Wang, and M. Xie, "Edge-based differential privacy computing for sensor-cloud systems," *J. Parallel Distrib. Comput.*, vol. 136, pp. 75–85, 2020.

[10] S. R. Kessler, S. Pindek, G. Kleinman, S. Andel, and P. E. Spector, "Information security climate and the assessment of information security risk among healthcare employees," *Health Informat. J.*, vol. 26, no. 1, pp. 461–473, 2020.

[11] L. Ogiela and M. R. Ogiela, "Cognitive security paradigm for cloud computing applications," *Concurrency Comput. Pract. Exp.*, vol. 32, no. 8, 2020, Art. no. e5316.

[12] A. G. Sreedevi, T. N. Harshitha, V. Sugumaran, and P. Shankar, "Application of cognitive computing in healthcare, cybersecurity, Big Data and IoT: A literature review," *Inf. Process. Manage.*, vol. 59, no. 2, 2022, Art. no. 102888.

[13] P. Radoglou-Grammatikis et al., "Modeling, detecting, and mitigating threats against industrial healthcare systems: A combined software defined networking and reinforcement learning approach," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 2041–2052, Mar. 2022.

[14] G. N. Nguyen, N. H. L. Viet, M. Elhoseny, K. Shankar, B. B. Gupta, and A. A. A. El-Latif, "Secure blockchain enabled cyber-physical systems in healthcare using deep belief network with resnet model," *J. Parallel Distrib. Comput.*, vol. 153, pp. 150–160, 2021.

[15] S. Nifakos et al., "Influence of human factors on cyber security within healthcare organisations: A systematic review," *Sensors*, vol. 21, no. 15, 2021, Art. no. 5119.

[16] A. Acar et al., "A lightweight privacy-aware continuous authentication protocol-paca," *ACM Trans. Privacy Secur.*, vol. 24, no. 4, pp. 1–28, 2021.

[17] P. Soni, J. Pradhan, A. K. Pal, and S. H. Islam, "Cybersecurity attack-resilience authentication mechanism for intelligent healthcare system," *IEEE Trans. Ind. Informat.*, early access, Jun. 1, 2022, doi: 10.1109/TII.2022.3179429.

[18] P. A. Apostolopoulos, E. E. Tsiropoulou, and S. Papavassiliou, "Risk-aware data offloading in multi-server multi-access edge computing environment," *IEEE/ACM Trans. Netw.*, vol. 28, no. 3, pp. 1405–1418, Jun. 2020.

[19] K. Shankar and P. Eswaran, "RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography," *China Commun.*, vol. 14, no. 2, pp. 118–130, Feb. 2017.

[20] A. Anand and A. K. Singh, "SDH: Secure data hiding in fused medical image for smart healthcare," *IEEE Trans. Computat. Social Syst.*, vol. 9, no. 4, pp. 1265–1273, Aug. 2022.

[21] Z. Li, C. Peng, W. Tan, and L. Li, "A novel chaos-based image encryption scheme by using randomly DNA encode and plaintext related permutation," *Appl. Sci.*, vol. 10, no. 21, 2020, Art. no. 7469.

[22] J. Chen, Z. Zhu, L. Zhang, Y. Zhang, and B. Yang, "Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption," *Signal Process.*, vol. 142, pp. 340–353, 2018.

[23] Q. Zhang, J. Han, and Y. Ye, "Multi-image encryption algorithm based on image hash, bit-plane decomposition and dynamic DNA coding," *IET Image Process.*, vol. 15, no. 4, pp. 885–896, 2021.

[24] W. Xingyuan, W. Yu, Z. Xiaoqiang, and L. Chao, "A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and dna level," *Opt. Lasers Eng.*, vol. 125, 2020, Art. no. 105851.

[25] E. Z. Zefreh, "An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions," *Multimedia Tools Appl.*, vol. 79, no. 33-34, pp. 24993–25022, 2020.

[26] K. Zhan, D. Wei, J. Shi, and J. Yu, "Cross-utilizing hyperchaotic and DNA sequences for image encryption," *J. Electron. Imag.*, vol. 26, no. 1, 2017, Art. no. 13021.

[27] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 1, pp. 219–237, 2019.

[28] X. Yan, X. Wang, and Y. Xian, "Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation," *Multimedia Tools Appl.*, vol. 80, no. 7, pp. 10949–10983, 2021.

[29] I. Aouissaoui, T. Bakir, and A. Sakly, "Robustly correlated key-medical image for dna-chaos based encryption," *IET Image Process.*, vol. 15, no. 12, pp. 2770–2786, 2021.

Yirui Wu (Member, IEEE) received the B.S. and Ph.D. degrees in computer science and technology from Nanjing University, Nanjing, China, in 2011 and 206, respectively.

He is currently an Associate Professor with Hohai University, Nanjing, China. His research interests include computer vision and multimedia understanding.

Lilai Zhang received the B.E. degree in computer science and technology from the Taiyuan University of Technology, Taiyuan, China, in 2021. He is currently working toward the M.E. degree in computer science and technology with the College of Computer and Information, Hohai University, Nanjing, China.

His research interests include computer vision and artificial intelligence.

Stefano Berretti (Senior Member, IEEE) received the Ph.D. degree in informatics and telecommunication engineering from the University of Florence, Florence, Italy, in 2001.

He is currently an Associate Professor with Media Integration and Communication Center and the Department of Information Engineering, University of Florence. He has authored or coauthored more than 190 scientific contributions in high-impact conferences and journals. His research interests include computer vision, pattern recognition, and multimedia.

Shaohua Wan (Senior Member, IEEE) received the Ph.D. degree in computer science and technology from the School of Computer, Wuhan University, Wuhan, China, in 2010.

He is currently a Full Professor with the Shenzhen Institute for Advanced Study, University of Electronic Science and Technology of China, Shenzhen, China. From 2016 to 2017, he was a Visiting Professor with the Department of Electrical and Computer Engineering, Technical University of Munich, Germany. He has authored 150 peer-reviewed research papers and books, including more than 40 IEEE/ACM transactions papers, such as IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, *ACM Transactions on Internet Technology*, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, IEEE TRANSACTIONS ON MULTIMEDIA, IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS, *ACM Transactions on Multimedia Computing, Communications, and Applications*, IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTATIONAL INTELLIGENCE, and *Pattern Recognition*, and many top conference papers in the fields of edge intelligence. His research focuses on deep learning for Internet of Things.