Plausible Deniable Medical Image Encryption by Large Language Models and Reversible Content-Aware Strategy

Yirui Wu†, *Member, IEEE*, Xinfu Liu†, Lucia Cascone, *Member, IEEE*, Michele Nappi, *Senior Member, IEEE* and Shaohua Wan*, *Senior Member, IEEE*

***Abstract*— There is a rising concern about healthcare system security, where data loss could bring lots of damages to patients and hospitals. As a promising encryption method for medical images, DNA encoding own characteristics of high speed, parallelism computation, minimal storage, and unbreakable cryptosystems. Inspired by the idea of involving Large Language Models(LLMs) to improve DNA encoding, we propose a medical image encryption method with LLM-enhanced DNA encoding, which consists of LLM enhancing module and content-aware permutation&diffusion module. Regarding medical images generally have plain backgrounds with low-entropy pixels, the first module compresses pixels into highly compact signals with features of probabilistic varying and plausibly deniability, serving as another LLM-based layer of defence against privacy breaches before DNA encoding. The second module not only adds permutation by randomly sampling from a redundant correlation between adjacent pixels to break the internal links between pixels but also performs a DNA-based diffusion process to greatly increase the complexity of cracking. Experiments on ChestXray-14, COVID-CT and fcon-1000 datasets show that the proposed method outperforms all comparative methods in sensitivity, correlation and entropy.**

***Index Terms*— Medical Image Encryption, Large Language Models, Plausible Deniability, DNA Coding**

I. Introduction

HEALTHCARE systems are particularly vulnerable to cyber-attacks, due to their significant economic interests and weak defences. Unauthorized activities such as data loss, theft, modification, attack, and transfer without official authorization are defined as cyber-security breaches for medical data. Reported by [1], at least 150 million patients' personal information was illegally stolen from 94% of healthcare companies between 2009 and 2014.

As the most informative form of medical data, researchers have proposed several methods for encryption of medical images. To create the key sequence in a generative manner, Ding et al. [2] propose DeepKeyGen, which adopts GAN to generate the private key and designs a transformation domain to guide the generation process. Inspired by the Lorenz system, Singh et al. [3] propose EiMOL, where an optimized random sequence is generated through directed weighted complex network GDWCN-PSO, thus obtaining the cipher messages with Lorenz system. To promote secure healthcare, Wu et al. [4] propose a content-aware DNA computing system, which utilizes a random mechanism to increase the difficulty of cracking. Due to the promising properties of high speed, parallelism computation, and unbreakable cryptosystems, DNA encoding is now widely applied to encrypt medical images for safe and convincing data transfer.

Following the idea of utilizing DNA encoding for encryption, we propose an LLM-enhanced DNA encoding method to encrypt medical images, which has realized two purposes: First, probabilistic varying and plausible deniability introduced by LLM. Utilizing ImageGPT as LLM, it firstly compresses low-entropy medical images into compact and optimal-encoded signals, which would be lossless for image content and friendly for computation with further operations like DNA encoding and so on, ensuring fast and easy-implement performance. Afterward, ImageGPT serves as an explicit probabilistic model to first generate random masks for occlusion and then predict the occluded pixels to involve distribution obeyed variations, thus creating varying signals of input medical images for DNA-based encryption. In the later decryption process, ImageGPT will recover the occluded part to keep content consistent in the transmission. Therefore, ImageGPT acts as a 'black box' as well as another layer of defense to disavow the true meaning of the original image, thus acquiring the feature of plausible deniability.

Second, content-aware securing capability is introduced by operations of permutation and diffusion. Regarding high-dimensional images as a natural source bringing complexity, we design a content-aware algorithm to randomly sample from correlations of adjacent pixels, thus generating permuta-

† indicated equally contribution, * indicated the corresponding author. *(Yirui Wu and Xinfu Liu contributed equally to this work.) (Corresponding author: Shaohua Wan.)*

Yirui Wu, and Xinfu Liu were both with Key Laboratory of Water Big Data Technology of Ministry of Water Resources, Hohai University. They are also with the College of Computer Science and Software Engineering, Hohai University, Fochengxi Street, Nanjing 210096, China (e-mail: wuyirui@hhu.edu.cn, liuxinfu@hhu.edu.cn).

Lucia Cascone is a Ph.D. student in computer science at the University of Salerno, 84084 Fisciano, Italy (email: lcascone@unisa.it).

Michele Nappi is with Department of Computer Science, University of Salerno, Via Giovanni Paolo II, 132, Fisciano (SA), Italy (email: mnappi@unisa.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).

tion to increase the complexity of encrypted data. Following permutation, we design DNA-based diffusion operations to imitate biological diffusion, i.e., a passive transport process that moves bases across sequences to increase complexity. The contributions are three-fold:

- The proposed LLM enhancing module serves as another layer of defense before DNA encoding, realizing plausible deniability and probabilistic varying to disavow meaningful parts of input medical images.
- The proposed content-aware permutation&diffusion module involves the correlation between adjacent pixels and DNA-based diffusion operations to increase complexity in cracking greatly.
- Experiments demonstrate that the proposed method outperforms the comparative methods on popular benchmarks.

The rest of the paper is organized as follows. Section II reviews the related work. The framework overview, details of the proposed LLM enhancing module, and the content-aware permutation&diffusion module are discussed in Section III. Section IV presents the experimental results and discussions. Finally, Section V concludes the paper.

II. RELATED WORK

In this section, we divide related work into three parts, i.e., cyber-security in healthcare systems, statistic theory in encryption, and image encryption.

A. Cyber-security in Healthcare Systems

A rising demand exists to safeguard personal information from unauthorized access within the healthcare domain. Therefore, numerous researchers [5]–[7] have devoted extensive efforts to solve security issues in healthcare systems.

For example, Acar et al. [8] propose a lightweight Privacy-Aware Continuous Authentication protocol (PACA), which authenticates users with their biometrics in a privacy-aware manner, thus significantly enhancing defense capabilities. Later, Grammatikis et al. [9] assess the severity of the IEC 60870-5-104 protocol and propose Intrusion Detection and Prevention System (IDPS) to automatically mitigate it, which transforms the automated mitigation into a multiarmed bandit problem, thus increasing the accuracy of intrusion detection in healthcare systems. To ensure adequate medical services in remote areas, Soni et al. [10] propose an intelligent user recognition mechanism, which ascertains the possibility of risky behaviors for idle users, thus offering enhanced security over authentication systems.

With the implementation of the cloud to construct healthcare systems, significant risks in data transmission have been raised as a focus topic by several researchers [4], [6], [11]. For example, Xu et al. [11] propose a security performance intelligent prediction algorithm, including an improved convolutional neural network with four convolution layers and four inception block, which analyzes the security of IoT-enabled healthcare networks in real-time. Later, Ji et al. [12] propose an Intelligent Reflective Surface (IRS)-driven healthcare system, which transmits independent medical data streams to doctors with a Multiple-Input Single-Output (MISO) setting, thus keeping medical data secret from patient spies. Simultaneously, Wu et al. [4] propose a novel content-aware DNA computing system, which transmits cipher medical images from sender to receiver with a randomly DNA encoding and a content-aware permutation&diffusion module, thus guaranteeing privacy and promoting secure healthcare environment.

Unlike the above approaches, we propose a plausibly deniable medical image encryption method, which utilizes an LLM-enhancing module to generate plausible medical images and a content-aware permutation&diffusion module to increase the complexity of cracking, thus safeguarding the healthcare system.

B. Statistic Theory in Encryption

Statistical theory [13] is a fundamental support for encryption algorithms. Many researchers [14]–[16] utilize classical statistical models to encryption scheme. For example, Liang et al. [15] propose the first and concrete deterministic finite automata-based functional PRE (DFA-based FPRE) system, which generates a new ciphertext by a semi-trusted proxy with a probability distribution, thus increasing the flexibility of delegating users' decryption rights. However, the probability distribution turns messy when meeting too many new nodes. To make probability distribution regular, Kwon et al. [13] propose an additive statistical method for data leakage analysis, employing an Exponential Mixture Model (EMM) to predict the leakage distribution only by a few leakage data, thus estimating any shape of leakage distribution regardless of new nodes or operating conditions.

Different from the classical statistical models, the neural network-based statistical methods [17]–[19] obtain convincing results by training on abundant of parameters. For example, Kato et al. [17] propose a new encryption method with Recurrent Neural Networks (RNNs), which predicts the F0 value from a spectrum and predicts a target sinusoidal waveform from the raw speech waveform, thus improving the estimating of noise-robust fundamental frequency signals. To characterize the soft error-induced data disturbance on each neuron, Huang et al. [18] utilize central limit theorem to develop a series of statistical models, which tackles soft errors and accelerates fault simulations of neural networks. To improve efficiency while ensuring security, Cai et al. [19] propose a Secure and efficient Federated learning scheme (SecFed) based on multi-key, which preserves user privacy and delegates some operations with an offline protection mechanism, thus ensuring the operations of disconnected participants.

Notably, numerous scholars [20]–[22] validate that LLMs equips with internal statistical characteristics, and which can be further applied to a range of downstream tasks. Inspired by auto-regressive transformers, Yu et al. [23] extend the statistical capabilities of existing models, developing a multi-scale decoder architecture to handle sequences with millions of bytes. This makes an ideal choice for compressing text, images, and other data along with their associated distributions. To assess the statistical and causal reasoning ability of LLMs, Liu et al. [24] introduce the Quantitative Reasoning

with Data (QRData) benchmark, which carefully constructs a dataset with 411 main questions and 290 auxiliary questions, thus acquiring accurate results of various LLMs. Inspired by the internal statistical characteristics of LLMs, we propose an LLM-enhanced DNA encoding method, which utilizes LLMs to decrypt medical images with the given keys. With the specific design for generating plausible images, we add another defense layer for medical image encryption.

C. Image Encryption

Image encryption aims to protect the inner information from unauthorized acquisition. Compared with text encryption, the difficulty of image encryption tasks is much greater [25]. We roughly divide image encryption into traditional methods [26]–[29] and deep learning-based methods [30]–[32].

For traditional image encryption methods, researchers utilize various mathematical models to realize encryption algorithms. For example, Zhang et al. [33] propose a 2D Lag-Complex Logistic Map (LCLM), which extends variables from real numbers in the conventional 2D logistic map to complex field, performing well in chaotic intervals, good ergodicity, and unpredictable trajectories. Later, Huang et al. [34] propose a real-time encryption system for Distribution Energy Systems (DESs). By constructing a 13-D chaotic system and simple encryption algorithm, they ensure the system's consistent running and resist malicious attacks in DESs. Some researchers found that although many methods show good encryption performance, they were often tested under ideal conditions. When confronted with more realistic scenarios, these methods frequently proved to be inefficient. Based on this observation, Zhang et al. [29] conduct more rigorous testing on certain DNA encryption algorithms, obtaining more credible evaluation results.

Unlike traditional methods, researchers utilize deep learning-based methods to encrypt images by training multiple-layer networks. For example, Ding et al. [30] propose a Deep learning-based image Encryption and Decryption Network (DeepEDN), which integrates the image encryption and decryption algorithms into deep neural networks, facilitating the development of deep medical image encryption. To increase the compression efficiency of color images, Wang et al. [35] propose the Encryption-Then-Lossy-Compression (ETLC) scheme, which utilizes a nonuniform down-sampling strategy and a customized deep network to integrate uniform and random sampling, thus achieving an arbitrary compression ratio. Furthermore, Gao et al. [36] propose a specially designed BP neural network to encrypt various types of images, boasting greater robustness and efficiency. Considering the high dimension of medical images, we put the encryption process into the LLM-enhanced DNA encoding and decoding phase, fulfilling the operation in an advanced compressed manner.

III. Methodology

In this section, we highlight the proposed medical image encryption method in detail. We divide this section into three parts, including framework overview, LLMs enhancing module, and content-aware permutation&diffusion module.

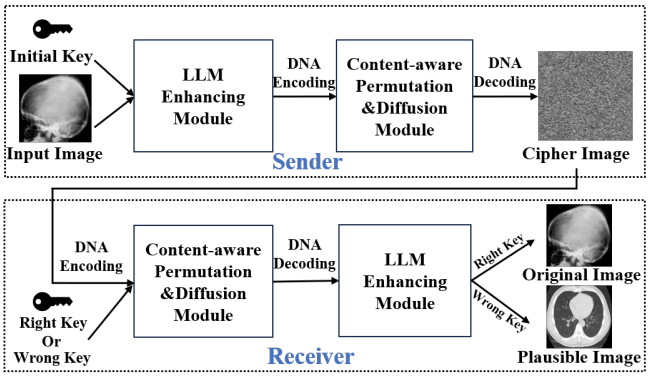

Fig. 1. The proposed framework includes the sender and receiver, which are opposite in operations.

A. Framework Overview

Fig. 1 illustrates the proposed framework, which consists of ImageGPT as an LLM enhancing module, content-aware permutation&diffusion module, and DNA encoding&decoding process. Specifically, we express encryption and decryption processes as Eq. 1 and 2, respectively. Inside the sender, we define the input image and initial key as I and K, where they are fed into the LLM enhancing module to generate masked sequence S_M and key sequence S_K, owing features of plausible deniability and probabilistic pixel varying. Then, S_M and S_K are transformed as $S_M^{'}$, $S_K^{'}$ with DNA coding, and fed into the content-aware permutation&diffusion module, resulting in a permutated and diffused sequence S_N. Finally, S_N and S_I are further processed by the DNA decoding process, generating the cipher image C for transmission.

$$\begin{cases} (S_M, S_K) = ImageGPT(I, K) \\ (S_M^{'}, S_K^{'}) = DNA_{en}(S_M, S_K) \\ S_N = PD(S_M^{'}, S_K^{'}) \\ C = DNA_{de}(S_N, S_M) \end{cases} \tag{1}$$

where $ImageGPT()$, $PD()$, $DNA_{en}()$, $DNA_{de}()$ represent operations of LLM-based enhancing module, content-aware permutation&diffusion module, DNA encoding and decoding, respectively.

The receiver first feeds C and S_K into the DNA encoding process, which generates sequences S_P and S_Q. Then, we input S_P and S_Q into the content-aware confusion&diffusion module, which recoveries the masked sequence S_R. Then, S_R are transformed as $S_R^{'}$ with S_P during DNA decoding process. Finally, S_K and $S_R^{'}$ are put into the LLM enhancing module, which randomly samples $S_R^{'}$ to recover the image I_R. It's noted that I_R created by ImageGPT with a wrong key would make attackers believe they achieved the right image, thus being equipped with the feature of plausible deniability.

$$\begin{cases} (S_P, S_Q) = DNA_{en}^{'}(C, S_K) \\ S_R = PD^{'}(S_P, S_Q) \\ (S_R^{'}) = DNA_{de}^{'}(S_P, S_R) \\ I_R = ImageGPT^{'}(S_K, S_R^{'}) \end{cases} \tag{2}$$

where $DNA_{en}^{'}()$, $DNA_{de}^{'}()$, $PD^{'}()$, $ImageGPT^{'}()$ represent opposite operations of that in Eq. 1.

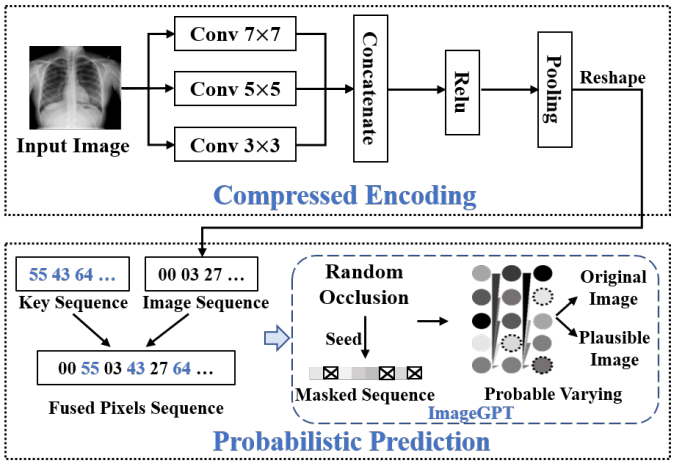

Fig. 2. The compressed encoding and probabilistic prediction process of LLM enhancing module.

Algorithm 1: The LLM Enhancing Module in Sender

Input: Image I, Key K
Output: Masked Sequence S_M, Key Sequence S_K

$C_I \leftarrow C_7(I) \oplus C_5(I) \oplus C_3(I)$
$\hat{S_I} \leftarrow \frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}(Relu(C_I))_{ij}$
$S_I \leftarrow Reshap(\hat{S_I})$; $S_K \leftarrow Reshap(K)$
$S_F \leftarrow (S_I + S_K)\%256$
$Seed \leftarrow Rand(100, 200)$
$S_M \leftarrow ImageGPT(S_F, Seed)$
return S_M, S_K;

Algorithm 2: The LLM Enhancing Module in Receiver

Input: Key Sequence S_K (which consists of right key sequence Kr **or** wrong key sequence Kw), Masked Sequence $S_R^{'}$
Output: Recovered Image I_R (which consists of original image I_{Ori} **or** plausible image I_{Pla})

if Kr **then**
  $I_{Ori} \leftarrow ImageGPT^{'}(Kr, S_R^{'})$
else
  $I_{Pla} \leftarrow ImageGPT^{'}(Kw, S_R^{'})$
end
$I_R \leftarrow (I_{Ori}$ **or** $I_{Pla})$
return I_R;

B. LLM Enhancing Module

To realize plausible deniability and probabilistic varying, we propose an LLM enhancing module, where we illustrate its process in Fig. 2, Algorithm 1, Algorithm 2 with steps of compressed encoding and probabilistic prediction. Notably, $Relu()$ means the relu activation function, and $Reshap()$ transfers a $N \times N$ pixels sequence to a $1 \times N^2$ form.

Compressed Encoding. Assuming attackers are familiar with image encryption algorithms, one important question arises: what if the attack could reveal all possible keys to crack? One solution is to additionally encode the cipher image, which could be decoded to a valid plausible image using any key. Differing from traditional algorithms [37] using statistical functions as additional encoding, we introduce pre-trained LLM as a powerful and dynamic model to realize plausible deniability. Regarding the LLM enhancing module as a compressor, we achieve optimal entropy form of encoding even if the pixel values of the input image are not dyadic [22], being difficult in optimally encoding with traditional algorithms. Based on optimal encoding, further by-product formulations such as DNA encoding could be lossless for image content and friendly for computation, ensuring fast and easy-implement performance as a defencing layer.

Regarding pixel values of the input image as sequences, an optimal variable-length code book could encode images with their occurring probabilities, thus achieving an optimal compression rate with low entropy for further processes. Since the computation cost will increase exponentially, we must take measures to reduce the context length of transformer architecture under dense attention conditions. The GPU devices could not afford such a vast computation cost when calculating a medical image with 255×255 pixels and larger, where a single layer would take tens of thousands of times to create the attention logits. To tackle this issue, we transfer the input gray-scale medical image to low-resolution sequences with 32×32, 48×48, or 64×64 pixels. However, the image size is still hard to calculate even with 32×32 pixels for a dense attention mechanism. Inspired by early color display palettes [38], we design a special palette for grayscale medical images, which differs from the previous RGB palettes by clustering pixel values using k-means with $k = 128$. We created 3 times smaller than the original image yet still kept the most details.

Specifically, we discuss the details of compressed encoding in Algorithm 1. Since most of the medical images have sparse backgrounds, it was essential to compress the extra background pixels for saving storage. We first fed the Image I and Key K into the proposed LLM enhancing module, then I will be convolved by several 7×7, 5×5, and 3×3 kernels to compress pixels. Subsequently, the pixels will be concatenated and transferred with relu activation functions, which were adapted by pooling operation to further create a low-dimensional image. To increase the random possibility of encryption, we transfer the pixel to a one-dimensional sequence to match the key sequence, both of which were fused to create a new sequence. Finally, we set seeds by random generated a number between 100 to 200, which are utilized with ImageGPT to mask the fused sequence randomly. Benefiting from the powerful auto-regressive ability of the sequence Transformer, the ImageGPT could predict pixels with high accuracy, which provides safeguards against random occlusion.

Probabilistic Prediction. Being a probability model that has an observed quantity of images, LLM could generate plausible medical images if attackers use the wrong keys. On the contrary, traditional algorithms tend to return vision-valid images that are too unrelated to the context. Guided by the probability distribution from ImageGPT, the context-

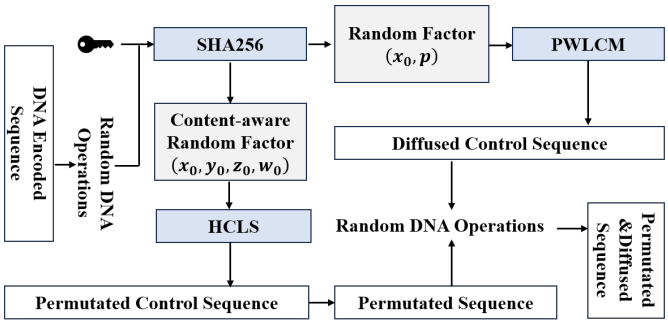

Fig. 3. The design of content-aware permutation&diffusion module. Given DNA encoded sequence, the module utilizes several algorithms to permute and diffuse sequence.

setting mechanism inside LLM towards producing responses that align with expected responses, makes it powerful and effective to resist the attack of revealing all keys.

We discuss the details of probabilistic prediction in Algorithm 2. To improve the security of medical image encryption, we sample probable varying and recover masked pixels in a random manner, which benefits from the complete inner probability distribution of ImageGPT. For each pixel fed through the ImageGPT, the model explicitly predicts the probability distribution of the next pixels conditioned on all previous pixels. Generating pixels involves sampling from this probability distribution and repeating the process in a feedback fashion. From a more technical perspective, sampling is implemented using the inverse transform sampling algorithm, which involves (i) computing the cumulative distribution function of the probability distribution, (ii) sampling a random number n from $U[1, N^2]$, and (iii) finding the bin in which n falls through binary search. When it is carried out deterministically using a stream of numbers n (which appear as random, but may or may not be the result of a random process) provided externally.

Specifically, we utilize the remaining $N^2 - n$ original pixels to predict the n masked pixels one after another. Benefiting from the powerful prediction ability of ImageGPT, we can recover original pixels from n masked pixels more accurately. Afterward, we get the recovered sequences I_{Ori} or I_{Pla} from predicted pixels with Kr or Kw, respectively. Notably, we will get the original image with the most probability from Kr. In contrast, we will get a random but plausible image from ImageGPT with Kw, which was selected from the training datasets according to the probability distribution. Formally, considering a sequence of $N^2 - n$ pixels denoted as $p_1, ..., p_i, ..., p_{N^2-n}$. Our objective involves predicting and generating the next n pixels to complete the sequence totaling N^2 pixels. The module fills in the masked pixels in a left-to-right sequence through a pixel probability distribution.

C. Content-aware Permutation&Diffusion Module

To increase the complexity of cracking, we propose a content-aware permutation&diffusion module, where we illustrate its structure in Fig. 3 with major steps of content-aware permutation and DNA-based diffusion.

Algorithm 3: The Process of Permutation

Input: Right Key Kr **or** Wrong Key Kw, Sequence $S_M^{'}$, $S_K^{'}$ **or** S_P, S_Q Encoded by DNA Principal
Output: Permutation Result S_{N1} **or** S_{R1}

$length \leftarrow Length(S_M^{'})$
$AR \leftarrow S_M^{'}(0); XR \leftarrow S_M^{'}(0)$
for $i \leftarrow 0$ ***to*** $length - 1$ **do**
  $AR \leftarrow Ta(AR_i, S_M^{'}(i))$
  $XR \leftarrow Tx(XR_i, S_M^{'}(i))$
end
$hash_D \leftarrow SHA256(AR, XR)$
$hash_K \leftarrow SHA256(Kr, Kw)$
$hash_{DK} \leftarrow hash_D \oplus hash_K$
$A_1 \leftarrow hash_{DK}(0:63)$
$A_2 \leftarrow hash_{DK}(64:127)$
$A_3 \leftarrow hash_{DK}(128:191)$
$A_4 \leftarrow hash_{DK}(192:255)$
$x_1 \leftarrow (mod(fix(A_1/10^8), 80) - 40) + (A_1/10^{14} - fix(A_1/10^{14}))$
$y_1 \leftarrow (mod(fix(A_2/10^8), 80) - 40) + (A_2/10^{14} - fix(A_2/10^{14}))$
$z_1 \leftarrow (mod(fix(A_3/10^8), 80) + 1) + (A_3/10^{14} - fix(A_3/10^{14}))$
$w_1 \leftarrow (mod(fix(A_4/10^8), 500) - 250) + (A_4/10^{14} - fix(A_4/10^{14}))$
$[x_0, x_1, x_2, ..., x_n] \leftarrow HCLS(x_0, y_0, z_0, w_0)$
$S_p \leftarrow mod(floor(\boldsymbol{X} \times 10^{15}), length - 1)$
if *encryption* **then**
  $i \leftarrow 1, j \leftarrow length/2 + 1$
else
  $i \leftarrow length/2 + 1, j \leftarrow 1$
end
for $k \leftarrow i$ ***to*** j **do**
  $S_M^{'}(S_p(k)) \leftrightarrow S_M^{'}(S_p(length - k))$
end
$S_{N1} \leftarrow S_M^{'}$ **or** $S_{R1} \leftarrow S_M^{'}$
return S_{N1} ***or*** S_{R1}

Previous methods [39] acquire data only from the key sequence, which lacks sensitivity due to the limited diversity, thus transferring hash values from the original image to the cipher image to ensure the security of medical healthcare. Since high-dimensional images contain ample redundant pixels, we propose a content-aware algorithm for random sampling from high-dimensional images, which offers enough diverse forms to increase the complexity of encrypted images. In addition, we put the permutation and diffusion operations under DNA coding conditions, which both utilize the reversibility of permutation operation and the commutative law of DNA operation, without adding any extra data.

Specifically, the sequence will be encoded following the DNA principal and be directly calculated with DNA operations. In this paper, the DAN operations include ADD, SUB, and XOR, which calculate permutation operations with the same algorithm and parameters, eliminating additional compu-

Algorithm 4: The Process of Diffusion

Input: Right Key Kr **or** Wrong Key Kw, Sequence $S_M^{'}$, $S_K^{'}$ **or** S_P, S_Q Encoded by DNA Principal
Output: Diffused Result S_{N2} **or** S_{R2}

Change $S_M^{'}$ into S_M^{bit} with Binary;
$length \leftarrow \text{Length}(S_M^{'})$;
$hash_K \leftarrow SHA256(S_K^{'})$;
$H_1 \leftarrow hash_K(128:191)$; $H_2 \leftarrow hash_K(192:255)$;
$x_0 \leftarrow mod(fix(H_1/10^{15}))$;
$p \leftarrow mod(fix(H_2/10^{15}))$;
for $t \leftarrow 0$ ***to*** $length/2$ **do**
  $x_{t+1} \leftarrow PWLCM(x_t, p)$;
end
$X \leftarrow [x_0, x_1, ..., x_{length/2}]$;
$Y \leftarrow mod(floor(\boldsymbol{X} \times 10^{15}), 256)$;
for $i \leftarrow 1$ ***to*** $length/2+1$ **do**
  $S_{key}(i) \leftarrow DNA_{en}(S_M^{'}(i), Y(2i, 2i+1))$;
end
if *encryption* **then**
  for $i \leftarrow 0$ ***to*** $length$ **do**
    if $mod(i,2) == 1$ **then**
      $D(i) \leftarrow Tx(S_M^{'}(i), S_{key}(i))$;
      $D(i) \leftarrow Tx(D(i), D(i-1))$;
    else
      $D(i) \leftarrow Ta(S_M^{'}(i), S_{key}(i))$;
      $D(i) \leftarrow Tx(D(i), D(i-1))$;
    end
  end
else
  for $i \leftarrow length$ ***to*** 0 **do**
    if $mod(i,2) == 1$ **then**
      $D(i) \leftarrow Tx(S_M^{'}(i), S_{key}(i))$;
      $D(i) \leftarrow Tx(D(i), S_M^{'}(i-1))$;
    else
      $D(i) \leftarrow Ta(S_M^{'}(i), S_M^{'}(i))$;
      $D(i) \leftarrow Tx(D(i), S_{key}(i-1))$;
    end
  end
end
$S_{N2} \leftarrow D(0:length-1)$ **or** $S_{R2} \leftarrow D(0:length-1)$;
return S_{N2} ***or*** S_{R2}

tation costs. Given a key (right or wrong), the proposed method employs the SHA256 algorithm to generate a random factor (x_0, p) and a content-aware random factor (x_0, y_0, z_0, w_0). From one aspect, we utilize (x_0, y_0, z_0, w_0) and the HCLS algorithm to produce a permutated control sequence, which provides chaotic parameters and environment. The HCLS algorithm is defined as Eq. 3:

$$\begin{cases} \dot{x} = a(y-x) + w \\ \dot{y} = bx - y - xz \\ \dot{z} = xy - cz \\ \dot{w} = -dw + yz \end{cases} \tag{3}$$

where a, b, c, and d are parameters. The system will be chaotic when satisfy $a = 10$, $b = 8/3$, $c = 28$, and $y \in [-1.52, -0.06]$. Subsequently, we produce the permutated sequence with chaotic parameters and environment. We show the details of permutation in Algorithm 3, where Ta means DNA ADD table, Ts means DNA SUB table, and Tx means DNA XOR table. Notably, we solely show the transmission process of $S_M^{'}$, other sequences perform the same process.

From another aspect, we first apply the PWLCM algorithm to generate a pseudo-random DNA-rule-select sequence, which generates a huge variation sequence with light adaption, thus improving the key sensitivity. The PWLCM algorithm can be written as Eq. 4:

$$x_{t+1} = \begin{cases} \frac{x_t}{\mu}, & 0 \leq x_t < \mu \\ \frac{x_t - \mu}{0.5 - \mu}, & \mu < x_t \leq 0.5 \\ f(\frac{1-x_t}{\mu}), & 0.5 < x_t \leq 1 \end{cases} \tag{4}$$

where $\mu \in (0, 0.5]$ is a parameter. Then, we imitate the biological diffusion process, generating a diffused sequence with (x_0, p) and a DNA-rule-select sequence. The details of the diffusion process are elaborated in Algorithm 4, where Ts means DNA SUB operation table and Kr or Kw is used again to produce the diffused sequence. Finally, we calculate both diffused sequence and permutated sequence, creating the permutated and diffused sequence.

IV. Experiment

In this section, we design sufficient experimental sessions to verify the validity and rationality of the proposed method. This section contains eleven parts overall, including the description of the dataset, implementation details, cryptography keyspace, histogram analysis, pixel correlation analysis, information entropy analysis, sensitivity analysis, computation cost analysis, ablation study, comparison with other methods, and visualization.

A. Dataset

We employ ChestXray-14 [40], COVID-CT [41], and fcon-1000 [4] to validate the performance of the proposed method. The ChestXray-14 dataset is a substantial medical dataset including 112,120 X-ray images, each image has a dimension of 1024×1024 pixels and 8-bit depth. This dataset was collected from 30,805 distinct patients with specific medical conditions, including 14 disease classes mined by NLP from relevant radiology reports. The dataset contains 14 categories of common chest pathology, including lung atelectasis, solidification, infiltrates, pneumothorax, edema, emphysema, fibrous degeneration, effusion, pneumonia, pleural thickening, cardiac hypertrophy, nodules, masses, and hernias.

The COVID-CT dataset has a total of 746 lung CT images, including 349 neocoronavirus-infected images and 397 non-neocoronavirus-infected images. For each new coronavirus-infected CT image, the dataset provides a related description of the patient's basic information (e.g., location, age, infected condition, brief medical history, onset time with other medical conditions). In particular, the original CT images in the dataset

were 3D, but only the slices were considered by the physician to select key features. Due to the clinical information is sufficient, this dataset does not significantly affect the diagnostic accuracy. The purpose of the COVID-CT dataset is to boost the development of algorithms for identifying new crown infections in lung CT (2D).

The fcon-1000 dataset was initiated by the 1000 Functional Connectomes Project (FCP), which is ushering in a new era of research on human brain function through the active sharing of magnetic resonance imaging data. These data were collected from more than a thousand subjects with 35 centers, and the primary modalities include structural Magnetic Resonance Imaging (sMRI) and resting-state Functional Magnetic Resonance Imaging (rs-fMRI). This dataset aims to investigate the associations between brain activity, behavior, cognitive functions, and psychiatric disorders. Each volunteer contributes multiple time points of fMRI scan data, encompassing various tasks and resting states, providing researchers with abundant material to explore the relationships between functional brain networks and behavioral performances.

B. Implement details

We utilize a computer with 13th Gen Intel(R) Core(TM) i5-13490F CPU 2.50GHz, one NVIDIA TITAN Xp GPU, 32G memory, and a Win10 operating system. The initial key is configured as a 2048 rows and 2 columns digital matrix. HCLS algorithm parameters are set to $d = 10$, $c = 8/3$, $e = 28$, and $r = -0.5$. To comprehensively validate the stability and security of network transmission, we constructed a realistic network environment with TCP/IP protocol for the proposed method. We establish a Local Area Network (LAN) for closed testing with the Tenda-AC7 router model, which has 1200M power.

C. Cryptography Keyspace

The keyspace refers to the set including all possible keys within a cryptographic system. The size of a keyspace is typically expressed in terms of bits, which determines the effort that potential attackers decrypt the cipher image with all possible keys. A larger keyspace implies greater difficulty for attackers to decrypt the cipher image. Due to the constraints imposed by the rules, different encryption algorithms correspond to different constraints on the keyspace. Since brute-force methods attempt every possible key to break the healthcare system, the available keyspace must reserve a sufficient number of alternatives. Ideally, this space should be larger than 2^{100}. In the proposed method, we particularly address the issue of keyspace and design a sufficiently large one. To enhance the diversity of keys, we add key $p \in (0, 0.5)$ during the key generation process. This extra key is used to increase the randomness of the generated keys. To match the additional key, we have also set an extra initial value $x_1 \in (0, 1)$ for the PWLCM system's initialization. Additionally, there are four initial values for HCLS: $x \in (-40, 40)$, $y \in (-40, 40)$, $z \in (1, 81)$ and $w \in (-250, 250)$. Therefore, the keyspace of our system is approximately: $S = (0.5\times10^{15})^2\times(1\times10^{15})^2\times(80\times10^{14})^3\times(500\times10^{14}) = 6.4\times10^{127} \approx 2^{418}$. Furthermore,

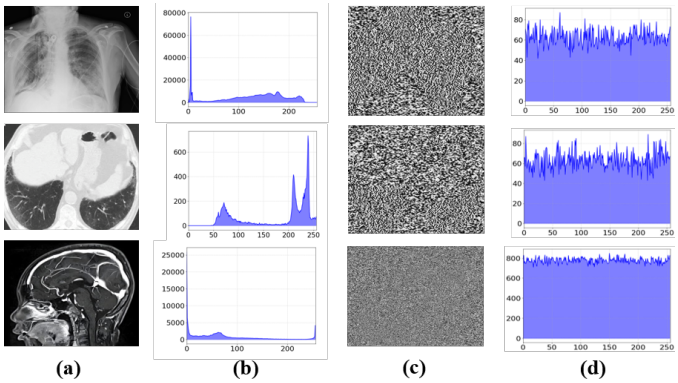

Fig. 4. The grayscale histograms of medical images. Where (a) represents initial images, (b) represents the grayscale histograms of initial images, (c) represents the cipher images encrypted with the proposed method, and (d) represents the grayscale histograms of cipher images.

if an attacker obtains a cipher image and attempts to acquire the initial key through brute force, the expandable space of the key space can reach 2^{256}. After such expansion, the SHA256 algorithm is equivalent to extending to 2^{256} output results, which is quite an astonishing scale. Therefore, obtaining the initial key through brute force is hard work, the proposed method possesses an adequate keyspace to ensure security.

D. Histogram Analysis

Researchers tend to utilize grayscale histograms to visually represent the number of pixel values at each grayscale level. For image encryption, the grayscale histogram directly expresses a certain amount of information, which poses a risk of information leakage. Hence, it is necessary to adjust the grayscale pixel distribution in cipher images. We utilize the proposed method to encrypt medical images, which creates a cipher image with random grayscale pixel distribution, the visual results are shown in Fig. 4. From the figure, the grayscale pixel distribution of initial images looks very regular, which performs clear features and is easily cracked subjectively. However, the grayscale pixel distribution of the cipher image encrypted by the proposed method looks very messy, it is difficult to distinguish the cipher image from white noise. This greatly increases the difficulty of decrypting the cipher image, making it an almost impossible task. The above analysis shows that the proposed method maintains a high security against information leakage and is hard to crack.

E. Pixel Correlation Analysis

Adjacent pixels often exhibit a strong correlation coefficient within one image, which provides crucial clues for illegal decryption. Breaking this correlation is crucial for image encryption, as failure to do so significantly reduces the difficulty of illegal decryption. We can describe the correlation

TABLE I
COMPARISON OF CORRELATION COEFFICIENTS BETWEEN PLAIN IMAGES AND CIPHER IMAGES

Source	Plain			Cipher		
	H	V	D	H	V	D
ChestX1	0.7105	0.7424	0.7735	0.0015	0.0016	0.0023
ChestX2	0.9396	0.9875	0.9912	0.0016	0.0025	-0.0015
COVID1	0.7619	0.8496	0.7841	0.0019	0.0012	0.0017
COVID2	0.7630	0.9013	0.8412	0.0009	0.0014	0.0011
fcon1	0.8915	0.8266	0.8315	0.0021	0.0008	-0.0009
fcon2	0.7992	0.7934	0.8229	0.0019	0.0011	-0.0015

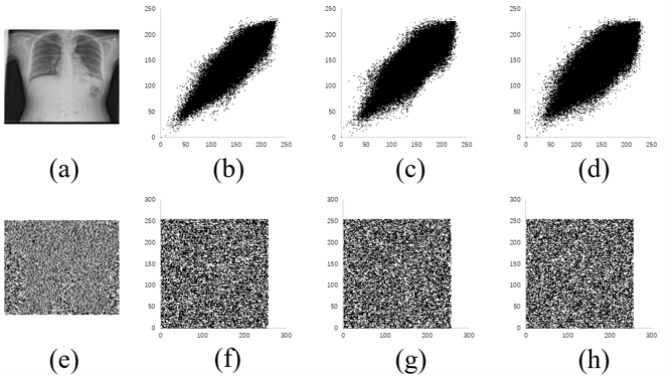

Fig. 5. The visualization of correlation coefficients between medical images before and after encryption. As illustrated, (a) represents the plain image before encryption, and (e) represents the cipher image after encryption. (b)-(d) represents the correlation coefficients before encryption in the horizontal, vertical, and diagonal directions, respectively. Similarly, (f)-(h) represents the correlation coefficients after encryption in horizontal, vertical, and diagonal directions.

coefficient with the following formula:

$$\begin{cases} r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \\ cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \\ D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \\ E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \end{cases} \tag{5}$$

We define x to a specific pixel and define y to its adjacent pixel, $cov(x, y)$ is their covariance. $E(x)$ computes the expectation of x, and $D(x)$ computes the variance of x, the same applies to y. To further elucidate the issue of correlation, we calculate the correlation coefficients of adjacent pixels from three different directions: horizontal, vertical, and diagonal. These calculations can be presented in Table I. From the table, we can directly observe that the correlation coefficient between adjacent pixels of plain images performs high before encryption, indicating a significant correlation between adjacent pixels. However, the correlation coefficient between adjacent pixels of cipher images is low after encryption, indicating that the correlation between adjacent pixels has been disrupted. Additionally, Fig. 5 illustrates a visual comparison of correlation coefficients before and after encryption for a given medical image, which further validates the efficacy of the proposed method.

F. Information Entropy Analysis

Information entropy aims to measure the magnitude of information, which primarily serves to quantify the uncertainty or randomness of information. Generally, higher information entropy indicates greater uncertainty, further signifying richer information content. If an event is highly random, its information entropy value performs high. Conversely, if an event is highly certain, its information entropy value performs relatively low. In this paper, we employ information entropy to characterize the information diffusion degrees in encrypted images. Specifically, higher information entropy of encrypted images indicates greater complexity and randomness, which increases the difficulty of illegal decryption. We propose an LLM enhancing module and content-aware permutation&diffusion module, integrating with the DNA operations to increase randomness and complexity of pixel information, thus increasing the confusion for information entropy. For a random variable X, the information entropy $H(X)$ is defined as [42]:

$$H(X) = -\sum_{i=1}^{256} p(x_i)\log_2 p(x_i) \tag{6}$$

where x_i represents pixel values, and $p(x_i)$ denotes the probability value corresponding to x_i. We randomly select 6 images from 3 datasets and calculate their information entropy after encryption. The calculated entropy values of these encrypted images are as follows: 1) 7.9895 2) 7.9894 3) 7.9882 4) 7.9860 5) 7.9991 6) 7.9993. These results show that the entropy value of the encrypted image is significantly higher and almost reaches 8, which indicates the proposed method can disrupt the regularity among pixels, thus effectively boosting the safety of image encryption.

G. Sensitivity Analysis

Differential cryptanalysis [43] is a kind of cryptographic attack technique, which aims to break cryptographic systems or encryption algorithms. It leverages the differences between plain images and cipher images to extract information about the cryptographic key or algorithm structure. This attack typically exploits small variations between inputs to infer properties of the key or algorithm, which poses a significant threat to the cryptographic system. To capture such subtle variations, researchers commonly employ NPCR [36] and UACI [44] for assessment. We provide the calculation formulas here for both metrics:

$$\begin{cases} NPCR = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D_{ij} \times 100\% \\ UACI = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(\frac{C_i(i,j) - C_i^{'}(i,j)}{255}) \times 100\% \end{cases} \tag{7}$$

$$D_{ij} = \begin{cases} 1, C_i(i,j) \neq C_i^{'}(i,j) \\ 0, C_i(i,j) = C_i^{'}(i,j) \end{cases} \tag{8}$$

Given C_i as a cipher image, we alter only a single pixel in C_i to obtain another cipher image $C_i^{'}$, the rest pixels remain identical. Therefore, we can verify the impact of minor changes by comparing C_i and $C_i^{'}$. In this paper, we analyze the sensitivity of the input plain image and initial key. Specifically, for a given plain image, we select a certain pixel and add the pixel value by 100 to distinguish the original image. To mitigate randomness, we select 6 images from three datasets

TABLE II
SENSITIVITY ANALYSIS OF PLAIN IMAGES AND CIPHER IMAGES

Plain Images	NPCR	UACI
1	99.6189	33.4882
2	99.6093	33.5011
3	99.6093	33.4387
4	99.6167	38.4619
5	99.6198	33.4723
6	99.6052	33.5083
Cipher Image	NPCR	UACI
$C_1 \leftrightarrow C_2$	99.5945	33.3915
$C_1 \leftrightarrow C_3$	99.6069	33.4239
$C_2 \leftrightarrow C_3$	99.5774	33.4037

and compute the values 20 times for each image, averaging the results to obtain the final results. The evaluation results are presented in Table II, which shows the proposed method achieves almost the theoretical upper limits of NPCR and UACI, thus demonstrating the excellent performance of the proposed method.

We set the initial key as a 2048×2 matrix and utilize LLM-enhanced DNA algorithms to encode and encrypt the image, generating the cipher image C_1. Meanwhile, we obtain random factors x_0 and p with the content-aware permutation&diffusion module. Specifically, we set x_0=0.954835655147937 and p=0.651258963465537. We slightly modify x_0 and p by setting $x_0 = x_0 + 10^{-14}$ and $p = p + 10^{-14}$, generating cipher images C_2 and C_3, respectively. Next, we evaluate these three cipher images with NPCR and UACI metrics. To visually compare and analyze the sensitivity of plain images and cipher images, we put specific calculation results in Table II.

H. Computation Cost Analysis

In this paper, we propose a plausibly deniable medical image encryption method consisting of LLM enhancing module and content-aware permutation&diffusion module. For the LLM enhancing module, the computation cost mainly focuses on the vision transformer architecture. Given an $H \times W$ image, we initially utilize the proposed method to divide the image into n blocks. Subsequently, each image block is mapped through a fully connected layer. Assuming the length of each image block is d, the time complexity of patch embedding is $O(nd^2)$. Then, the vector sequence is encoded to create an encoding time complexity of $O(n^2d+nh)$, where the hidden layer dimension is h. Finally, considering the aforementioned scenarios, the overall time complexity of LLM enhancing module is $O(nd^2+n^2d+nh)$. For the content-aware permutation&diffusion module, the focus of time complexity includes PWLCM and HCLS algorithms, which can be both identified as $l \times l$. Where l represents the length of the inputted sequence. Finally, the overall time complexity of the proposed method becomes $O(nd^2 + n^2d + nh + l^2)$. Especially, with the experimental environment we implement, it takes 0.49s to encrypt a 256×256 grayscale image and 1.97s to encrypt a 512×512 grayscale image in test mode. This time cost is satisfactory and it will be even lower with the improvement of hardware equipment.

I. Comparison with Other Methods

To further evaluate the performance of the proposed method, we list some of the published state-of-the-art methods to serve as a reference, the results are presented in Table III with specifically highlight the best results. Table III shows that the proposed method achieves the best performance in general, especially in sensitivity. The NPCR value reached 99.6953 and the UACI value reached 33.6047. We attribute this to involve additional adjacent pixel information by the content-aware permutation&diffusion module. However, it ranks slightly lower than the best in terms of correlation and information entropy. We believe that the discrepancy might arise from the best method utilizing RGB color images for encryption, whereas the proposed method focuses on encrypting single-channel grayscale images. As the proposed method is designed for encrypting medical images, we find the advantage of our approach in medical image encryption.

J. Ablation Study

We combine different modules in various ways to further analyze the role of each module. The modules evaluated primarily include LLMs coding, DNA coding, and content-aware permutation&diffusion module. We adopt a progressively incremental manner to combine different modules and present the calculation results in Table IV to facilitate comparative analysis. The evaluation metrics include pixel correlation in H, V, and D directions, information entropy, and sensitivity. From the table, it can be observed that the performance of DNA coding is slightly superior to LLM coding. We attribute this to the fact that LLMs are not dedicated encoding algorithms. We mainly utilize the powerful generating ability of LLMs instead of its auxiliary coding ability. In this paper, we primarily utilize LLMs to generate plausible deniable images, which is the core contribution. Furthermore, the combination of DNA coding, LLMs coding, and content-aware permutation&diffusion module create the best performance, indicating the indispensability of each module.

K. Visualization

To emphatically demonstrate the generation of plausible images under the scenario of inputting wrong keys, we provide several examples here, as shown in Fig. 6. We select 3 samples from the ChestX-ray 14, COVID-CT, and fcon-1000 datasets, and showcase intermediate figures during the encryption and decryption process. For each sample, we present 1 inputted plain image, 1 encrypted image, 1 decrypted image through the right key, and 3 decrypted images through the wrong keys to thoroughly validate the effectiveness of the plausible deniability approach. During the decryption process, if the right key is provided, an original medical image can be decrypted from a single cipher image. Otherwise, if a wrong key is given, the cipher image will be randomly decrypted into a wrong but plausible plain image. These plausible images differ from right-plain images with a clear distribution boundary, however, they still look like the images from the training set. This makes potential attackers confused and convinces them to get the

TABLE III
COMPARISON WITH OTHER METHODS

Cryptosystems	Correlation			Entropy	Sensitivity	
	V	H	D		NPCR	UACI
Zhan et al. [45]	0.0039	0.0052	0.0215	7.9978	76.26	28.30
Chai et al. [46]	-0.0082	-0.0068	0.0036	7.9992	99.62	33.51
Yan et al. [47]	-0.0056	-0.0012	-0.0020	**7.9994**	99.62	33.55
Aouissaoui et al. [48]	0.0240	0.0014	-0.0014	7.9978	99.6552	33.5871
Chen et al. [49]	-0.0064	0.0003	0.0110	7.9993	99.6218	33.5084
Zhang et al. [50]	**0.0000016**	**-0.000003**	**-0.0000001**	-	99.5009	33.4408
Wu et al. [4]	0.0014	0.0009	0.0004	7.9992	99.6841	33.5539
Ours	0.0009	0.0009	-0.0003	7.9993	**99.6953**	**33.6047**

TABLE IV
ABLATION STUDY OF DIFFERENT MODULES

Cryptosystems	Correlation			Entropy	Sensitivity	
	V	H	D		NPCR	UACI
DNA	0.0031	0.0034	0.0029	7.5531	97.5846	31.8367
LLMs	0.0038	0.0041	0.0035	7.5039	96.8776	30.9941
DNA+Permutation&Diffusion	-0.0017	0.0013	0.0018	7.9123	98.9318	33.4084
LLMs+Permutation&Diffusion	0.0027	-0.0020	-0.0023	7.8868	98.3560	32.7764
DNA+LLMs+Permutation&Diffusion	0.0009	0.0009	-0.0003	7.9993	99.6953	33.6047

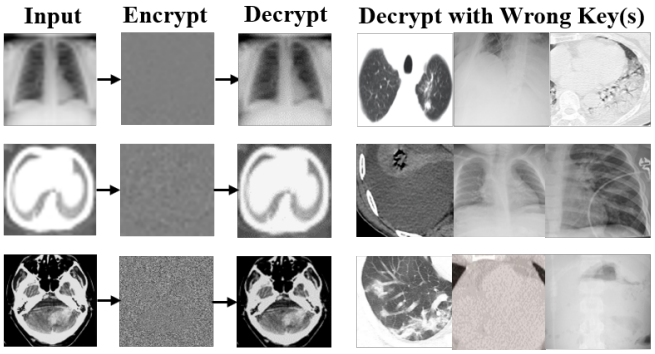

Fig. 6. The different processing steps for right and wrong keys are illustrated in the figure. Firstly, the input plain image undergoes encoding and encryption. Subsequently, if the right key is given, we utilize the proposed method to decrypt the right plain image. In contrast, a wrong yet plausible image will be randomly decrypted with a wrong key.

right image. Specifically, each wrong key can only decrypt to 1 random plausible image, and repeating the operation creates the same plausible image. This keeps the decryption process is same between right and wrong keys, making it difficult for potential attackers to distinguish between two kinds of results. In this figure, 3 plausible images require 3 different wrong keys to be decrypted.

V. CONCLUSION

In this paper, we first integrate LLMs into medical image encryption, complemented by DNA encoding and content-aware permutation&diffusion module, achieving satisfactory results in medical image encryption tasks. Before DNA encoding, the LLM enhancing module compresses pixels into highly compact signals with probabilistic variations and plausible deniability, functioning as an additional privacy-preserving layer utilizing LLM to mitigate privacy leakage. The content-aware permutation&diffusion module enhances security by adding permutation and introducing randomness through sampling from adjacent pixel correlations to disrupt internal pixel links, it also implements a DNA-based diffusion process to significantly elevate the difficulty of cracking. The proposed method employing LLMs offers a different approach to medical image encryption. In the future, with the continuous advancement of LLMs, we anticipate further improvements in our model's performance.

ACKNOWLEDGEMENT

This work was supported by the High Performance Computing Platform, Hohai University.

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] Y. Ding, F. Tan, Z. Qin, M. Cao, K. R. Choo, and Z. Qin, "Deepkeygen: A deep learning-based stream cipher generator for medical image encryption and decryption," *IEEE Trans. Neural Networks Learn. Syst.*, vol. 33, no. 9, pp. 4915–4929, 2022.

[3] K. N. Singh, O. P. Singh, A. K. Singh, and A. K. Agrawal, "Eimol: A secure medical image encryption algorithm based on optimization and the lorenz system," *ACM Trans. Multim. Comput. Commun. Appl.*, vol. 19, no. 2s, pp. 94:1–94:19, 2023.

[4] Y. Wu, L. Zhang, S. Berretti, and S. Wan, "Medical image encryption by content-aware DNA computing for secure healthcare," *IEEE Trans. Ind. Informatics*, vol. 19, no. 2, pp. 2089–2098, 2023.

[5] W. Gao, H. Li, M. Zhong, and M. Lu, "An underestimated cybersecurity problem: Quick-impact time synchronization attacks and a fast-triggered detection method," *IEEE Trans. Smart Grid*, vol. 14, no. 6, pp. 4784–4798, 2023.

[6] Y. Li, J. Yang, Z. Zhang, J. Wen, and P. Kumar, "Healthcare data quality assessment for cybersecurity intelligence," *IEEE Trans. Ind. Informatics*, vol. 19, no. 1, pp. 841–848, 2023.

[7] P. Sarosh, S. A. Parah, B. A. Malik, M. Hijji, and K. Muhammad, "Real-time medical data security solution for smart healthcare," *IEEE Trans. Ind. Informatics*, vol. 19, no. 7, pp. 8137–8147, 2023.

[8] 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.

[9] P. I. Radoglou-Grammatikis, K. Rompolos, P. G. Sarigiannidis, V. Argyriou, T. Lagkas, A. Sarigiannidis, S. K. Goudos, and S. Wan, "Modeling, detecting, and mitigating threats against industrial healthcare systems: A combined software defined networking and reinforcement learning approach," *IEEE Trans. Ind. Informatics*, vol. 18, no. 3, pp. 2041–2052, 2022.

[10] P. Soni, J. Pradhan, A. K. Pal, and S. H. Islam, "Cybersecurity attack-resilience authentication mechanism for intelligent healthcare system," *IEEE Trans. Ind. Informatics*, vol. 19, no. 1, pp. 830–840, 2023.

[11] L. Xu, X. Zhou, Y. Tao, L. Liu, X. Yu, and N. Kumar, "Intelligent security performance prediction for iot-enabled healthcare networks using an improved CNN," *IEEE Trans. Ind. Informatics*, vol. 18, no. 3, pp. 2063–2074, 2022.

[12] B. Ji, Y. Wang, L. Xing, C. Li, Y. Wang, and H. Wen, "Irs-driven cybersecurity of healthcare cyber physical systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 2564–2573, 2023.

[13] H. Kwon, S. Lee, Y. H. Kim, and S. Kang, "Additive statistical leakage analysis using exponential mixture model," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, vol. 39, no. 12, pp. 4985–4998, 2020.

[14] H. M. Heys and L. Zhang, "Pipelined statistical cipher feedback: A new mode for high-speed self-synchronizing stream encryption," *IEEE Trans. Computers*, vol. 60, no. 11, pp. 1581–1595, 2011.

[15] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X. Phuong, and Q. Xie, "A dfa-based functional proxy re-encryption scheme for secure public cloud data sharing," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 10, pp. 1667–1680, 2014.

[16] N. Y. Yu, "Indistinguishability and energy sensitivity of gaussian and bernoulli compressed encryption," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 7, pp. 1722–1735, 2018.

[17] A. Kato and T. H. Kinnunen, "Statistical regression models for noise robust F0 estimation using recurrent deep neural networks," *IEEE ACM Trans. Audio Speech Lang. Process.*, vol. 27, no. 12, pp. 2336–2349, 2019.

[18] H. Huang, X. Xue, C. Liu, Y. Wang, T. Luo, L. Cheng, H. Li, and X. Li, "Statistical modeling of soft error influence on neural networks," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, vol. 42, no. 11, pp. 4152–4163, 2023.

[19] Y. Cai, W. Ding, Y. Xiao, Z. Yan, X. Liu, and Z. Wan, "Secfed: A secure and efficient federated learning based on multi-key homomorphic encryption," *IEEE Trans. Dependable Secur. Comput.*, vol. 21, no. 4, pp. 3817–3833, 2024.

[20] T. B. Brown, B. Mann, and N. Ryder, "Language models are few-shot learners," in *Proceedings of Conference on Neural Information Processing Systems*, 2020.

[21] Z. Wang, M. Li, R. Xu, L. Zhou, J. Lei, X. Lin, S. Wang, Z. Yang, C. Zhu, D. Hoiem, S. Chang, M. Bansal, and H. Ji, "Language models with image descriptors are strong few-shot video-language learners," in *Proceedings of Conference on Neural Information Processing Systems*, 2022.

[22] H. Touvron, L. Martin, and K. Stone, "Llama 2: Open foundation and fine-tuned chat models," *CoRR*, vol. abs/2307.09288, 2023.

[23] L. Yu, D. Simig, C. Flaherty, A. Aghajanyan, L. Zettlemoyer, and M. Lewis, "MEGABYTE: predicting million-byte sequences with multi-scale transformers," in *Proceedings of Conference on Neural Information Processing Systems*, 2023.

[24] X. Liu, Z. Wu, X. Wu, P. Lu, K. Chang, and Y. Feng, "Are llms capable of data-based statistical and causal reasoning? benchmarking advanced quantitative reasoning with data," in *Proceedings of the Association for Computational Linguistics*, 2024, pp. 9215–9235.

[25] P. Liu, X. Wang, and Y. Su, "Image encryption via complementary embedding algorithm and new spatiotemporal chaotic system," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 33, no. 5, pp. 2506–2519, 2023.

[26] A. Jolfaei, X. Wu, and V. Muthukkumarasamy, "On the security of permutation-only image encryption schemes," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 2, pp. 235–246, 2016.

[27] M. Preishuber, T. Hütter, S. Katzenbeisser, and A. Uhl, "Depreciating motivation and empirical security analysis of chaos-based image and video encryption," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 9, pp. 2137–2150, 2018.

[28] J. Chen, L. Chen, and Y. Zhou, "Universal chosen-ciphertext attack for a family of image encryption schemes," *IEEE Trans. Multim.*, vol. 23, pp. 2372–2385, 2021.

[29] C. Zhang, J. Chen, D. Chen, W. Wang, Y. Zhang, and Y. Zhou, "Exploiting substitution box for cryptanalyzing image encryption schemes with DNA coding and nonlinear dynamics," *IEEE Trans. Multim.*, vol. 26, pp. 1114–1128, 2024.

[30] Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, M. Cao, and Z. Qin, "Deepedn: A deep-learning-based image encryption and decryption network for internet of medical things," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1504–1518, 2021.

[31] U. Erkan, A. Toktas, S. Enginoglu, E. Akbacak, and D. N. H. Thanh, "An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN," *Multim. Tools Appl.*, vol. 81, no. 5, pp. 7365–7391, 2022.

[32] S. Haddad, G. Coatrieux, A. Moreau-Gaudry, and M. Cozic, "Joint watermarking-encryption-jpeg-ls for medical image reliability control in encrypted and compressed domains," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2556–2569, 2020.

[33] F. Zhang, X. Zhang, M. Cao, F. Ma, and Z. Li, "Characteristic analysis of 2d lag-complex logistic map and its application in image encryption," *IEEE Multim.*, vol. 28, no. 4, pp. 96–106, 2021.

[34] Z. Huang, F. Zhang, L. Kou, Q. Yuan, and Y. Liu, "A real-time image encryption algorithm for a distributed energy system based on the 13-d complex chaotic sequence," *IEEE Multim.*, vol. 30, no. 4, pp. 71–81, 2023.

[35] C. Wang, J. Hu, S. Bian, J. Ni, and X. Zhang, "A customized deep network based encryption-then-lossy-compression scheme of color images achieving arbitrary compression ratios," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 33, no. 8, pp. 4322–4336, 2023.

[36] X. Gao, J. Mou, S. Banerjee, and Y. Zhang, "Color-gray multi-image hybrid compression-encryption scheme based on BP neural network and knight tour," *IEEE Trans. Cybern.*, vol. 53, no. 8, pp. 5037–5047, 2023.

[37] D. Pavllo and S. Anagnostidis, "Plausibly deniable encryption with large language models."

[38] M. Chen, A. Radford, R. Child, J. Wu, H. Jun, D. Luan, and I. Sutskever, "Generative pretraining from pixels," in *Proceedings of International Conference on Machine Learning*, 2020, pp. 1691–1703.

[39] 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.

[40] B. Chen, Z. Zhang, Y. Li, G. Lu, and D. Zhang, "Multi-label chest x-ray image classification via semantic similarity graph embedding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 4, pp. 2455–2468, 2022.

[41] J. Zhao, Y. Zhang, X. He, and P. Xie, "Covid-ct-dataset: A CT scan dataset about COVID-19," *CoRR*, vol. abs/2003.13865, 2020.

[42] G. Gour and M. Tomamichel, "Entropy and relative entropy from information-theoretic principles," *IEEE Trans. Inf. Theory*, vol. 67, no. 10, pp. 6313–6327, 2021.

[43] T. Cui, Y. Zhang, J. Zhang, C. Jin, and S. Chen, "Differential-invariant subspace cryptanalysis - A real-time attack against iot-friendly word-based block ciphers," *IEEE Internet Things J.*, vol. 11, no. 10, pp. 17 642–17 650, 2024.

[44] P. Liu, X. Wang, Y. Su, H. Liu, and S. Unar, "Globally coupled private image encryption algorithm based on infinite interval spatiotemporal chaotic system," *IEEE Trans. Circuits Syst. I Regul. Pap.*, vol. 70, no. 6, pp. 2511–2522, 2023.

[45] 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.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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.