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 concerns 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 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&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*— Cybersecurity for Healthcare System, Medical Image Encryption, DNA Computing, Context-aware DNA Permutation&Diffusion**

I. Introduction

With the involvement of cloud computing and Internet of Medical Things (IoMT), 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's reported in [1] 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 re-distribution, and identity theft arise even with encryption process, since healthcare data is substantially valuable estimated as over 1000 dollars per patient [2]. Aiming to guarantee the security of medical images in the transfer process, efficient and reliable image encryption system is required. Famous methods such as RSA, DES, AES and 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, DNA computing is adopted to encrypt medical images in the transfer process other than common methods like chaos [3], Elliptic Curve Cryptography [4] and etc [5], [6].

Following the idea of DNA computing for encryption, a content-aware DNA computing for medical image encryption is put forward in this paper, designed with 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

†indicated equally contribution. This work was supported by National Key R&D Program of China under Grant No. 2021YFB3900601, National Natural Science Foundation of China under Grant No. 62172438, the Fundamental Research Funds for the Central Universities under Grant B220202074. Corresponding author: Shaohua Wan.

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

Stefano Berretti is with Department of Information Engineering (DINFO), University of Florence, via S. Marta 3 - 50139, Florence, ITALY (stefano.berretti@unifi.it).

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

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 shares the characteristics of naturally and smoothly varying. How to link image content and encryption process for higher complexity becomes our focus in this paper. Inspired by these ideas, highlights of the proposed work are listed below.

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 minimal storage property to guarantee high-capacity ability with small cost.
2) We introduce Randomly DNA Encoding module to build random mappings between image pixels and computing, and content-aware permutation&diffusion module to construct an content related permutation sequence, where both modules greatly improve secure ability.
3) Inspired by neighboring characteristics of medical image pixels, content-aware DNA permutation&diffusion module reorganizes transmitting data structure by highly non-linear functions for higher difficulty in cracking, which originate from correlation relationship of pixels and patches in medical images.

II. Related Work

Cybersecurity for Healthcare System Facing serious crime in cybersecurity, it's crucial to develop technologies for protection of patients' safety. To offer background knowledge, Bhuyan et al. [1] systematically examines cybersecurity threats in healthcare, and classifies cyberattacks to different types. They lay a firm foundation for healthcare organizations and policymakers in better understanding cybersecurity.

Focusing on a special category of cyber threats to healthcare system, researchers have proposed quantity of solutions. For example, To place real-time, affordable and consistent CPS in healthcare applications, Rajhans et al. [7] deploy 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 organisation, Sing et al. [8] present recommendations aiding healthcare professionals, which successfully identify phishing email attacks in practise. Considering the purpose of reducing the load of terminal equipment, Wang et al. [9] introduced 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] argue that the majority of data breaches lies with employee negligence and/or carelessness on information security. They thus build cybersecurity risk method to model employee behaviour surrounding information security, where they introduce Information Security Climate Index (ISCI) as a parsimonious tool to represent an extensive validation effort. Using cognitive computing, Ogiela et al. [11] propose a Linguistic Biometric Threshold scheme for data sharing, where biometric stage is designed to allocate the 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] propose a secure intrusion detection with blockchain based data transmission and artificial intelligence based classification model for Cyber-physical system in healthcare sector, which involve blockchain and AI for better security in healthcare. Last but not least, Nifakos et al. [15] offer a systematic review, which firstly identifies commonly encountered solutions that mitigate cyber defence strategy, and then reviews organisational 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] introduces biometric template with wearable assisted keystroke dynamic privacy-aware continuous authentication protocol to capture the user's behavioral features to continuously monitors user behaviors to adjust their access based on the activity they have performed. Soni et al. [17] propose 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 suddeness, 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 has relatively low tolerance to risk, so it should be considered more from the perspective of data security. [18] presents a risk-based distributed framework, which allow the users to determine the computation load to be offloaded at each MEC server under risk. It properly captures users' behavior under losses and gains, and strike a balance between safety and efficiency.

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 data arrangement. For example, Shankar et al. [19] propose a new RGB based share creation model using elliptic curve cryptography (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, Aashiq et al. [20] propose a secure data hiding in fused medical image for smart healthcare, where they first create a fused medical image as a cover by nonsubsampled contourlet transform (NSCT), then the method could be applied to conceal the image and electronic patient records (EPR) mark into the fused image. They claim their methods has achieved a balanced compromise with the privacy and security of medical images.

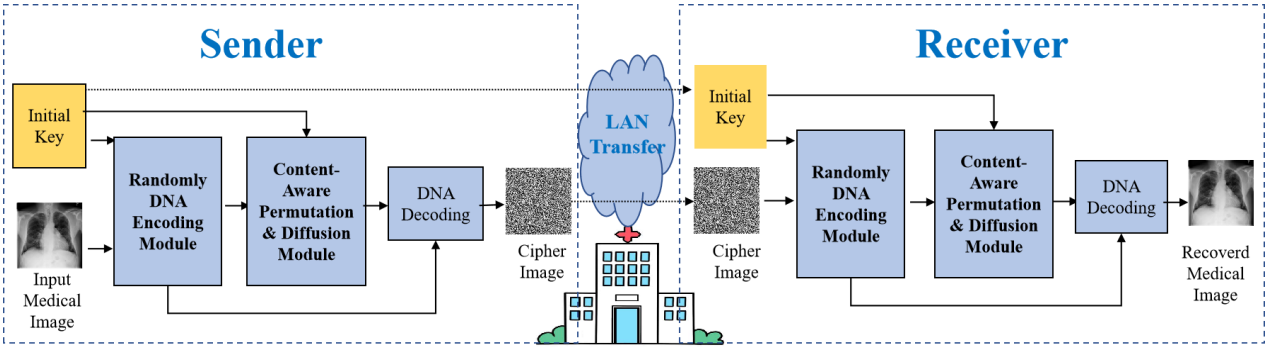

Fig. 1. The general workflow of a sender, LAN transfer and a receiver in healthcare organization, where sender and receiver correspond to the encryption process and decryption process, respectively.

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.

Recently, Li et al. [21] propose a novel chaos based image encryption scheme by using randomly DNA encode and plaintext related permutation, where they randomly encode plain image into a nucleotide sequence with piecewise linear chaotic map (PWLCM). Most relevant to our work, Chen et al. [22] propose a secure and efficient image encryption method, where self-adaptive permutation-diffusion model utilize the reusability of the random variables to promote efficiency of the cryptosystem. Later, Zhang et al. [23] 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 depicted 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's 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&Diffusion Module. We then goes into two modules for algorithm explanation.

TABLE I
DNA Encoding Rules

DNA Base	A	C	G	T
Rule1	00	01	01	11
Rule2	00	10	10	11
Rule3	01	11	00	10
Rule4	01	00	11	10
Rule5	10	11	00	01
Rule6	10	00	11	01
Rule7	11	01	01	00
Rule8	11	10	10	00

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 4 kinds of DNA bases, named adenine (A), guanine (G), cytosine (C) and thymine (T). Aadenine and thymine are a complementary pair, while cytosine and guanine are a complementary pair. In this case, there are totally 8 kinds of encoding rules, shown in the 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 , 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 Piece Wise

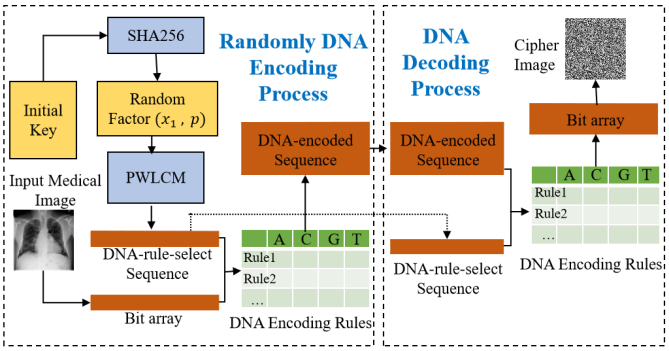

Fig. 2. The workflow of the Randomly DNA-Encoding Process and DNA Decoding Process inside encryption.

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

Change the plain image I into bit array I_{bit};
len $\leftarrow$ Length(I_bit);
$HASH_K \leftarrow$ SHA256(K) ;
$H_1, H_2 \leftarrow HASH_K$;
$x_1 = mod\left(H_1/10^{15}, 1\right)$,$p = mod\left(H_2/10^{15}, 1\right)$;
Put x_1, p into PWLCM to generate a sequence $X = [x_1, x_2, ..., x_n]$ by iterating ;
$S_{rule} = mod\left(floor\left(\boldsymbol{X} \times 10^{15}\right), 8\right)$;
Introduce the DNA Encoding Table T ;
For(i = 0 **to** $2 \times len$);
    $S_1(i) \leftarrow T(S_{rule}(i), I_{bit}(2i, 2i+1))$;

Linear Chaotic Map(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 8 different DNA encoding rules. The PWLCM is defined as:

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

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

B. Content-Aware Permutation&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

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) ;
$len \leftarrow$ Length(S_1);
$AR \leftarrow S_1(0); XR \leftarrow S_1(0)$;
For(i = 1 **to** len);
    $AR \leftarrow TA(AR, S_1(i))$;
    $XR \leftarrow TX(XR, S_1(i))$;
$HASH_D \leftarrow$ SHA256$([AR, XR])$;
$HASH_K \leftarrow$ SHA256(K) ;
$HASH_{DK} \leftarrow HASH_D \oplus HASH_K$;
$A_1, A_2, A_3, A_4 \leftarrow HASH_{DK}$;
$x_1 \leftarrow \left(\text{mod}\left(\text{fix}\left(A_1/10^8\right), 80\right) - 40\right) + \left(A_1/10^{14} - fix\left(A_1/10^{14}\right)\right)$;
$y_1 \leftarrow \left(\text{mod}\left(\text{fix}\left(A_2/10^8\right), 80\right) - 40\right) + \left(A_2/10^{14} - fix\left(A_2/10^{14}\right)\right)$;
$z_1 \leftarrow \left(\text{mod}\left(\text{fix}\left(A_3/10^8\right), 80\right) + 1\right) + \left(A_3/10^{14} - fix\left(A_3/10^{14}\right)\right)$;
$w_1 \leftarrow \left(\text{mod}\left(\text{fix}\left(A_4/10^8\right), 500\right) - 250\right) + \left(A_4/10^{14} - fix\left(A_4/10^{14}\right)\right)$;
For($i = 0$ **to** $length(S_1)$);
    $x_{i+1}, y_{i+1}, zi + 1, w_{i+1}$ = $HCLS(x_i, y_i, zi, w_i)$;
X=$[x_1, x_2, ...]$;
$S_p = mod\left(floor\left(\boldsymbol{X} \times 10^{15}\right), len\right)$;
If(This is encryption process);
    $m = 0, n = len/2$;
Else;
    $m = len/2, n = 0$;
For($k = m$ **to** n);
    $S_1(S_p(k)) \leftrightarrow S_1(S_p(len - k))$;
$S_1^p \leftarrow S_1$

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 two methods mentioned above.

The Content-Aware Permutation and Diffusion Module, shown in the Fig. 3, contains reversible plaintext related permutation algorithm and diffusion algorithm that the information of plain image can directly calculated in the decryption part without transmitting from the encryption part. This two algorithm take advantage of three types of DNA Operations: ADD, SUB and 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 above ADD and XOR operations satisfy the commutative law, which means the result of these operations is exactly the same for the DNA sequence

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 $\leftarrow$ Length(S_p);
$HASH_K \leftarrow$ SHA256(K) ;
$H_1 \leftarrow HASH_K(128:191)$;
$H_2 \leftarrow HASH_K(192:255)$;
$x_1 = mod\left(H_1/10^{15}, 1\right)$;
$p = mod\left(H_2/10^{15}, 1\right)$;
Put x_1, p into PWLCM to generate a sequence $X = [x_1, x_2, ..., x_n]$ by iterating ;
$Y = mod\left(floor\left(\boldsymbol{X} \times 10^{15}\right), 256\right)$;
Introduce the DNA Encoding Table T ;
For(i = 0 **to** $2 \times len$);
    $S_{key}(i) \leftarrow T(S_{rule}(i), Y(2i, 2i+1))$;
Introduce the DNA ADD Table TA ; Introduce the DNA SUB Table TS ; Introduce the DNA XOR Table TX ;
If(encrypting)
    $D(0) \leftarrow TA(S_p(0), S_{key}(0))$;
$D(0) \leftarrow TX(D(0), S_{key}(0))$;
    For $i = 1$ **to** $len - 1$;
        If $\mathrm{mod}(i, 2) = 1$ then ;
            $D(i) \leftarrow TX(S_p(i), S_{key}(i))$;
$D(i) \leftarrow TX(D(i), D(i-1))$;
        Else ;
            $D(i) \leftarrow TA(S_p(i), S_{key}(i))$;
$D(i) \leftarrow TX(D(i), D(i-1))$;
Else ;
    For $i = len - 1$ **to** 1 ;
        If $\mathrm{mod}(i, 2) = 1$ then ;
            $D(i) \leftarrow TX(S_p(i), S_{key}(i))$;
$D(i) \leftarrow TX(D(i), S_p(i-1))$;
        Else ;
            $D(i) \leftarrow TA(S_p(i), S_p(i))$;
$D(i) \leftarrow TX(D(i), S_{key}(i-1))$;
    $D(0) \leftarrow TA(S_p(0), S_{key}(0))$;
$D(0) \leftarrow TX(D(0), S_{key}(0))$;

before and after permutation. So the permutation procedures of encryption process and decryption process 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 shown in the pesudo code Algorithm.3. Then input this result into the Hyper Chaotic Lorenz System(HCLS) to generate a content-aware permutation control sequence S_p. The HCLS is given by:

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

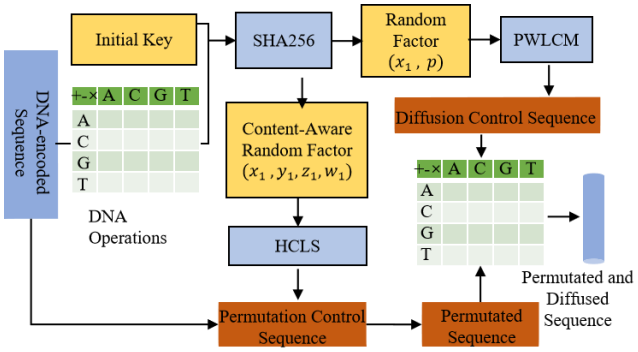

Fig. 3. Structure design of the proposed Content-Aware Permutation&Diffusion Module.

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

Then, we make the permutation control sequence the rule perform content aware permutation, and get a permutated sequence. After that, the permutated sequence is input into the DNA diffusion process. During this procedure the Initial Key K is utilized again to generate a diffusion control sequence. Finally, DNA operations is 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*1024*8 bit 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 has no specific size, but are also 8bit single channel gray images. Fcon_1000 contains a large number of nii format brain MRI images. In our experiment, they are converted into 8 bit gray images for processing.

B. Implement Details

The experiment is conducted on the proposed RC-DNA based on Python 3.8, with a HP personal laptop with Intel(R) Core(TM) i7-9750H CPU 2.60GHz, and 8G 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 $a = 10$, $b = \frac{8}{3}$, $c = 28$ and $\gamma = -0.5$. Moreover, to verify effectiveness and feasibility of proposed cryptosystem on the TCP/IP based IoT environment, we test it on the LAN with a router Tenda-AC7 1200M, and the image is transmitted via IP Messenger.

C. Key space Analysis

Keyspace is the set of all valid, possible, distinct keys of a given cryptosystem. Different cipher algorithms usually have

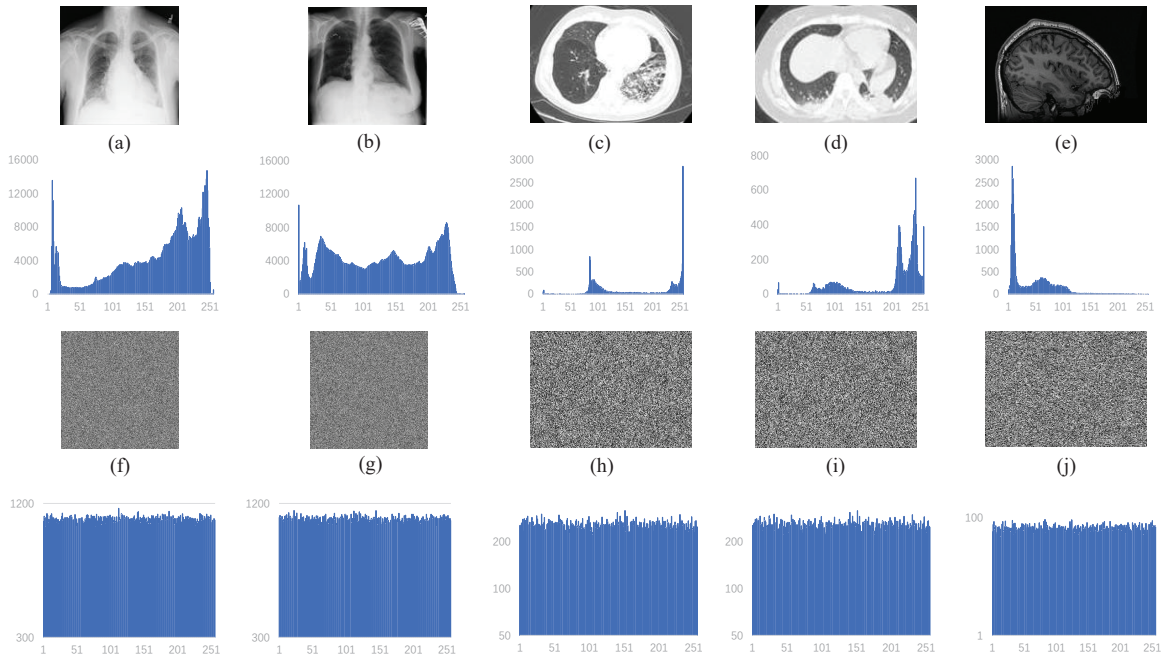

Fig. 4. The histograms of images before and after encryption. (a)(b) are images of representative chest X-ray images, (c)(d) are chest CT images form COVID-CT dataset, and (e) is a brain Magnetic Resonance Image from fcon1000 dataset. (f)-(j) are their corresponding cipher image. The graphs below are the histograms

different limit to the number of keys by their encryption rules. To resist a brute-force attack, the key space requires be large enouth, no less than 2^{100} . There are two circumstances for the key space: **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 4 initial values $x_1 \in (-40, 40)$, $y_1 \in (-40, 40)$, $z_1 \in (1, 81)$, $w_1 \in (-250, 250)$ of the HCLS system. Finally, the key space of RC-DNA can be calculated as $S = (0.5\times10^{15})^2\times(1\times10^{15})^2\times(80\times10^{14})^3\times(500\times10^{14}) = 6.410^{127} \approx 2^{418}$. **2.** if the attacker gets the cipher image and expects to use brute-force to get the initial key, the key space can be 2^{256} as the SHA256 algorithm has 2^{256} different outputs. These results shows that our key space 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 Equation (3).

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

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

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

The correlation coefficients of some images are 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 comparision 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 cryptosys-

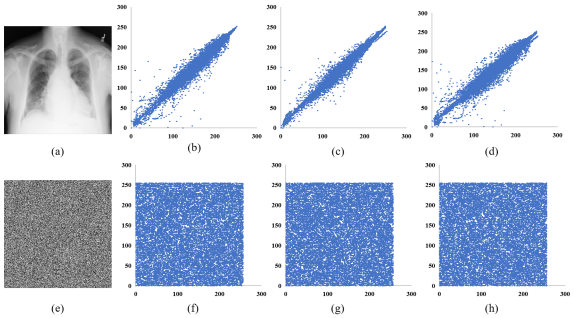

Fig. 5. Correlation coefficients distributions of chest X-ray image and its cipher image. In the graph, a point represents a pixel, and the value of its abscissa is its gray value. The ordinates of (b) and (f) are the gray value of right adjacent pixel, the ordinates of (c) and (g) are the gray value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

tem. 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-bit gray images, the equation of information entropy is given below.

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

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 shown in Table.III. For the ideal case of a K-bit image, the information entropy is $H = K$. The information entropy of the $8 - bit$ encrypted images by our proposed cryptosystem is close 8, indicating that it has good diffusion performance.

G. Sensitivity Analysis

Differential attack usually used 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 incex to evaluate the sensitivity: **1.**number of pixels change rate (NPCR) **2.**unified average changing intensity (UACI). They are given in the following equations.

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

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

The sensitivity of the proposed cryptosystem is estimated in two aspects: plain image sensitivity and key sensitivity. Firstly, we test the sensitivity of plain images. We conduct this experiment by changing a certain pixel value of a plain image. The Fig. 6 shows the effect of changing the value of the pixel (20,20) from 14 to 15 in the chest image. Moreover, we calculate the NPCR and UACI of the 5 images for 20 times, and the average results are shown 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.

TABLE IV
THE 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
THE 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

Secondly, 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 Section3.2. Then make changes: $x_1 = x_1 + 10^{-14}$, 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 result shown 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 PWLCM and HCLS, and the time complexity of both processes is $O(m\ timesn)$, proportional to the size of the image. Using the software and hardware mentioned in Section 4.1, encryption of a 256×256 image totally costs 2.12 seconds, and that of a 512×512 image costs 9.56 seconds. 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 3. The choice between the two modules can be divided into the following four cases and the result is presented in Table. VI:

- There is no randomly DNA encoding for plain image. Permutation and diffusion is performed directly at pixel level and not content related.

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
The proposed	0.0014	0.0009	0.0004	7.9992	99.6841	33.5539

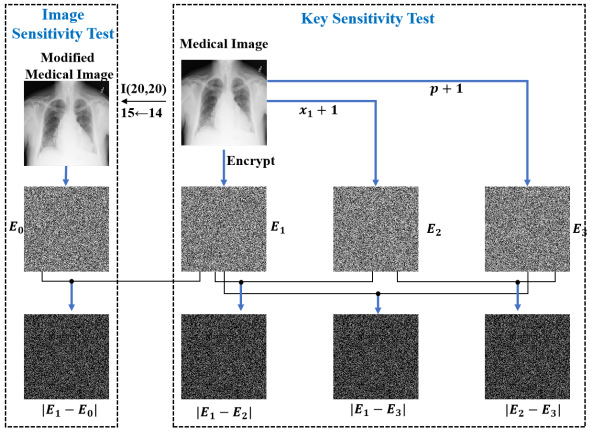

Fig. 6. The differential cipher image. Both image sensitivity and key sensitivity is shown in this figure.

- No randomly DNA encoding for plain images. Content-aware permutation and diffusion is performed directly at pixel level.
- There is a randomly DNA-Encoding process, but permutation and diffusion module is not content related.
- There is a randomly DNA-Encoding process, and content-aware permutation and diffusion is also performed.

It can conducted from Tab. 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 shown in Table.VII. Although our method is not optimal in some certain indicators, 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 8bit 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 a HP personal laptop with Intel(R) Core(TM) i7-9750H CPU 2.60GHz, and 8G 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 $a = 10$, $b = \frac{8}{3}$, $c = 28$ and $\gamma = -0.5$.

V. CONCLUSION

To ensure the security of cipher images, this paper proposes a novel cryptosystem for secure healthcare with two effective modules: Randomly-DNA Encoding Module and Content-Aware Permutation&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, U. Y. Kabir, J. M. Escareno, K. Ector, S. Palakodeti, D. K. Wyant, S. Kumar, M. Levy, S. Kedia, D. Dasgupta, and A. Dobalian, "Transforming healthcare cybersecurity from reactive to proactive: Current status and future recommendations," *J. Medical Syst.*, vol. 44, no. 5, p. 98, 2020.

[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," *Concurr. Comput. Pract. Exp.*, vol. 34, no. 4, 2022.

[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, p. 116193, 2022.
[6] Z. Gu, H. Li, S. Khan, L. Deng, X. Du, M. Guizani, and Z. Tian, "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, 2022.
[7] A. Rajhans, A. Bhave, I. Ruchkin, B. H. Krogh, D. Garlan, A. Platzer, and B. R. Schmerl, "Supporting heterogeneity in cyber-physical systems architectures," *IEEE Trans. Autom. Control.*, vol. 59, no. 12, pp. 3178–3193, 2014.
[8] H. Singh and D. F. Sittig, "A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks," *Appl. Clin. Inform.*, vol. 07, no. 02, 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 Distributed 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 Informatics J.*, vol. 26, no. 1, 2020.
[11] L. Ogiela and M. R. Ogiela, "Cognitive security paradigm for cloud computing applications," *Concurr. Comput. Pract. Exp.*, vol. 32, no. 8, 2020.
[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. Manag.*, vol. 59, no. 2, p. 102888, 2022.
[13] P. Radoglou-Grammatikis, K. Rompolos, P. Sarigiannidis, V. Argyriou, T. Lagkas, A. Sarigiannidis, S. Goudos, and S. Wan, "Modeling, detecting, and mitigating threats against industrial healthcare systems: a combined software defined networking and reinforcement learning approach," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 2041–2052, 2021.
[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 Distributed Comput.*, vol. 153, pp. 150–160, 2021.
[15] S. Nifakos, K. Chandramouli, C. K. Nikolaou, P. Papachristou, S. Koch, E. Panaousis, and S. Bonacina, "Influence of human factors on cyber security within healthcare organisations: A systematic review," *Sensors*, vol. 21, no. 15, p. 5119, 2021.
[16] A. Acar, S. Ali, K. Karabina, C. Kaygusuz, H. Aksu, K. Akkaya, and A. S. Uluagac, "A lightweight privacy-aware continuous authentication protocol-paca," *ACM Trans. Priv. Secur.*, vol. 24, no. 4, pp. 24:1–24:28, 2021.
[17] S. Preeti, P. Jitesh, P. A. Kumar, and I. S. Hafizul, "Cybersecurity attack-resilience authentication mechanism for intelligent healthcare system," *IEEE Transactions on Industrial Informatics*, 2022.
[18] P. A. Apostolopoulos, 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, 2020.
[19] K., Shankar, P., and Eswaran, "Rgb based multiple share creation in visual cryptography with aid of elliptic curve cryptography," *China Communications*, 2017.
[20] A. Anand and A. K. Singh, "Sdh: Secure data hiding in fused medical image for smart healthcare," *IEEE Transactions on Computational Social Systems*, pp. 1–9, 2021.
[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," *Applied Sciences*, vol. 10, no. 21, 2020.
[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," *Optics and Lasers in Engineering*, vol. 125, p. 105851, 2020.
[25] E. Z. Zefreh, "An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions," *Multim. Tools Appl.*, vol. 79, no. 33-34, pp. 24 993–25 022, 2020.
[26] K. Zhan, D. Wei, J. Shi, and J. Yu, "Cross-utilizing hyperchaotic and DNA sequences for image encryption," *J. Electronic Imaging*, vol. 26, no. 1, p. 13021, 2017.
[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," *Multim. Tools Appl.*, vol. 80, no. 7, pp. 10 949–10 983, 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 is currently an Associate Professor at Hohai University. Before coming to Hohai, he obtained his Ph.D. degree from Nanjing University in 2016. He received his B.S. Degree from Nanjing University in 2011 as well. His current research interests include computer vision and multimedia understanding.

Lilai Zhang received a B.E. degree in computer science and technology from Taiyuan University of Technology, Taiyuan, China, in 2021. He is currently working toward a M.E. degree in the College of Computer and Information, Hohai University. His current 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 the Media Integration and Communication Center and the Department of Information Engineering, University of Florence, Florence, Italy. 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 Ph.D. degree from School of Computer, Wuhan University in 2010. He is currently a full Professor with the Shenzhen Institute for Advanced Study, University of Electronic Science and Technology of China. From 2016 to 2017, he was a visiting professor at the Department of Electrical and Computer Engineering, Technical University of Munich, Germany. His main research interests include deep learning for Internet of Things. He is an author of over 150 peer-reviewed research papers and books, including over 40 IEEE/ACM Transactions papers such as TII, TITS, TOIT, TNSE, TMM, TCSS, TOMM, TETCI, PR, etc., and many top conference papers in the fields of edge intelligence.