DPPAD-IE: Dynamic Polyhedra Permutating and Arnold Diffusing Medical Image Encryption Using 2D Cross Gaussian Hyperchaotic Map

Quanjun Li, Qian Li, Bingo Wing-Kuen Ling, *Senior Member, IEEE*, Chi-Man Pun, *Senior Member, IEEE*, Guoheng Huang*, Xiaochen Yuan, *Senior Member, IEEE*, Guo Zhong*, Sarra Ayouni, and Jianwu Chen*

***Abstract*—With the rapid improvement of medical consumer electronics (CE), the transmission of multiple images has become increasingly common in the medical field. During the transmission and storage of image data, sensitive information, including medical images, may be accessed by unauthorized parties, resulting in possible privacy violations. Consequently, several multi-image encryption (MIE) algorithms have been proposed to solve this real-world problem. Nevertheless, current MIE schemes exhibit several drawbacks, including insufficient security in permutation and diffusion algorithms, as well as the insensitivity of chaotic maps. This paper presents a new encryption algorithm called DPPAD-IE. The algorithm primarily consists of three components. First, we developed an innovative hyperchaotic map called the 2D Cross Gaussian Hyperchaotic Map (2D-CGHM), which has an expanded chaotic interval and is proficient in producing chaotic sequences with improved pseudorandomness. Second, we introduce a new Dynamic Polyhedra Permutation algorithm (DPP) that successfully alters pixel locations of the image, hence diminishing the connection between neighboring pixels. Third, we propose an Arnold Diffusion algorithm (AD), using chaotic sequences to further encrypt the permuted image. The DPPAD-IE is capable of encrypting images of any quantity and size concurrently. The experimental results confirm that this approach is both robust and effective, capable of defending against various security attacks. The code are available at: https://github.com/QuincyQAQ/DPPAD-IE.**

***Index Terms*—Consumer electronics, Hyperchaotic map, Multi-image encryption, Efficiency, Smart healthcare**

I. INTRODUCTION

As medical management services develop, consumer electronics (CE), which include devices such as smartphones, wearables, tablets, and personal computers, are increasingly being incorporated into public healthcare systems. For instance, numerous medical images used in online diagnostics are exchanged through consumer electronic (CE) devicess [1]. These devices enable real-time medical diagnostics and data sharing, but their widespread use also introduces significant security challenges. Additionally, many images processed by artificial intelligence also need to be protected[2], [3], [4]. These images, like others, require robust protection during transmission to prevent unauthorized access [5], [6], [7]. As a result, securing the transmission of such sensitive data has become a critical concern, particularly as data breaches could compromise patient confidentiality and trust in medical services [8], [9], [4]. Encryption is essential for safeguarding digital images, as it transforms them into encrypted formats through the use of public or private keys [10], [11]. This ensures data integrity and confidentiality during transmission, even in potentially insecure environments. However, consumer electronics often operate under resource constraints, such as limited memory and computational power, further complicating the implementation of robust encryption schemes. Beyond security, there is also a need to achieve fast transmission of multiple images and low storage requirements, thereby saving memory and computation for consumer electronic devices with limited memory [12]. However, most existing encryption techniques are tailored for Single Image Encryption (SIE), which results in low efficiency when handling the transmission of multiple images. Therefore, advanced multi-image encryption schemes are urgently needed for faster, more secure and resource-efficient data exchange [13].

Typically, image encryption algorithms based on chaos involve three primary stages: the generation of Chaotic se-

This work was supported by Key Areas Research and Development Program of Guangzhou Grant 2023B01J0029, the Guangdong Provincial Key Laboratory of Cyber-Physical System under Grant 2020B1212060069, the University of Macau under Grant MYRG2022-00190-FST, and in part by the Science and Technology Development Fund, Macau SAR, under Grant 0141/2023/RIA2 and 0193/2023/RIA3, and Princess Nourah bint Abdulrahman University Researchers Supporting Projectnumber (PNURSP2025R896), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. (*Corresponding author: Guoheng Huang; Guo Zhong; Jianwu Chen.)

Quanjun Li is with School of Advanced Manufacturing, Guangdong University of Technology, Jieyang 522000, China (e-mail: 3122008887@mail2.gdut.edu.cn).

Qian Li is with School of Electronics and Information Engineering, Wuyi University, Jiangmen 510006, China (e-mail: 3222003726@wyu.edu.cn).

Bingo Wing-Kuen Ling is with the School of Information Engineering, Guangdong University of Technology, Guangzhou 510006, China (e-mail: yongquanling@gdut.edu.cn)

Chi-Man Pun is with the Faculty of Science and Technology, University of Macau, Macau S.A.R. (e-mail: cmpun@um.edu.mo).

Guoheng Huang is with the School of Computer Science and Technology, Guangdong University of Technology, Guangzhou 510006, China (e-mail: kevinwong@ gdut.edu.cn).

Xiaochen Yuan is with the Faculty of Applied Sciences, Macau Polytechnic University, Macau, China (e-mail: xcyuan@mpu.edu.mo).

Guo Zhong is with the School of Information Science and Technology, Guangdong University of Foreign Studies, Guangzhou 510420, China (e-mail:yb77410@um.edu.mo).

Sarra Ayouni is with the Department of Information Systems, College of Computer and Information sciences, Princess Nourah bint Abdulrahman University, P.O. BoX 84428, Riyadh 11671, Saudi Arabia (e-mail:saayouni@pnu.edu.sa).

Jianwu Chen is with the Department of Radiation Oncology, Fujian Medical University Union Hospital, Fuzhou, Fujian province, China; Fujian Key Laboratory of Intelligent Imaging and Precision Radiotherapy for Tumors (Fujian Medical University), Fuzhou, Fujian province, China; Clinical Research Center for Radiology and Radiotherapy of Fujian Province (Digestive, Hematological and Breast Malignancies), Fuzhou, Fujian province, China (email:chenjianwucn@aliyun.com).

quences via chaotic maps, rearrangement of pixel positions, and pixel value modification [14]. Chaotic key sequences play a critical role in introducing randomness into encryption systems and are generally derived from chaotic maps, which are categorized into one-dimensional (1D) and high-dimensional (HD) types [15]. Although 1D chaotic maps are efficient and simple, they suffer from a limited range of control parameters and Lyapunov exponents, displaying only chaotic behavior without hyperchaotic characteristics [16]. Additionally, HD chaotic maps, while having better chaotic performance, require a lot of computation when used to generate keystreams. To address this trade-off between security and efficiency, researchers have developed 2D chaotic maps, which offer a compromise between 1D and HD variants[17], [18], [19], [18], [20], [21]. Despite their high performance, 2D maps often involve considerable complexity, and their hyperchaotic parameter space is discontinuous [18]. Zheng et al. introduced a 2D logistic sine chaotic map (2D-LSMM) and proposed an advanced image encryption method by incorporating DeoxyriboNucleic Acid (DNA) coding [20]. This innovation enhanced the randomness and complexity of the system's state, resulting in a larger key space compared to 1D chaotic maps. However, the 2D-LSMM's parameter range is limited, with $\mu 1$ and $\mu 2$ confined to [0, 4]. To overcome this limitation, Teng et al. presented a 2D cross-logistic-sin-sin chaotic map (2D-CLSS) combined with a cryptosystem strategy [21]. By integrating trigonometric sine functions, the system achieved greater structural complexity and significantly improved chaotic behavior. However, four critical issues are associated with the aforementioned 2D chaotic maps: First, its chaotic characteristics, including chaotic sequences, control parameters, and initial conditions, are predictable [22]. Second, minor degradation in control parameters, resulting in a shift to periodic behavior, which reduces chaotic properties [23]. Third, simplified chaotic properties that degrade system dynamics and pose severe security risks [24]. Forth, some chaotic maps are prone to produce aggregated chaotic sequences, for example, 2D-CLSS has the problems of uneven distribution of phase diagrams and single control parameter therefore it is prone to produce aggregated chaotic sequences [21]. Therefore, inspired by the observation that many existing methods obtain better performance of 2D chaotic maps through the integration of 1D chaotic maps [25], [26], [21], [20], we present a novel 2D chaotic map named 2D-CGHM. This new map combines two Gaussian maps, offering a straightforward structure, enhanced dynamic properties, an extensive parameter range, and continuous hyperchaotic behavior. These features makes it difficult to crack and more suitable for key stream generation.

Changing the pixel distribution within a standard image modifies its inherent statistical properties, thereby improving its ability to resist statistical analysis-based attacks. This is because statistical attacks, such as histogram analysis and correlation analysis, rely on predictable patterns in the pixel intensity and spatial relationships of the original image. By disrupting these patterns through pixel redistribution, the statistical features become indistinguishable, rendering such attacks ineffective [27]. Consequently, image encryption frequently employs permutation methods that utilize chaotic maps. As a permutation method, scanning techniques are extensively applied in this field because they require minimal computational resources and are effective in reducing high correlations present in images, including zigzag patterns [27], [28], raster and continuous raster patterns [29], [30], and spiral patterns [31], [32]. By following a specific scan route, an image is transformed into a new 1D vector, which is subsequently reconstituted into a new image according to the raster order. Wang et al. propose four improved scan routes based on the zigzag permutation structure and use them to permute natural images. Rashmi and colleagues proposed an innovative cryptographic system for images, which utilizes chaotic maps, continuous raster scanning techniques, and a layered block structure. Although the algorithms could obtain good permutational performance, they have several drawbacks: First, at least two pixels' position failing to change, rectangular images like X-rays of long bones and diagnostic images of Alzheimer's disease cannot be encrypted. Second, the algorithms exhibit periodicity issues [33]. Third, simple scanning algorithms are easily cracked. For example, Cao et al. proposed a raster-scan-based algorithm [34], as illustrated in Figure 1(a). This algorithm employs a straightforward and linear raster scanning pattern, making it highly predictable and vulnerable to brute-force attacks. Shi et al. demonstrated the insecurity of this approach by successfully cracking it using both ciphertext-only and plaintext-based attacks [35]. Forth, these scanning techniques are capable of encrypting only one image at a time, which prevents them from processing several images concurrently. In many applications, there is often a need to transmit large volumes of images over a network [36]. For instance, in the medical field, CT scans and MRIs produce multi-layered images [37] to accurately assess the condition of various organs. While methods for encrypting a single image (SIE) can repeatedly process multiple images, their efficiency is often deemed inadequate [38]. Consequently, enhancing secure approaches for multi-image scanning and shuffling becomes crucial in medical applications. To address this, as far as we are aware, we introduce for the first time the Chainsaw Scan Algorithm, which stands apart from other methods due to its capability to traverse rectangular edges and rearrange images of arbitrary shapes, eliminating permutation periodicity. Based on the Chainsaw Scan Algorithm, we propose DPP that can encrypt multiple images simultaneously.

Image encryption systems that rely solely on permutation lack security against threats like ciphertext-only, known-plaintext attacks or chosen-plaintext attacks, as well as against image correlations, as they preserve the original image's statistical properties [39]. Attackers can exploit these properties using techniques like differential or statistical analysis, leading to the encryption system being broken. This problem can be solved by changing the pixel values using the diffusion algorithm, which effectively disrupts the local structure of the image data and makes the relationship between neighbouring pixels more complex, thus enhancing the encryption effect. However, in most image encryption schemes discussed, the diffusion process operates independently of the original image. This characteristic introduces a security vulnerability where the cryptosystem lacks sensitivity to both the secret keys and

the original images, rendering it susceptible to differential attacks [40], [41], [42]. To address the problem of insufficient sensitivity to plaintext and keys in image encryption systems, researchers have recently developed several diffusion algorithms that are directly linked to plaintext [43], [44], [45], [46]. For example, Murillo et al. introduced a novel plaintext correlation diffusion algorithm [43], illustrated in Figure 1(b). This algorithm computes a plaintext-related value from the plaintext image and generates chaotic sequences through two logical maps. Similarly, Parvin et al. introduced a highly sensitive image encryption scheme using the logical operator xor, which utilises two chaotic functions and the XOR operation for enhanced sensitivity to the original image [44]. In other image encryption methods presented in [43], [44], [45], [46], the process of generating security keys, which must be shared with the receiver, relies on the initial image. As a consequence, encrypting diverse plain images with such an encryption scheme may prove inadequate for situations that demand real-time image encryption, especially in the case of encrypting live video streams. Furthermore, the diffusion algorithms of these cryptosystem are susceptible to chosen-plaintext and known-plaintext attacks because of their insufficient nonlinearity, limited secure key space, and failure to produce significant avalanche effects. For instance, the image encryption systems proposed by [43], [44] were analyzed and cracked by chosen plaintext attacks [47], [48]. To address these issues, our strategy incorporates the Arnold map into the diffusion process, introducing stronger nonlinearity and higher entropy [49]. Its large parameter space and chaotic properties offer enormous potential, but most existing schemes use it only as a pixel replacement tool or key generator without fully exploiting its capabilities [50], [51], [52]. In contrast, we break with tradition and propose a new effective Arnold diffusion algorithm that ensures diffusion by a strong avalanche effect connecting each encrypted pixel with its neighbouring pixels.

In the case of encryption multiple images, the SIE algorithms are inefficient and insecure [13]. To address this issue, numerous algorithms for multi image encryption (MIE) have been developed [38], [53]. Nonetheless, these MIE schemes exhibit certain limitations. Firstly, a few algorithms are designed exclusively for encrypting images of uniform dimensions, rendering them incapable of processing images with varying sizes. Secondly, some algorithms can only encrypt a predetermined quantity of images at once, preventing them from supporting a variable number of images. Third, the majority of existing algorithms commonly use standard grayscale images as test examples; however, encryption schemes specifically designed for medical images are exceedingly rare. To overcome the above drawbacks, this paper introduces a novel and efficient encryption algorithm, referred to as DPPAD-IE, specifically designed for multi-medical images. The main contributions and unique aspects of this study are summarized as follows:

1) While numerous algorithms for image encryption have been introduced, they frequently face challenges such as restricted key space and a lack of adequate nonlinear characteristics, which diminish both their efficiency and security. Thus, we propose a new DPPAD-IE algorithm, which consists of a new permutation algorithm, a new diffusion algorithm, and a new chaotic system to overcome the drawbacks of existing schemes, such as the low security key space and the poor nonlinear performance.
2) Many traditional chaotic maps suffer from inadequate security due to their limited chaotic range and the small number of control parameters in a chaotic state. To address these limitations, this paper introduces the Two-Dimensional Cross Gaussian Hyperchaotic Map (2D-CGHM), which overcomes the deficiencies of existing chaotic systems by expanding both the parameter space and the chaotic range.
3) Most permutation algorithms cannot encrypt multiple images simultaneously, and even encrypting multiple images separately is often inefficient. Thus, we propose a new scanning algorithm that can scan images of any shape. Based on this, we propose a Dynamic Polyhedra Permutation algorithm (DPP) that can simultaneously permutate multiple images.
4) The results of thorough experiments performed on two publicly available datasets, one for chest X-ray images and the other for brain tumors, highlight that DPPAD-IE achieves outstanding performance compared to state-of-the-art methods, along with exceptional reconstruction quality.

The rest of this paper can be summarized as follows: Section II introduces the methodology. Section III describes the experimental results. In section IV, we come to conclusions.

II. METHODOLOGY

This section presents a new encryption algorithm designed for multi-medical images, which leverages the 2D-CGHM and is referred to as DPPAD-IE. Figure 2 illustrates the flowchart of DPPAD-IE, which comprises three main modules: Chaotic sequences generation, Dynamic Polyhedra Permutation, and Arnold diffusion. Our proposed algorithm supports simultaneous encryption of multiple images. Assume that there are N original images, each of size $m \times n$, labeled as $Img1, Img2, \ldots, ImgN$. The corresponding keys include Key_{x1}, Key_{y1}, Key_{a1}, Key_{b1}, Key_a, Key_b, and $N0$. The specific details for every module involved in the encryption procedure are elaborated below:

A. Chaotic sequences generation using 2D-CGHM

In general, hyperchaotic map is more disordered than ordinary chaos, and hyperchaotic systems have more complicated topological structures and dynamics than ordinary chaotic ones[54]. The Gaussian map and Logistics map, given by Equation 1 and 2, are classic 1D chaotic maps commonly used in image encryption. Nevertheless, their chaotic range remains constrained, and the randomness of output sequences tends to be insufficient [55].

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

$$x_{n+1} = e^{-\varphi x_n^2} - \varepsilon \tag{2}$$

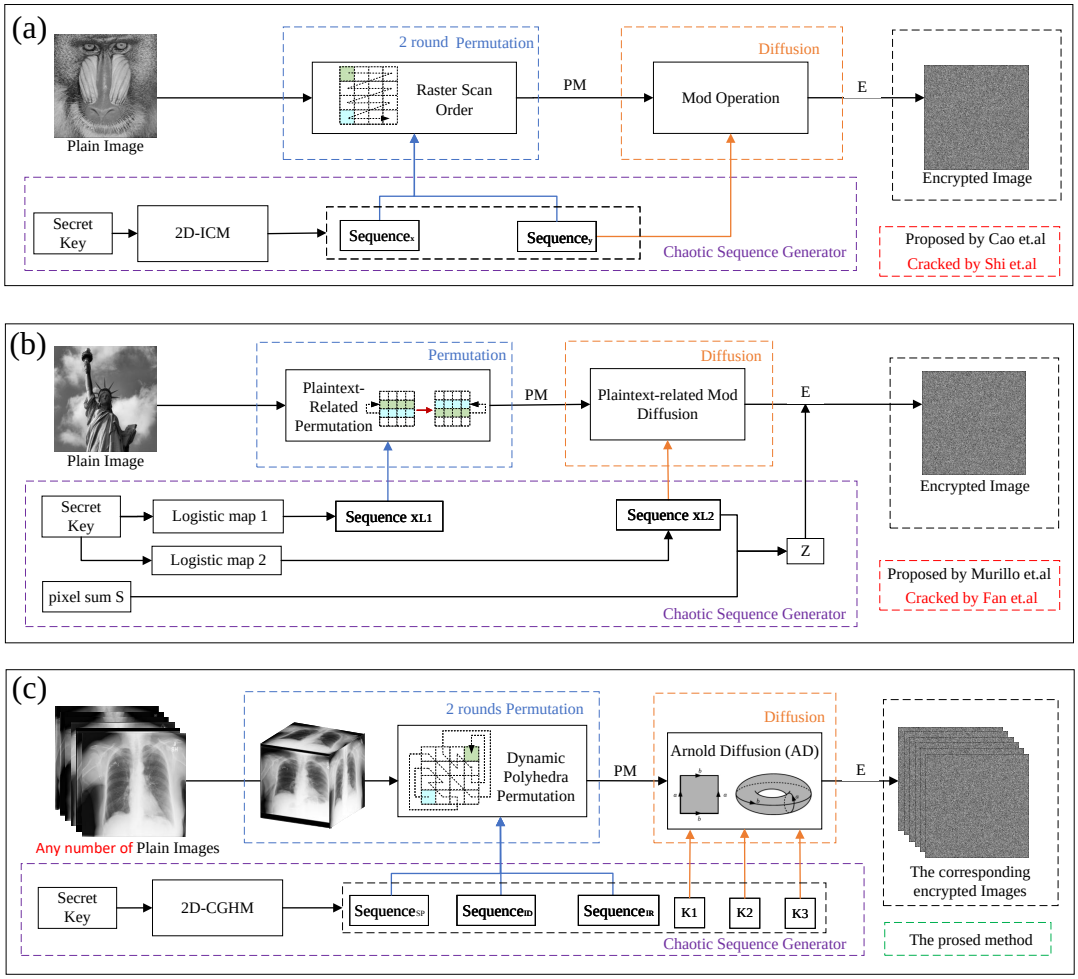


Fig. 1. Illustration of the difference among different methods, where PM represents the permuted image and E represents the encrypted image: (a) Cao et al.'s method [34]; (b) In Murillo et al.'s method [43]; (c) The proposed method.

To address this, a new hyperchaotic map was proposed, described in Equation 3, where the control parameters $a \in (0, 25)$ and $b \in (0, 25)$. The stochasticity of chaotic systems mainly originates from their sensitivity to initial conditions and nonlinear dynamics[56]. The 2D-CGHM map achieves sequence generation with strong stochasticity by combining the nonlinear properties of sine and cosine functions, Gaussian mapping, and the dynamic adjustment of multiple control parameters a and b.

$$\begin{cases} x_{n+1} = a\sin(e^{y_n^2} + x_n); \\ y_{n+1} = b\cos(e^{x_n^2} + y_n); \end{cases} \tag{3}$$

We use the newly proposed 2D-CGHM as a chaotic sequence generator, and the following are the chaotic sequence generation steps:

Step 1: Setting the initial parameters of a spatiotemporal chaotic map using Key: $x_1' = Key_{x_1'}$, $y_1' = Key_{y_1'}$, $a1 = Key_{a1}$, $b1 = Key_{b1}$, $N0 = Key_{N0}$.

Step 2: Two chaotic sequences are produced by iterating the 2D-CGHM $(N+2\times m\times n+N0)$ times. And the sequences $x_n = \{x_1, \ldots, x_{N+2\times m\times n}\}$ and $y_n = \{y_1, \ldots, y_{N+2\times m\times n}\}$ are produced by discarding the first $N0$ terms of two chaotic sequences to prevent transient effects [25].

Step 3: Then, illustrated in Algorithm 1, three Chaotic sequences $Sequence_{SP}$, $Matrix_{ID}$ and $Sequence_{IR}$ are generated based on the sequences x_n and y_n.

B. Dynamic Polyhedra Permutation algorithm(DPP)

A new scanning path, called the Chainsaw scan, is proposed as shown in Figure 4. Unlike traditional scanning algorithms, the proposed approach supports images of arbitrary size, with its scanning paths illustrated in Figures 4(a) and 4(b) for square and rectangular images, respectively. The specific steps of Chao-based Chainsaw Scanning Algorithm are as follows. First, we use chaotic sequences to determine the starting point of scanning to increase nonlinearity and ensure the security of scanning algorithms. After selecting the starting point, bidirectional Chainsaw scanning is performed from that point. An example of the entire Chao-based Chainsaw Scanning Algorithm is shown in Figure 4(c). In order to quickly and effectively permutate the multiple images, based on this scanning algorithm, we propose a new permutation al-

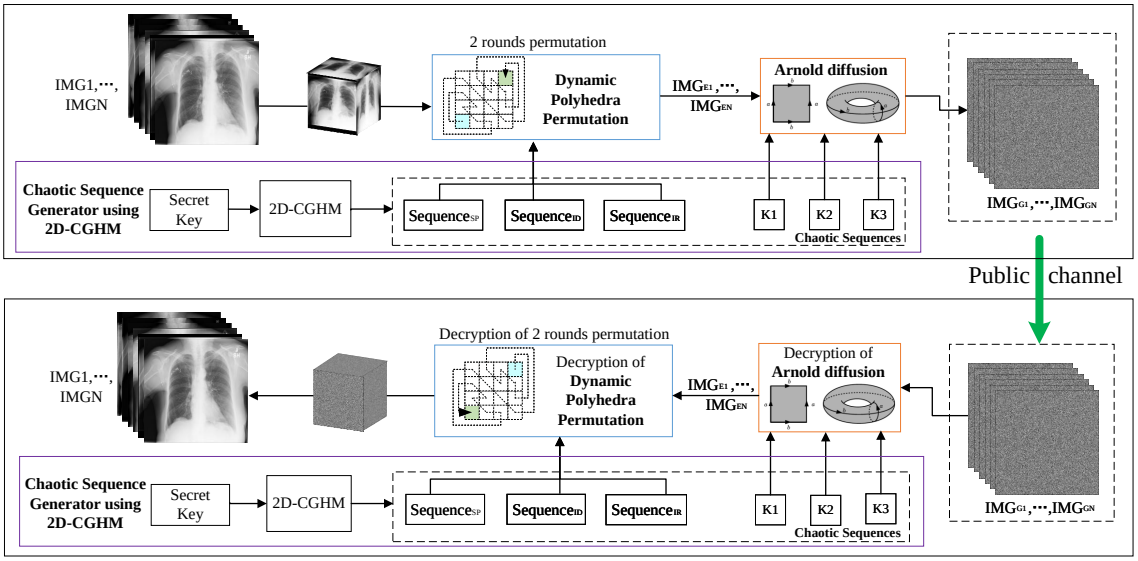


Fig. 2. Illustration of the DPPAD-IE. The encryption process includes three main modules: Chaotic sequences generation, Dynamic Polyhedra Permutation, and Arnold diffusion.

Algorithm 1 Chaotic sequences generation

Input: Number of images N, size of $m \times n$.

Output: $Sequence_{SP}, Matrix_{ID}, Sequence_{IR}, K_1, K_2, K_3$.

$Chotic_p = cat(x_n(1 : N + 2 \times m \times n + N0), y_n(1 : N + 2 \times m \times n + N0))$

$Sequence_{SP}(1 : N) = \lfloor(\mathrm{mod}(Chaotic_P(1 : N) \times 10^{15}, m \times n)\rfloor + 1$

$Sequence_{IDO}(1 : N) = Chaotic_P(N : 2 \times N)$

$Sequence_{IR}(1 : m \times n) = \lfloor \mathrm{mod}(Chaotic_P(1 + 2 \times N : m \times n + 2 \times N) \times 10^{15}, N)\rfloor + 1$

$min = min(Sequence_{IDO}(1 : N))$;

$max = max(Sequence_{IDO}(1 : N))$;

for i = 1 to N **do**

    $Sequence_{ID}(i) = \left\lceil \frac{\mathrm{Sequence}_{IDO}(i) - min}{max - min} \times (N - 1) + 1 \right\rceil$

end for

for i = 1 to N **do**

    $Sequence_{ID}(i,:)$ = circshift(img1, [0, -(i-1)]);

end for

$K_1(1 : m \times n) = \lfloor(Chaotic_P(m \times n + 2 \times N + 1 : 2 \times m \times n + 2 \times N)\rfloor$

$K_2(1 : m \times n) = \lfloor(Chaotic_P(2 \times m \times n + 2 \times N + 1 : 3 \times m \times n + 2 \times N)\rfloor$

$K_3(1 : m \times n) = \lfloor(Chaotic_P(3 \times m \times n + 2 \times N + 1 : 4 \times m \times n + 2 \times N)\rfloor$

gorithm called Dynamic Polyhedral Permutation (DPP) based on chainsaw scanning algorithm, which will be described in this section.

Step 1 (Polyhedralization): N images $Img1, \ldots, ImgN$ are posed in the shape of a polytope.

Step 2 (Chainsaw Scan): The chainsaw scan is performed on N original images $Img1, \ldots, ImgN$ to obtain N sequences $Line_1, ..., Line_N$ using the $Sequence_{SP}$.

Step 3 (Dynamic arrangement): Based on the value of $Sequence_{IR}(i)$, which determines the specific indexing rule, we select different index patterns in $Matrix_{ID}$, an indexing matrix designed for this purpose to sort the N pixels $Line_1(i), \ldots, Line_N(i)$ with i taking values from 1 to $m \times n$.

Step 4 (Pixels link): After sorting, a 1D sequence $Line_s$ is obtained according to Equation 4.

$$Line_S = \{Line_{S1}(1), ..., Line_{SN}(1), ..., Line_{S1}(m \times n), , ..., Line_{SN}(m \times n)\} \tag{4}$$

Step 5 (Re-polyhedralization): The 1D sequence $Line_S$ is reshaped into N images IMG_{E1}, IMG_{E2}, ..., IMG_{EN}, each maintaining the same dimensions as the original images..

C. Arnold Diffusion algorithm(AD)

Arnold map is commonly used for image permutation [57]. In this paper, we extend the functionality of the Arnold map and develop a diffusion architecture combined with the chaotic system named Arnold diffusion, which can be outlined as follows:

Step 1: N images are converted into a new 1D sequence P.

Step 2: We set the initial parameters using the key values: $a = Key_a$, $b = Key_b$. Then, using parameters a, b and chaotic sequences K_1, K_2, K_3, we perform the proposed Arnold diffusion on P to get the diffused image C, which can be expressed as Equation 5 and Equation 6.

$$\begin{bmatrix} C(1) \\ T(1) \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & a \times b + 1 \end{bmatrix} \times \begin{bmatrix} P(1) \\ K1(1) \end{bmatrix} + \begin{bmatrix} K2(1) \\ K3(1) \end{bmatrix} \tag{5}$$

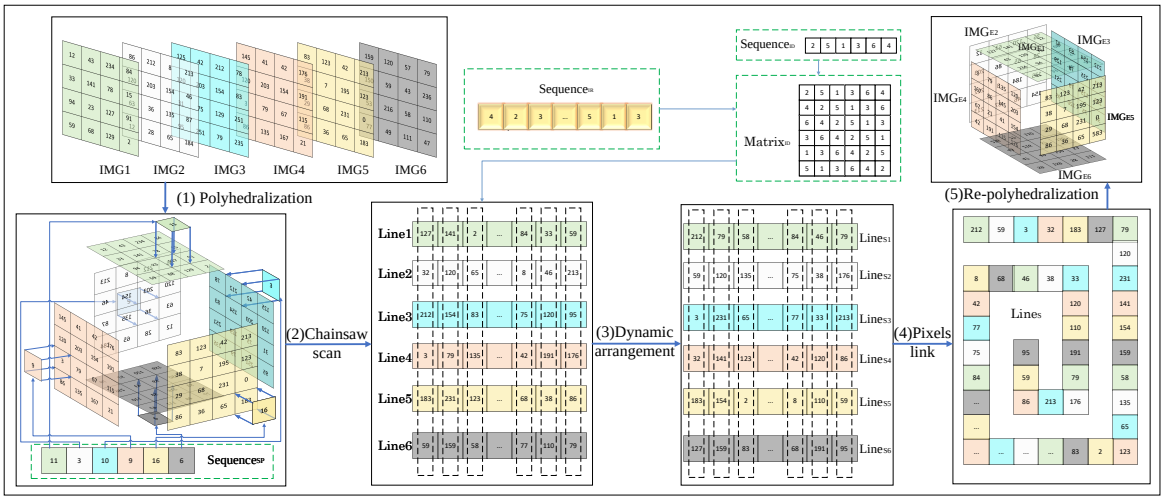


Fig. 3. Illustration of the Dynamic Polyhedra Permutation (DPP) algorithm.

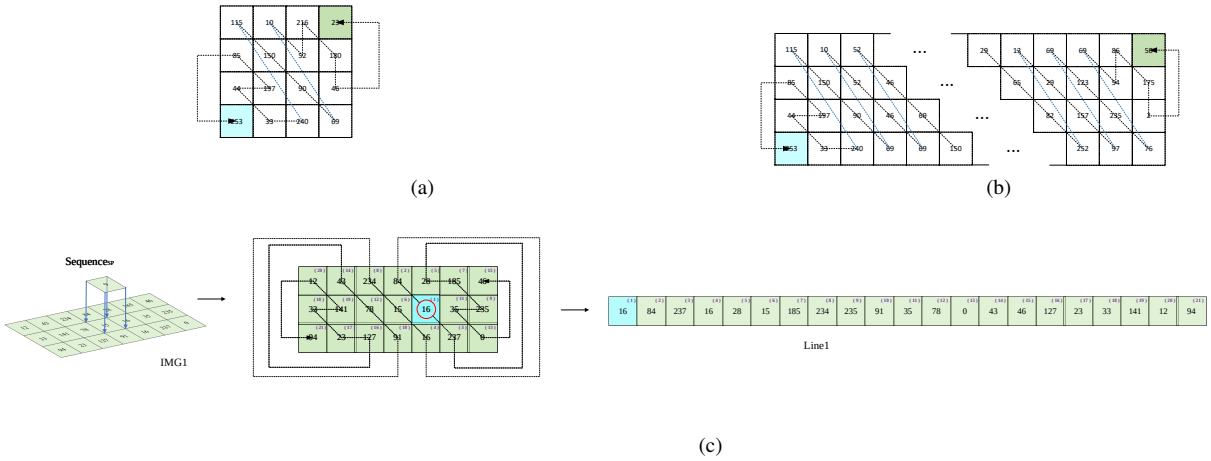


Fig. 4. Visualisation of Chainsaw Scan Algorithm: (a)square images; (b) rectangular images; (c)An example of the Chao-based Chainsaw Scanning Algorithm using a randomized starting point.

$$\begin{cases} S(i) = T(i-1) + P(i) \\ \begin{bmatrix} C(i) \\ T(i) \end{bmatrix} = \left(\begin{bmatrix} 1 & a \\ b & a \times b + 1 \end{bmatrix} \times \begin{bmatrix} S(i) \\ K1(i) \end{bmatrix} + \begin{bmatrix} K2(i) \\ K3(i) \end{bmatrix} \right) \mod 256 \end{cases} \tag{6}$$

where $i \in \{2, 3, ..., N \times m \times n\}$.

Step 3: Using the same chaotic sequences K_1, K_2, K_3 and parameters a, b, we perform the Arnold diffusion again on C inreverse order which can be expressed as Equation 7 and Equation 8.

$$\begin{bmatrix} C1(i) \\ T(i) \end{bmatrix} = \left(\begin{bmatrix} 1 & a \\ b & a \times b + 1 \end{bmatrix} \times \begin{bmatrix} C(i) \\ K1(i) \end{bmatrix} + \begin{bmatrix} K2(i) \\ K3(i) \end{bmatrix} \right) mod \ 256 \tag{7}$$

where $i = N \times m \times n$;

$$\begin{cases} S(n) = T(n-1) + C1(n) \\ \begin{bmatrix} C1(i) \\ T(i) \end{bmatrix} = \left(\begin{bmatrix} 1 & a \\ b & a \times b + 1 \end{bmatrix} \times \begin{bmatrix} S(i) \\ K1(i) \end{bmatrix} + \begin{bmatrix} K2(i) \\ K3(i) \end{bmatrix} \right) mod \ 256 \end{cases} \tag{8}$$

where $i \in \{N \times m \times n - 1, N \times m \times n - 2, ..., 1\}$.

Step 4: Finally, $C1$ is divided into N encrypted images IMG_{G1}, IMG_{G2}, ..., IMG_{GN} of the same size.

D. Decryption scheme of the DPPAD-IE

At the receiving end, the process of decryption works in reverse order compared to encryption. Specifically, the procedures for decrypting DPP and AD are detailed in Algorithm 4 and Algorithm 5, respectively.

Algorithm 2 DPP algorithm

Input: N images $Img_1, Img_2, ..., Img_N$ of size $a \times b$, three sequences $Sequence_{SP}$, $Matrix_{ID}$, and $Sequence_{IR}$.
Output: N images $IMG_{E1}, ..., IMG_{EN}$.

for o = 1 to N **do**
  $(m, n) = (\max(a, b), \min(a, b))$
  if $a > b$ **then**
    $Img_o \leftarrow \text{rot90}(Img_o, 1)$
  end if
  for i = 1 to $\frac{n}{2}$ **do**
    for j = 1 to $4 \times (i-1) + 1$ **do**
      $Line1[(4(i-1)-2)(i-1)/2+j] = Img_o[n - 2(i-1) + \lfloor \frac{j}{2} \rfloor, 2 + \lfloor \frac{j-1}{4} \rfloor \times 2 - (j \mod 2)]$
    end for
  end for
  for i = 1 to $m - n + 1$ **do**
    for j = 1 to n **do**
      $Line2(i) = Img_o(j + (i-1), j)$
    end for
  end for
  for i = $\frac{n}{2}$ to 1 **do**
    for j = 1 to $4 \times (i-1) + 1$ **do**
      $Line3[(4(\frac{n-2}{2} + 1) + 4i + 1) \times (\frac{n-2}{2} + 1 - i)/2 + j] = Img_N[2 + \lfloor \frac{j-1}{4} \rfloor \times 2 - (j \mod 2), (n - 2(i-1) + \lfloor \frac{j}{2} \rfloor) + (m - n)]$
    end for
  end for
  $Line \leftarrow \text{horzcat}(Line1, Line2, Line3)$
  $line\_s1 \leftarrow \text{fliplr}(Line[1 : Sequence_{SP}(N)])$
  $line\_s2 \leftarrow Line[Sequence_{SP}(N) + 1 : N \times N]$
  Interleaving of $line\_s1$ and $line\_s2$ to obtain $line\_p$
end for
for i = 1 to $a \times b$ **do**
  for k = 1 to N **do**
    $Line(N(i\text{-}1) + Matrix_{ID}(Sequence_{IR}(i), N)) = line_p[K](i)$
  end for
end for
$IMG \leftarrow \text{reshape}(Line, a, b \times N)$
Split the IMG into N images $IMG_{E1}, ..., IMG_{EN}$, each of size $a \times b$

Algorithm 3 Diffusion Algorithm

Input: N Images $IMG_{E1}, ..., IMG_{EN}$ of size $m \times n$, chaotic sequences $K1$, $K2$, $K3$, a, b.
Output: N Encrypted images $IMG_{G1}, \ldots, IMG_{GN}$.

$L = m \times n \times N$
$P \leftarrow \text{reshape}([IMG_{E1}, ..., IMG_{EN}], 1, L)$
$C(1) = \text{mod}(1 \times P(1) + a \times K1(1) + K2(1), 256)$
$T(1) = \text{mod}(b \times P(1) + (a \times b + 1) \times K1(1) + K3(1), 256)$
$S(2) = \text{mod}(T(1) + P(2), 256)$
for $i = 2$ to $L - 1$ **do**
  $C(i) = \text{mod}(1 \times S(i) + a \times K1(i) + K2(i), 256)$
  $T(i) = \text{mod}(b \times S(i) + (a \times b + 1) \times K1(i) + K3(i), 256)$
  $S(i + 1) = \text{mod}(T(i) + P(i + 1), 256)$
end for
$C(L) = \text{mod}(1 \times S(L) + a \times K1(L) + K2(L), 256)$
$E(L) = \text{mod}(1 \times C(L) + a \times K1(1) + K2(1), 256)$
$T(L) = \text{mod}(b \times C(L) + (a \times b + 1) \times K1(1) + K3(1), 256)$
$S(L - 1) = \text{mod}(T(L) + C(L - 1), 256)$
for $i = 1$ to $L - 1$ **do**
  $C1(i) = \text{mod}(1 \times P(i) + a \times K1(i) + K2(i), 256)$
  $T(i) = \text{mod}(b \times S(i) + (a \times b + 1) \times K1(i) + K3(i), 256)$
  $S(i + 1) = \text{mod}(T(i) + P(i + 1), 256)$
end for
$C1(L) = \text{mod}(H(1, 1) \times S(L) + H(1, 2) \times K1(L) + K2(L), 256)$
Split the $C1$ into N images $IMG_{G1}, \ldots, IMG_{GN}$, each of size $m \times n$

III. EXPERIMENTAL RESULTS

This part examines the efficiency and security of the introduced cryptosystem. The performance of DPPAD-IE and 2D-CGHM is highlighted in III-B9-III-B16 and III-B1-III-B8, respectively.

In the experimental section analyzing chaos performance, three two-dimensional chaos maps will be used to compare with the 2D-CGHM, aiming to assess its hyperchaotic behavior. Table I presents a comparative analysis of the proposed 2D Cross Gaussian Hyperchaotic Map (2D-CGHM) with three other existing 2D chaotic maps. These include the 2D-trigonometric-map (2D-TM) [17], the 2D hyperchaotic system with a simple structure and complex dynamic behavior (2D-SSCDB) [18], and the cross 2D hyperchaotic map (Cross-2DHM) [19]. Table II displays the mean values of various indicators corresponding to different 2D chaotic maps. For the experimental evaluation of the encryption algorithm, six images labeled as "IMG1", "IMG2", "IMG3", "IMG4", "IMG5", and "IMG6" are chosen. These images are utilized to carry out a comparison between the proposed encryption method and other existing techniques [31], [32], [58], [59], [60], [61], [62], [63], [64] based on various key performance metrics. Table XI presents the comparison results of six images, which indicate that the proposed cryptosystem performs considerably well in many aspects and could defend against different types of attacks.

A. Experimental Setup

During the testing phase, medical images are utilized from two datasets: the Brain Tumors dataset [65] and the Computer-Aided Diagnostic dataset for classifying Chest X-Ray Images Using Deep Ensemble Learning [66]. The Brain Tumors dataset [65] includes 3,264 preprocessed MRI images categorized into benign, malignant, and pituitary tumors. The Computer-Aided Diagnostic dataset [66] combines chest X-ray images of tuberculosis, COVID-19, pneumonia, and healthy cases from the "Tuberculosis Chest X-Ray Database" and "COVID-19 Radiography Database." Images are in PNG format with resolutions of 512 x 512 or 256 x 256. The encryption scheme utilizes keys that are randomly assigned as follows: $Key_{x_1} = -0.1$, $Key_{y_1} = -0.6$, $Key_{x_1'} = -0.6$, $Key_{y_1'} = -0.2$, $Key_{a1} = 20$, $Key_{b1} = 17$, $Key_a = 15$,

Algorithm 4 Decryption Algorithm of the Diffusion Stage

Input: N Encrypted Images $IMG_{G1}, \ldots, IMG_{GN}$ with length L, chaotic sequences $K1$, $K2$, $K3$.
Output: N Images $IMG_{E1}, \ldots, IMG_{EN}$.

$L = m \times n \times N$
$C_d \leftarrow \text{reshape}(IMG_{G1}, \ldots, IMG_{GN}, 1, L)$
$T(L) = \text{mod}(K1(1) + b \times (C_d(L) - K2(1)) + 1 \times K3(1), 256)$
$C(L) = \text{mod}((a \times b+1) \times (C_d(L) - K2(1)) - a \times (T(L) - K3(1)), 256)$
for $n = 1$ to $L - 1$ **do**
  $T(n) = \text{mod}(K1(L+1-n) + b \times (C_d(n) - K2(L+1-n)) + 1 \times K3(L+1-n), 256)$
  $S(n) = \text{mod}((a \times b+1) \times (C_d(n) - K2(L+1-n)) - a \times (T(n) - K3(L+1-n)), 256)$
  $C(n) = \text{mod}(S(n) - T(n+1), 256)$
end for
$T(1) = \text{mod}(K1(1) + b \times (C(1) - K2(1)) + 1 \times K3(1), 256)$
$P(1) = \text{mod}((a \times b+1) \times (C(1) - K2(1)) - a \times (T(1) - K3(1)), 256)$
for $n = 2$ to L **do**
  $t(n) = \text{mod}(K1(n) + b \times (C(n) - K2(n)) + 1 \times K3(n), 256)$
  $S(n) = \text{mod}((a \times b + 1) \times (C(n) - K2(n)) - a \times (t(n) - K3(n)), 256)$
  $P_p(n) = \text{mod}(S(n) - T(n-1), 256)$
end for
Split the P_p into N images $IMG_{E1}, \ldots, IMG_{EN}$, each of size $m \times n$

$Key_b = 24$, and $Key_{N0} = 2000$. For testing, we selected $N = 6$ as the number of original images. Specifically, in the dataset "Viral Pneumonia" [66], six gray-scale images of size 512×512 were used: "IMG1", "IMG2", "IMG3", "IMG4", "IMG5", and "IMG6", correspond to images 1-001, 1-002, 1-003, 1-004, 1-005, and 1-006, respectively. Similarly, six gray-scale images, each with a size of 256×256, were selected from the dataset "glioma_tumor" presented in [65]. These images, labeled as "IMG7", "IMG8", "IMG9", "IMG10", "IMG11", and "IMG12", correspond to images G-1, G-2, G-3, G-4, G-5, and G-6, respectively.

B. Comparative Experiments

This section presents an evaluation of the 2D-CGHM map and the DPPAD-IE algorithms, focusing on III-B1-III-B8 for the 2D-CGHM and III-B9-III-B16 for the DPPAD-IE algorithm.

1) bifurcation and trajectory diagram Analysis: The bifurcation diagram and trajectory diagram could show the dynamic behaviour of a chaotic map. Figure 5 illustrates four bifurcation diagrams in two dimensions and two in three dimensions for 2D-CGHM. These diagrams show that the state values of the 2D-CGHM exhibit a consistently uniform distribution. Additionally, the trajectory diagrams in both 2D and 3D for 2D-CGHM, displayed in Figure 6, indicate that

Algorithm 5 Decryption of DPP algorithm.

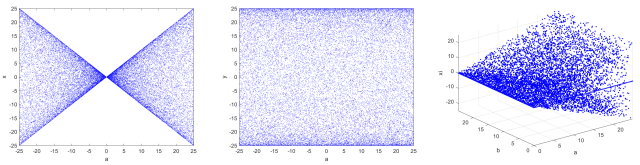
Input: N Encrypted images Img_{E1}..., Img_{EN} of size $a \times b$, three sequences $Sequence_{SP}$, $Matrix_{ID}$, and $Sequence_{IR}$.
Output: N images $Img_1, Img_2, ..., Img_N$.

$Line \leftarrow \text{reshape}([Img1, ..., Imgn], 1, a \times b \times N)$;
for i=1 to $a \times b$ **do**
  for k=1 to N **do**
    $line_p[k](i) = Line(N \times (i-1) + Matrix_{ID}(Sequence_{IR}(i), N))$;
  end for
end for
for $o : 1$ to N **do**
  for $i = 1 tomin(Sequence_{SP}(N), N \times a \times b - Sequence_{SP}(N))$ **do**
    $line_s1(i) = Line(2 \times (i-1) + 1)$;
  end for
  for $i = 1$ to $min(Sequence_{SP}(N), N \times a \times b - Sequence_{SP}(N))$ **do**
    $line_s2(i) = Line(2 \times i)$;
  end for
  Reverse the dynamic interleaving of $line_p$ to restore the original two sequences $line_s1$ and $line_s2$
  $line_s1 = \text{fliplr}(line_s1)$;
  $Line = \text{horzcat}(line_s1, line_s2)$;
  $(m, n) = (\max(a, b), \min(a, b))$
  $Line1 = Line[1 : \frac{m \times n - (m-n+1) \times n}{2}]$
  $Line2 = Line[\frac{m \times n - (m-n+1) \times n}{2} + 1 : \frac{m \times n - (m-n+1) \times n}{2} + (m - n + 1) \times n]$
  $Line3 = Line[\frac{m \times n - (m-n+1) \times n}{2} + (m-n+1) \times n + 1 : \frac{m \times n - (m-n+1) \times}{n} 2 + (m - n + 1) \times n + \frac{m \times n - (m-n+1) \times n}{2}]$
  for $i : 1$ to $\frac{n-2}{2} + 1$ **do**
    for $j : 1$ to $4(i-1) + 1$ **do**
      $Img_o[n - 2(i-1) + \lfloor \frac{j}{2} \rfloor, 2 + \lfloor \frac{j-1}{4} \rfloor \times 2 - (j \mod 2)] = Line1[(4(i-1) - 2)(i-1)/2 + j]$
    end for
  end for
  for $i : 1$ to $m - n + 1$ **do**
    for $j = 1$ to n **do**
      $Img_o[j, j + (i-1)] = Line2[(i-1) \times n + j]$
    end for
  end for
  for $i : \frac{n-2}{2} + 1$ to 1 **do**
    for $j : 1$ to $4(i-1) + 1$ **do**
      $Img_o[2 + \lfloor \frac{j-1}{4} \rfloor \times 2 - (j \mod 2), (n - 2(i-1) + \lfloor \frac{j}{2} \rfloor) + (m - n)] = Line3[(4(\frac{n-2}{2} + 1) + 4i + 1) \times (\frac{n-2}{2} + 1 - i)/2 + j]$
    end for
    if $a < b$ **then**
      $Img_o \leftarrow \text{rot90}(Img_o, -1)$
    end if
  end for
end for

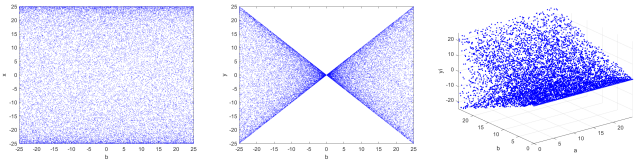
TABLE I
SOME 2D HYPERCHAOTIC MAPS THAT USED IN THE COMPARISON.

Name	F(x, y)	Parameters	Ref
2D-TM	$\begin{cases} x_{n+1} = \sin(\omega x_n) - r\sin(\omega y_n) \\ y_{n+1} = \cos(\omega x_n) \end{cases}$	ω, r	[17]
2D-SSCDB	$\begin{cases} x_{n+1} = \sin(\mu x_n(1-y_n)+1), \\ y_{n+1} = \sin\left(\frac{\eta}{(x_n+y_n)}+1\right) \end{cases}$	μ, η	[18]
Cross-2DHM	$\begin{cases} x_{i+1} = \sin\left(\frac{\alpha}{\sin(y_i)}\right) \\ y_{i+1} = \beta\sin(\pi(x_i+y_i)) \end{cases}$	α, β	[19]
2D-CGHM	$\begin{cases} x_{n+1} = a\sin(e^{y_n^2}+x_n); \\ y_{n+1} = b\cos(e^{x_n^2}+y_n); \end{cases}$	a, b	-

the entry elements are spread evenly across the phase space. This observation confirms that 2D-CGHM exhibits excellent performance regarding trajectory distribution.

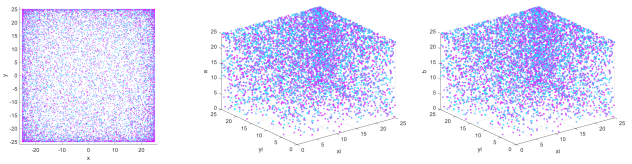


(a) (b) (c)



(d) (e) (f)

Fig. 5. Bifurcation diagrams of the 2D-CGHM: (a) and (b) depict 2D diagrams with b = 25; (d) and (e) depict 2D diagrams with a = 25; (c) and (f) depict 3D diagrams.



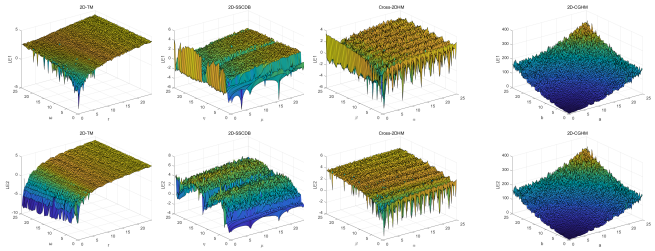
(a) (b) (c)

Fig. 6. Trajectory diagrams: (a) 2D phase space trajectory for a = 25, b = 25; (b) 3D phase space trajectory for a = 25; (c) 3D phase space trajectory for b = 25.

2) Lyapunov exponent test: The Lyapunov exponent, which can be computed using Equation 9, serves as a reliable approach for determining if a nonlinear dynamical system exhibits chaos or hyperchaos.

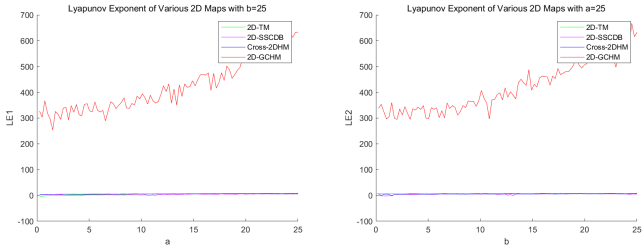
$$LE = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln|f'(x_i)|. \tag{9}$$

The 3D and 2D Lyapunov of different maps are plotted in Figure 7 and Figure 8, respectively. LE1 and LE2 are the Lyapunov exponents of various hyperchaotic maps when the control variables b = 25 and $a \in$ (0,25) or a = 25 and $b \in$ (0,25), respectively. The averages of LE1 and LE2 are shown in Table II. The maximum LEs of 2D-CGHM can reach nearly 300 and is larger than the ones of 2D-TM, 22D-SSCDB, and Cross-2DHM. The excellent performance shows that 2D-CGHM is more competitive because it is highly stochastic.



(a) 2D-TM (b) 2D-SSCDB (c) Cross-2DHM (d) 2D-CGHM

Fig. 7. The three-dimensional Lyapunov exponent for various 2D chaotic maps.



(a) (b)

Fig. 8. The two-dimensional Lyapunov exponent for various 2D chaotic maps is presented: (a) LE1 with a as the control parameter while fixing b = 25; (b) LE2 with b as the control parameter while keeping a = 25.

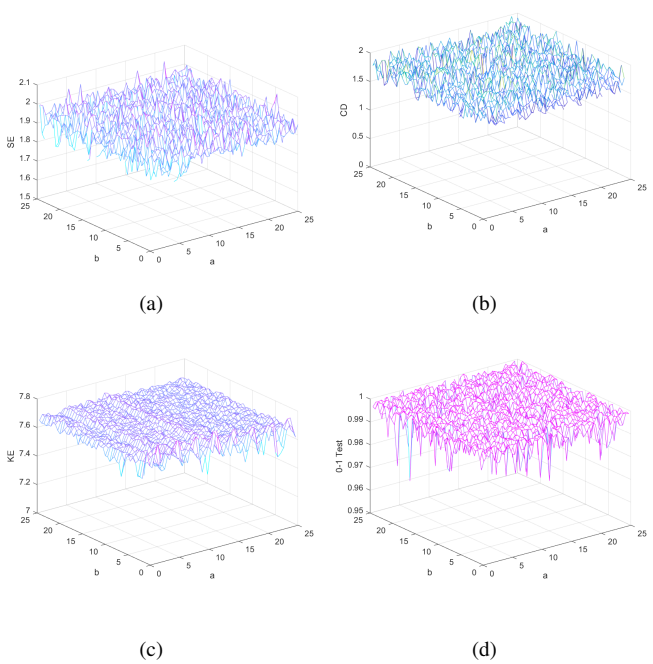
3) Sample entropy: Sample entropy (SE) is a metric commonly employed to evaluate the degree of self-similarity within a chaotic sequence. Its mathematical definition is expressed in Equation 10.

$$SE(m, r, n) = -\log\frac{C}{D} \tag{10}$$

In this formula, C represents the count of vector pairs satisfying $d[Y_m(i), Y_m(j)] < r$, while D denotes the count of vector pairs for which $d[Y_{m+1}(i), Y_{m+1}(j)] < r$. Here, $Y_m(i) = \{Y_i, Y_{i+1}, \ldots, Y_{i+m-1}\}$ represents the template vector with a dimension of m, and r is the maximum allowable tolerance. The term $d[Y_m(i), Y_m(j)]$ refers to the Chebyshev distance between $Y_m(i)$ and $Y_m(j)$, with $m = 2$ and $r = 0.2 \times \mathrm{std}(Y)$. A higher SE value implies reduced regularity in the time series, signifying increased randomness in the dynamical system. A comparative experiment involving SE is depicted in Figure 10(a). The 3D SE plot, which varies based on a and b, is displayed in Figure 9(a). Table II provides the average SE values, showing that the time series generated by 2D-CGHM exhibits greater irregularity.

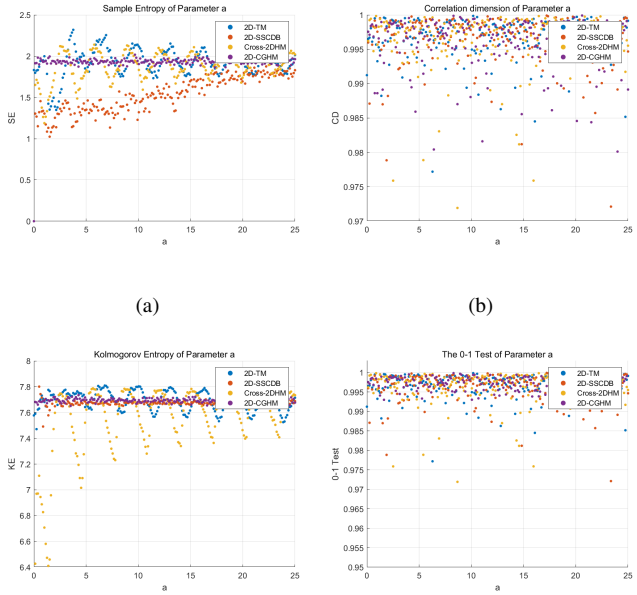
TABLE II
AVERAGE VALUES OF LE1, LE2, SE, 0-1, CD, AND KE FOR 2D-CGHM AND OTHER CHAOTIC MAPS.

Map name	Control Parameters	LE1	LE2	SE	0-1	CD	KE
2D-TM	ω, r	5.0573	1.9086	1.6167	0.9984	1.7695	5.0680
2D-SSCDB	μ, η	3.2324	1.4238	1.5541	0.9978	1.5899	3.3828
Cross-2DHM	α, β	3.2324	1.4238	1.5541	0.9978	1.5899	3.3828
2D-CGHM	a, b	349.7154	356.6653	1.9304	0.9995	1.8039	7.7017



(a) (b) (c) (d)

Fig. 9. 3D Chaos indicators of 2D CGHM map: (a) SE, (b) CD, (c) KE, (d) 0-1 Test.



(a) (b) (c) (d)

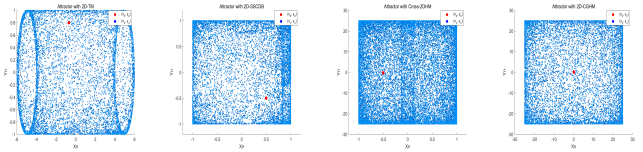
Fig. 10. Comparative chaos indicator plot: (a) SE, (b) CD, (c) KE, (d) 0-1 Test. (a is set as the control parameter and b = 25).

4) Attractor trajectory: The trajectory of the attractor acts as a straightforward approach for observation. In chaotic systems, randomness in the outputs of state variables can be noticed when the attractor's motion covers a broad range and exhibits a uniform distribution. Here, the control parameters were set to $a = 25$ and $b = 25$, with initial state variable values defined as $x_0 = 0.5$ and $y_0 = 0.5$. Then the 2D-CGHM underwent 40,000 iterations under these conditions. Figure 11 illustrates that the attractor trajectories corresponding to the x and y sequences display intricate geometric patterns, covering a substantial portion of the phase space.

5) Correlation dimension: The Correlation Dimension (CD) is frequently used to quantify the complexity or irregularity of an attractor within a dynamic system. Represented by Equation 11, the CD is characterized through the correlation integral, denoted as $Ce(r)$.

$$CD = \lim_{r\to 0} \lim_{M\to\infty} \frac{\log C_e(r)}{\log r} \tag{11}$$

A higher value of CD indicates that the time series occupies a higher dimensionality in the phase space. The 3D visualization and average value of CD are presented in Figure 9(b) and Table II respectively. A comparison of the CD values between the proposed 2D-CGHM and other 2D chaotic maps



(a) 2D-TM (b) 2D-SSCDB (c) Cross-2DHM (d) 2D-CGHM

Fig. 11. Attractors of various two-dimensional chaotic maps

is illustrated in Figure 10(b). It is evident that the dynamic behavior of the proposed 2D-CGHM is notably rich and diverse.

6) Kolmogorov entropy: The Kolmogorov entropy (KE), representing the evolution of states within a dynamical system, can be mathematically expressed as shown in equation 12.

$$K = -\lim_{n\to\infty} \lim_{\varepsilon\to 0} \lim_{\tau\to 0} \frac{1}{n\tau} \sum_{i_0,i_1,\ldots,i_n} p\left(i_1,\ldots,i_n\right) \ln\left[p\left(i_1,\ldots,i_n\right)\right] \tag{12}$$

The KE test partitions the n-dimensional phase space into several boxes $(i_0, i_1, \ldots, i_n)$ with a size of ε. In this context, n indicates the dimensionality of the embedding space, τ represents the temporal delay, and $p(i_1, \ldots, i_n)$ signifies the joint probability. This probability describes the system's trajectory

being located in i_0 at the initial time and in i_n after a delay of $n\tau$.

A positive KE value signifies that more information is necessary for precise trajectory prediction. Additionally, a higher KE value signifies increased unpredictability of the power system. Figure 9(c) and Figure 10(c) illustrate, respectively, the 3D visualization involving a and the comparison of KE with a and b. According to Table II, the average KE value and its standard deviation for 2D-CGHM are reported as 319.225934 and 3.066949, respectively. Therefore, the distribution of KE values is tightly clustered around the mean.

7) 0-1 Test: The 0-1 test provides a reliable binary approach to determine the chaotic nature of a system. The sequence-averaged square difference and its growth rate can be calculated using equations (15) and (16), respectively. In these equations, c is a constant within the range $(0, 2\pi)$, and ϕ represents the chaotic sequence.

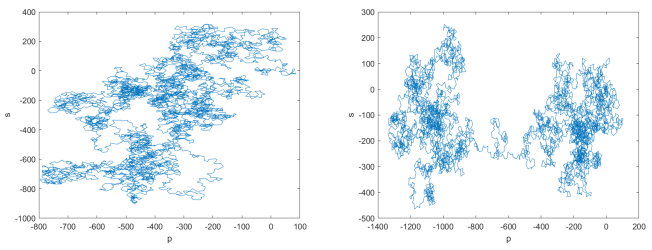
$$p(n+1) = p(n) + \phi(n)\cos(cn) \tag{13}$$

$$s(n+1) = s(n) + \phi(n)\sin(cn) \tag{14}$$

$$M(n) = \lim_{N\to\infty} \frac{1}{N} \sum_{j=1}^{N} \left([p(j+n) - p(j)]^2 + [s(j+n) - s(j)]^2 \right) \tag{15}$$

$$K = \lim_{n=\infty} \frac{\log M(n)}{\log n} \tag{16}$$

A system's dynamics are recognized as chaotic if K approaches 1, whereas they are considered regular when K nears 0. By setting a = 25, b = 25, x_0 = 0.5, and y_0 = 0.5, we generated the test result for the (p, s) diagram, as depicted in Figure 12. In Figure 10(d), the 0-1 analysis for the 2D-CGHM map is compared with other 2D chaotic maps, with corresponding average values summarized in Table II. Additionally, Figure 9(d) displays a three-dimensional 0-1 test graph, illustrating the variations in a and b. From these results, it is observed that the sequence trajectories resemble Brownian motion, confirming that the 2D-CGHM map exhibits chaotic properties.



(a) (b)

Fig. 12. The 0-1 test result of 2D-CGHM.

TABLE III
NIST TEST RESULTS OF 2D-CGHM.

Test index	$P-$value of x sequence	$P-$value of y sequence	Pass
Frequency	0.4749	0.0757	2/2
BlockFrequency	0.8513	0.6163	2/2
Cumulative Sums	0.3838	0.5151	2/2
Runs	0.2896	0.8513	2/2
Longest Run	0.0805	0.0628	2/2
Binary Matrix Rank	0.2133	0.3504	2/2
Discrete Fourier Transform	0.1916	0.1223	2/2
Non-overlapping Template	0.6355	0.5475	2/2
Overlapping Template	0.1153	0.4943	2/2
Maurers Universal Statistical	0.8165	0.8831	2/2
Approximate Entropy	0.0456	0.3041	2/2
Random Excursions	0.4731	0.2750	2/2
Random Excursions Variant	0.5491	0.4318	2/2
Serial Test	0.4620	0.7756	2/2
Linear Complexity Test	0.4283	0.9114	2/2

8) NIST SP 800-22 test: The evaluation conducted by the National Institute of Standards and Technology (NIST) involves fifteen unique test categories in total. To achieve validation, the P-values for these tests must exceed the threshold of 0.01. The outcomes of the NIST SP 800-22 assessments are displayed in Table III. It is evident that the 2D-CGHM has successfully met the requirements for all randomness tests.

9) Historgeam analysis: The outcomes of the encryption simulation, combined with the associated histogram analysis, are illustrated in Figure 13. It is clear that the pixel values of the original image have been completely concealed, while the histogram of the encrypted image demonstrates a uniform pattern. Additionally, the quality of encryption is evaluated using the peak signal-to-noise ratio (PSNR), which is described by equations (18) and (17).

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}} \sum_{\mathrm{i}=1}^{\mathrm{M}} \sum_{\mathrm{j}=1}^{\mathrm{N}} |\mathrm{PI}\,(\mathrm{i},\mathrm{j}) - \mathrm{CI}(\mathrm{i},\mathrm{j})|^2 \tag{17}$$

$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right)(\mathrm{db}) \tag{18}$$

The plaintext image (PI) and the cipher image (CI) are denoted as such. A lower PSNR value implies a higher encryption quality. As shown in Table V, the PSNR metrics for various images indicate that the proposed method achieves outstanding encryption performance.

10) Information entropy analysis: Information entropy (IE) is an essential measure used to evaluate the randomness and disorder present in an image. From a mathematical perspective, IE is defined in equation (19), where $p(m_i)$ denotes the probability corresponding to a specific grey value m_i.

$$H(m) = \sum_{i=0}^{255} p(m_i)\log_2 \frac{1}{p(m_i)} \tag{19}$$

For a grayscale image having 256 intensity levels, the optimal entropy value $H(m)$ should be 8. Table IV shows that the computed entropy values for the encrypted images are close to 8, indicating a high level of randomness in the encrypted images. Consequently, it validates the effectiveness

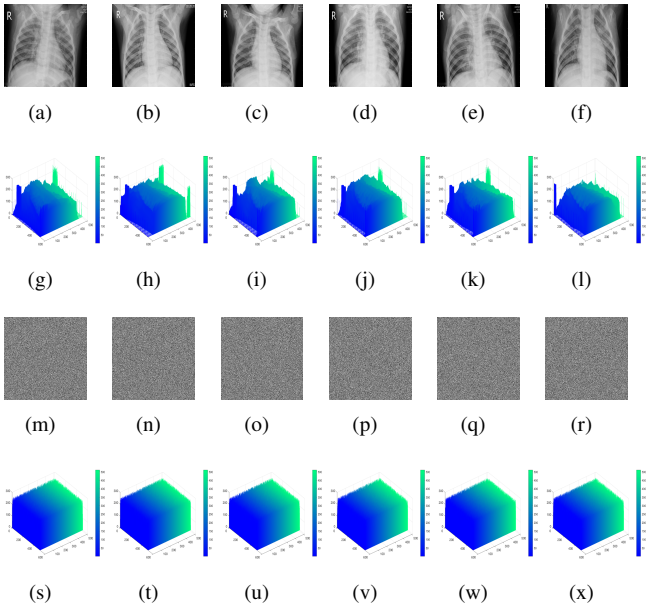


Fig. 13. The encryption simulation results and histograms of six medical images: (a)-(f) original images; (g)-(l) the histograms of (a)-(f); (m)-(r) the cipher images of (a)-(f); (s)-(x) the histograms of (m)-(r).

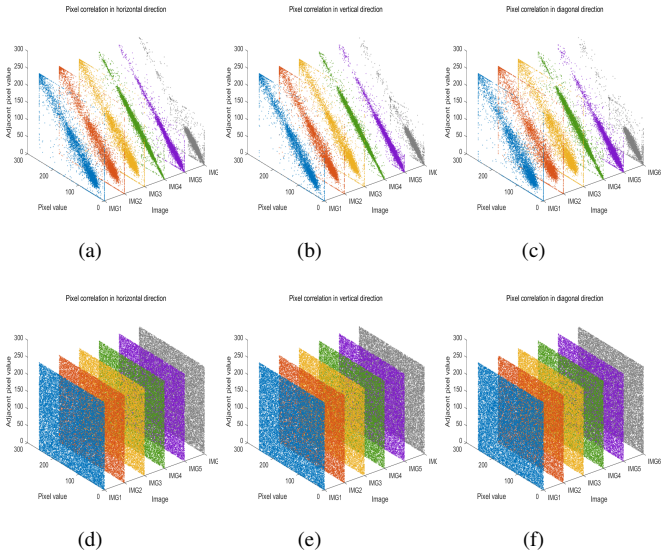


Fig. 14. Correlation analysis: the correlation of the original images in three directions: (a) Horizontal, (b) Vertical, (c) Diagonal; the correlation of the corresponding encrypted images in three directions: (a) Horizontal, (b) Vertical, (c) Diagonal.

of the proposed encryption system in resisting entropy-based cryptanalytic attacks.

11) Correlation between neighboring pixels: Encrypted images should present a low correlation between neighboring pixels to prevent cryptoanalysts from leveraging these correlations for attacks. Correlation analysis is frequently applied to evaluate relationships in various directions. Figure 14 presents the correlation plots for six images alongside their respective cipher images. To evaluate the correlation coefficient between neighboring pixels, the following set of formulas can be applied:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{20}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)^2 \tag{21}$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big) \tag{22}$$

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{23}$$

Here, x and y represent pixel intensities of two adjacent pixels in three different directions. The total number of neighboring pixel pairs is denoted by M. Additionally, the correlation coefficients of six medical images were computed both prior to and following encryption, with the results presented in Table 14.

12) Structural similarity index analysis: The similarity between two images is commonly assessed using the structural similarity index metric (SSIM), as described in equation (24).

$$SSIM(A,B) = \frac{(2\mu_x\mu_y + X)(2\delta_{xy} + Y)}{(\mu_x^2 + \mu_y^2 + X)(\delta_x^2 + \delta_y^2 + Y)} \tag{24}$$

In this context, $X = (k_1 L)^2$ and $Y = (k_2 L)^2$, where k_1 and k_2 are assigned values of 0.01 and 0.03, respectively. The variable L corresponds to the dynamic range of the pixel values. The symbols μ_x and μ_y refer to the average pixel intensities for images A and B, respectively, while δ_x^2 and δ_y^2 indicate their standard deviations. Additionally, δ_{xy} represents the covariance between these two images. As presented in Table V, the SSIM values confirm that the proposed cryptosystem provides excellent encryption performance.

13) Key space analysis: The effectiveness of a cryptosystem in resisting brute-force attacks depends significantly on the size of its key space. The ranges of the keys are defined as follows: $Key_{x1} \in (-1,1)$, $Key_{y1} \in (-1,1)$, $Key_{x2} \in (-1,1)$, $Key_{y2} \in (-1,1)$, $Key_{a1} \in (0,25)$, $Key_{b1} \in (0,\infty)$, $Key_{a2} \in (0,25)$, $Key_{b2} \in (0,25)$, $Key_a \in (0,\infty)$, $Key_b \in (0,\infty)$, and $Key_{N0} \in (1000,2000)$. Consequently, the key space can be considered infinite, which ensures that our cryptosystem possesses strong defenses against brute-force attacks.

14) Sensitivity analysis: To defend against chosen plaintext and differential attacks, an encryption system needs to demonstrate high sensitivity to both the keys and the plaintext images. In a strong encryption framework, even slight modifications in the keys or plain image pixel values must cause substantial variations in the corresponding encrypted images. Metrics frequently used to assess sensitivity include the number of pixels change rate (NPCR) and the unified average change intensity (UACI), which are specified in Equation 25. For these

TABLE IV
CORRELATION COEFFICIENTS AND INFORMATION ENTROPY ANALYSIS.

Images	Plain images				Encrypted images			
	V	H	D	IE	V	H	D	IE
IMG1	0.9959	0.9959	0.9917	2.8123	0.0060	-0.0071	0.0428	7.9993
IMG2	0.9898	0.9945	0.9925	2.8123	-0.0064	0.0009	-0.0040	7.9993
IMG3	0.9925	0.9967	0.9920	4.7816	-0.0039	0.0054	0.0015	7.9994
IMG4	0.9858	0.9897	0.9741	3.8817	-0.0072	-0.0037	0.0044	7.9993
IMG5	0.9853	0.9926	0.9772	3.7612	0.0020	0.0053	0.0061	7.9993
IMG6	0.9815	0.9869	0.9778	3.4769	-0.0061	-0.0060	0.0009	7.9993

TABLE V
THE RESULTS OF SSIM AND PSNR TESTS FOR DIFFERENT IMAGES.

Metrics	Encrypted images					
	IMG1	IMG2	IMG3	IMG4	IMG5	IMG6
SSIM	0.0141	0.0121	0.0109	0.0111	0.0094	0.0092
PSNR	8.4012	8.4376	8.4362	8.1931	8.2785	8.4336

indicators, the optimal values are 33.4635% and 99.6094%, respectively.

$$\begin{cases} NPCR = \sum_{i=0}^{H}\sum_{j=0}^{W} D(i,j) \times 100\% \\ UACI = \frac{1}{W \times H}\sum_{i=0}^{H}\sum_{j=0}^{W} \frac{|E1(i,j) - E2(i,j)|}{255} \times 100\% \end{cases} \tag{25}$$

In this context, $E1$ and $E2$ refer to two encrypted images, while $D(i,j)$ is defined as:

$$D(i,j) = \begin{cases} 0, & \text{if } E1(i,j) = E2(i,j) \\ 1, & \text{if } E1(i,j) \neq E2(i,j) \end{cases}.$$

The variables W and H correspond to the image's width and height, respectively. The sensitivity of plaintext and keys is evaluated using NPCR and UACI through the following methodology:

Step 1: We encrypt the six original images using unmodified keys to obtain six images $V_1, V_2, V_3, V_4, V_5, V_6$.

Step 2: A minor modification is made to one key, as shown in Table VI, and this altered key is applied to encrypt the same set of original images, resulting in six new images: $V_1', V_2', V_3', V_4', V_5', V_6'$.

Step 3: We change a pixel in one plaintext image at random and get the resulting encrypted images $V_1'', V_2'', V_3'', V_4'', V_5'', V_6''$ by using the unchanged keys.

Step 4: The analysis results of NPCR and UACI, which assess the sensitivities to secret keys and plaintexts, are computed and shown in Table VII and Table VIII, respectively. These results indicate that the NPCR and UACI values closely align with their theoretical expectations. As a result, the algorithm exhibits remarkable responsiveness to changes in both the plaintext and the key, thereby providing robust defense against attacks such as differential and chosen plaintext.

TABLE VI
SECRET KEYS AND THE CORRESPONDING CHANGED VALUES.

Item	x_1	y_1	a_1	b_1	a	b	N_0
The changed values	10^{-15}	10^{-15}	10^{-15}	10^{-15}	1	2	1

15) Encryption time analysis: An effective encryption system ought to operate at a high speed. To assess the performance of our cryptographic scheme, we make use of color and grayscale images of varying dimensions. After running 200 times, the average time required is obtained. The encryption time analysis results are shown in Table IX, which indicates that our cryptosystem has a high encryption efficiency.

16) Robustness analysis: To guarantee strong security, an image encryption algorithm must demonstrate resistance against both noise and occlusion attacks. In this section, we utilize medical images labeled "IMG1," "IMG2," "IMG3," "IMG4," "IMG5," and "IMG6" to evaluate the proposed cryptosystem's robustness. Figure 15 provides a detailed breakdown of the results, illustrating that, despite the presence of noise and occlusion in the encrypted images, the decrypted outputs remain visually identifiable. Furthermore, the PSNR and SSIM between the plain images and noised decrypted images are computed using equation (18) and equation (24), respectively. The corresponding results are presented in Table X. Hence, our encryption method is robust enough to resist noise attacks and cropping attacks.

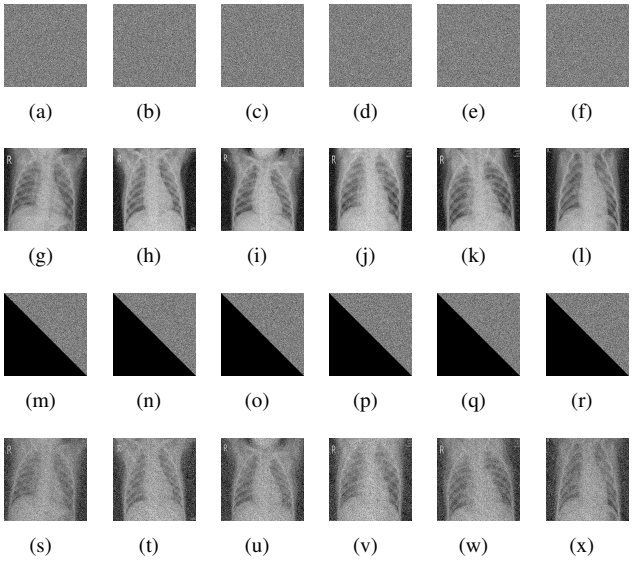


Fig. 15. Robustness analysis results: (a)-(f) the encrypted images added after 0.3 Salt & Pepper noise; (g)-(l) the decrypted images corresponding to (a)-(f); (m)-(r) the encrypted images with 50% data loss; (s)-(x) the corresponding decrypted images of (m)-(r);

TABLE VII
KEY SENSITIVITY ANALYSIS RESULT.

Image	Metrics	x_1	y_1	a_1	b_1	a	b	$N0$
IMG1	NPCR	99.6086	99.5917	99.6079	99.6093	99.6092	99.6094	99.6096
	UACI	33.4703	33,4742	33.4681	33,4642	33.4678	33.4692	33.4639
IMG2	NPCR	99.6092	99.6123	99.6089	99.6092	99.6111	99.6090	99.6089
	UACI	33,4685	33.4720	33.4690	33.4700	33.4642	33.4666	33.4664
IMG3	NPCR	99.6097	99.6087	99.6092	99.6104	99.6108	99.6089	99.6102
	UACI	33.4746	33.4712	33.4706	33.4682	33.4695	33.4657	33.4700
IMG4	NPCR	99.6101	99.6093	99.6103	99.6097	99.6083	99.6091	99.6113
	UACI	33.4656	33.4629	33.4694	33.4669	33.4653	33.4670	33.4676
IMG5	NPCR	99.6099	99.6106	99.6093	99.6087	99.6100	99.6095	99.6097
	UACI	33.4670	33.4666	33.4694	33.4659	33.4678	33.4650	33.4676
IMG6	NPCR	99.6099	99.6101	99.6091	99.6096	99.6094	99.6107	99.6100
	UACI	33.4671	33.4674	33.4659	33.4664	33.4666	33.4667	33.4672

TABLE VIII
PLAINTEXT SENSITIVITY ANALYSIS RESULTS.

Image	Metrics	Change in IMG1	Change in IMG2	Change in IMG3	Change in IMG4	Change in IMG5	Change in IMG6
IMG1	NPCR	99.7758	99.7312	99.7065	99.7796	99.7678	99.8013
	UACI	33.4761	33.4718	33.4842	33.4731	33.4706	33.4679
IMG2	NPCR	99.7324	99.7845	99.8036	99.6890	99.8345	99.7669
	UACI	33.4746	33.4633	33.4712	33.4751	33.4763	33.4743
IMG3	NPCR	99.7596	99.7734	99.7129	99.8321	99.7827	99.6958
	UACI	33.4651	33.4722	33.4760	33.4719	33.4719	33.4676
IMG4	NPCR	99.6798	99.7315	99.7542	99.8021	99.6837	99.8164
	UACI	33.4718	33.4724	33.4721	33.4753	33.4742	33.4743
IMG5	NPCR	99.7793	99.7489	99.8024	99.7365	99.8123	99.6789
	UACI	33.4715	33.4675	33.4835	33.4733	33.4710	33.4749
IMG6	NPCR	99.6812	99.7321	99.8045	99.7534	99.6765	99.8123
	UACI	33.4752	33.4673	33.4760	33.4758	33.4775	33.4811

TABLE IX
ENCRYPTION TIME (SECONDS).

Size	Images	
	Six images	One image Average
512×512	0.8432	0.1404
256×256	0.2132	0.1065

TABLE X
THE PSNR AND SSIM VALUES RESULTS.

Type of Noise	density	PSNR	SSIM
Salt & Pepper	1×10^{-5}	54.2854	0.9991
	5×10^{-5}	48.2577	0.9956
	7×10^{-5}	47.1625	0.9939
Speckle	1×10^{-5}	11.7011	0.0205
	5×10^{-5}	9.4565	0.0068
	7×10^{-5}	9.3040	0.0063
Gaussian	1×10^{-5}	9.3164	0.0076
	5×10^{-5}	8.8932	0.0039
	7×10^{-5}	8.8394	0.0032

C. Ablation study

To comprehensively analyze the proposed DPPAD-IE, we conduct ablation studies on its three modules, including Dynamic Polyhedra Permutation, Arnold Diffusion, and 2D-CGHM. Here, we predominantly perform ablation studies for four specific cases, detailed as follows: (1) Case1: The DPPAD-IE does not include the Arnold Diffusion module. During encryption, only the pixel positions of the original image are altered, while their pixel values remain unaffected. (2) Case2: The DPPAD-IE does not include the DPP. During encryption, the pixel positions in the original image are retained., but their values are modified. (3) Case3: The DPPAD-IE does not include the 2D-CGHM module. We only use a regular 1D logistic chaotic map to generate chaotic sequences. (4) Case4: The DPPAD-IE include all three modules. The results of the ablation experiment using the IMG1, IMG2, IMG3, IMG4, IMG5, and IMG6 as an example are shown in Table XII, it is evident that only the encrypted images generated under Case 4 (the proposed DPPAD-IE) satisfy all performance metrics. To sum up, the results of the ablation study demonstrate that the DPPAD-IE with three modules, achieves a more effective encryption performance.

IV. CONCLUSION

Current multi-image encryption methods have several limitations, including the lack of security and inefficiency of substitution and diffusion algorithms, and the insensitivity of chaotic mapping, making them unsuitable for applications that require real-time encryption or resource-constrained environments. Therefore, in this study, we introduce a unique 2D hyperchaotic system and evaluates its performance through various tests, such as the Lyapunov exponent and Kolmogorov entropy, highlighting its enhanced chaotic properties in contrast to existing 2D chaotic systems. A permutation approach named DPP, is developed to minimize the high correlation often observed between neighboring pixels in medical images. Additionally, the Arnold map is applied to construct an innovative diffusion algorithm, Arnold Diffusion, aimed at enhancing plaintext sensitivity. Leveraging the 2D-CGHM system, this work introduces a lightweight multi-image encryption method called DPPAD-IE, which integrates 2D-CGHM, DPP, and

TABLE XI
COMPARING COEFFICIENTS OF CORRELATION SCHEMES OF ONE IMAGE.

Algorithm	Correlation coefficients			Information entropy	time(s)	NPCR	UACI	Key space
	H	V	D					
Proposed	**0.0006**(↓)	**-0.0010**(↓)	**0.0016**(↓)	**7.9993** (↑)	**0.2839**(↓)	**99.6099**(*)	**33.4641**(*)	∞(↑)
[31]	-0.0094	-0.0031	0.0090	7.9988	2.1017	99.6107	33.4212	2^{407}
[32]	-0.0007	-0.0014	0.0005	7.9993	0.4212	99.6338	33.4303	2^{145}
[58]	-0.0011	0.0021	-0.0011	7.9992	3.8264	99.6062	33.4711	2^{199}
[59]	-0.0006	0.0036	-0.0016	7.9978	0.3077	99.6171	33.5426	2^{126}
[60]	0.0026	0.0075	0.0031	7.9015	3.3449	99.6067	33.4367	2^{180}
[61]	-0.0019	-0.0066	0.0031	7.9992	1.2972	99.6101	33.4509	2^{286}
[62]	0.0002	-0.0017	0.0020	7.9984	0.6011	99.6002	33.4454	2^{348}
[63]	0.0024	0.0011	0.0021	7.9971	1.4890	99.6554	33.4665	2^{124}
[64]	0.0145	0.0115	0.0087	7.9992	3.0901	99.6010	33.4389	2^{115}

(*This value is closest to the ideal value)

TABLE XII
COMPARING COEFFICIENTS OF CORRELATION SCHEMES OF ONE IMAGE.

Case	2D-CGHM	DPP	AD	Correlation coefficients			Information entropy	time(s)	NPCR	UACI	Key space
				H	V	D					
Case1	✓	✓		0.0039	-0.0026	-0.0069	7.2961	**0.0818**(↓)	0.0000	0.0000	0
Case2	✓		✓	-0.0104	0.0030	-0.0010	7.9992	0.2182	99.6081	33.4650	∞(↑)
Case3		✓	✓	0.0007	-0.0017	0.0021	7.9992	0.2828	99.6086	33.4661	∞(↑)
Case4	✓	✓	✓	**0.0006**(↓)	**-0.0010**(↓)	**0.0016**(↓)	**7.9993** (↑)	0.2839	**99.6094**(*)	**33.4641**(*)	∞(↑)

(*This value is closest to the ideal value)

Arnold Diffusion. Comprehensive experimental evaluations indicate that the designed cryptosystem excels in both security and efficiency, which makes it particularly well-suited for applications requiring real-time encryption or resource-constrained environments. In future research, efforts will be directed towards enhancing the encryption algorithm by leveraging parallel computing to minimize computational overhead. Based on this, we will apply our algorithm to medical consumer electronic devices, including wearable medical diagnostic devices and multimedia of smart devices, to achieve secure real-time transmission of sensitive data, promoting the in-depth development of medical consumer electronic devices in practical applications.

REFERENCES

[1] M. Ragab, F. Abukhodair, A. A.-M. AL-Ghamdi, S. Shabanah, B. Alfasi, and M. Alyamani, "Synergizing remora optimization algorithm and transfer learning for visual places recognition in intelligent transportation systems and consumer electronics," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3731–3739, 2024.

[2] X. Guo, X. Chen, S. Luo, S. Wang, and C.-M. Pun, "Dual-hybrid attention network for specular highlight removal," in *ACM MM*, 2024, pp. 10 173–10 181.

[3] X. Guo, X. Chen, S. Wang, and C.-M. Pun, "Underwater image restoration through a prior guided hybrid sense approach and extensive benchmark analysis," *IEEE Transactions on Circuits and Systems for Video Technology*, 2025.

[4] J. Yang, G. Huang, Y. Luo, X. Zhang, X. Yuan, X. Chen, C.-M. Pun, and M.-y. Cai, "Tcia: A transformer-cnn model with illumination adaptation for enhancing cell image saliency and contrast," *IEEE Transactions on Instrumentation and Measurement*, 2025.

[5] X. Guo, Y. Dong, X. Chen, W. Chen, Z. Li, F. Zheng, and C.-M. Pun, "Underwater image restoration via polymorphic large kernel cnns," *arXiv preprint arXiv:2412.18459*, 2024.

[6] X. Li, G. Huang, L. Cheng, G. Zhong, W. Liu, X. Chen, and M. Cai, "Cross-domain visual prompting with spatial proximity knowledge distillation for histological image classification," *Journal of Biomedical Informatics*, p. 104728, 2024.

[7] Z. Zhou, Y. Lei, X. Chen, S. Luo, W. Zhang, C.-M. Pun, and Z. Wang, "Docdeshadower: Frequency-aware transformer for document shadow removal," pp. 2468–2473, 2024.

[8] K.-C. Choi and C.-M. Pun, "High capacity digital audio reversible watermarking," in *2013 IEEE International Conference on Computational Intelligence and Cybernetics (CYBERNETICSCOM)*, 2013, pp. 72–75.

[9] F. Zheng, X. Chen, W. Liu, H. Li, Y. Lei, J. He, C.-M. Pun, and S. Zhou, "Smaformer: Synergistic multi-attention transformer for medical image segmentation," in *BIBM*, 2024.

[10] Y. Wu, L. Zhang, S. Berretti, and S. Wan, "Medical image encryption by content-aware dna computing for secure healthcare," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 2089–2098, 2022.

[11] K.-C. Choi and C.-M. Pun, "Difference expansion based robust reversible watermarking with region filtering," in *2016 13th International Conference on Computer Graphics, Imaging and Visualization (CGiV)*, 2016, pp. 278–282.

[12] S. Rani, D. Gupta, S. Garg, M. J. Piran, and M. S. Hossain, "Consumer electronic devices: Evolution and edge security solutions," *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 15–20, 2021.

[13] X. Wang and Y. Wang, "Multiple medical image encryption algorithm based on scrambling of region of interest and diffusion of odd-even interleaved points," *Expert Systems with Applications*, vol. 213, p. 118924, 2023.

[14] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," *Optics and Lasers in Engineering*, vol. 90, pp. 146–154, 2017.

[15] H. Saeed, T. O. Diab, M. Elsisi *et al.*, "Chaotic maps in cryptography," in *2024 International Telecommunications Conference (ITC-Egypt)*. IEEE, 2024, pp. 635–645.

[16] Y. Zhou, L. Bao, and C. P. Chen, "A new 1d chaotic system for image encryption," *Signal processing*, vol. 97, pp. 172–182, 2014.

[17] N. Tsafack, S. Sankar, B. Abd-El-Atty, J. Kengne, K. Jithin, A. Belazi, I. Mehmood, A. K. Bashir, O.-Y. Song, and A. A. Abd El-Latif, "A new chaotic map with dynamic analysis and encryption application in internet of health things," *IEEE Access*, vol. 8, pp. 137 731–137 744, 2020.

[18] Y. Hu and L. Nan, "A novel 2d hyperchaotic with a complex dynamic behavior for color image encryption." *Computers, Materials & Continua*, vol. 74, no. 3, 2023.

[19] L. Teng, X. Wang, F. Yang, and Y. Xian, "Color image encryption based on cross 2d hyperchaotic map using combined cycle shift scrambling and selecting diffusion," *Nonlinear Dynamics*, vol. 105, pp. 1859–1876, 2021.

[20] J. Zheng and L. Liu, "Novel image encryption by combining dynamic

dna sequence encryption and the improved 2d logistic sine map," *IET image processing*, vol. 14, no. 11, pp. 2310–2320, 2020.
[21] L. Teng, X. Wang, and Y. Xian, "Image encryption algorithm based on a 2d-clss hyperchaotic map using simultaneous permutation and diffusion," *Information Sciences*, vol. 605, pp. 71–85, 2022.
[22] Z. Zhu and H. Leung, "Identification of linear systems driven by chaotic signals using nonlinear prediction," *IEEE transactions on circuits and systems I: fundamental theory and applications*, vol. 49, no. 2, pp. 170–180, 2002.
[23] Z. Hua, Y. Chen, H. Bao, and Y. Zhou, "Two-dimensional parametric polynomial chaotic system," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 7, pp. 4402–4414, 2021.
[24] S. Zhang and L. Liu, "Generation of ideal chaotic sequences by reducing the dynamical degradation of digital chaotic maps," *Soft Computing*, vol. 28, no. 5, pp. 4471–4487, 2024.
[25] M. Li, M. Wang, H. Fan, K. An, and G. Liu, "A novel plaintext-related chaotic image encryption scheme with no additional plaintext information," *Chaos, Solitons & Fractals*, vol. 158, p. 111989, 2022.
[26] D. Li, J. Li, X. Di, and B. Li, "Design of cross-plane colour image encryption based on a new 2d chaotic map and combination of ecies framework," *Nonlinear Dynamics*, vol. 111, no. 3, pp. 2917–2942, 2023.
[27] W. Xingyuan, Z. Junjian, and C. Guanghui, "An image encryption algorithm based on zigzag transform and ll compound chaotic system," *Optics & Laser Technology*, vol. 119, p. 105581, 2019.
[28] X. Wang and H. Sun, "A chaotic image encryption algorithm based on zigzag-like transform and dna-like coding," *Multimedia Tools and Applications*, vol. 78, no. 24, pp. 34 981–34 997, 2019.
[29] A. Jolfaei, A. Vizandan, and A. Mirghadri, "Image encryption using hc-128 and hc-256 stream ciphers," *International Journal of Electronic Security and Digital Forensics*, vol. 4, no. 1, pp. 19–42, 2012.
[30] P. Rashmi and M. Supriya, "Optimized chaotic encrypted image based on continuous raster scan method," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 589–593, 2021.
[31] Z. Tang, Y. Yang, S. Xu, C. Yu, X. Zhang *et al.*, "Image encryption with double spiral scans and chaotic maps," *Security and Communication Networks*, vol. 2019, 2019.
[32] Q. Wang, X. Zhang, and X. Zhao, "Color image encryption algorithm based on bidirectional spiral transformation and dna coding," *Physica Scripta*, vol. 98, no. 2, p. 025211, 2023.
[33] Y. Xiao, X. Tong, M. Zhang, and Z. Wang, "Image lossless encoding and encryption method of ebcot tier1 based on 4d hyperchaos," *Multimedia Systems*, vol. 28, no. 3, pp. 727–748, 2022.
[34] W. Cao, Y. Mao, and Y. Zhou, "Designing a 2d infinite collapse map for image encryption," *Signal Processing*, vol. 171, p. 107457, 2020.
[35] G. Shi, S. Yu, and Q. Wang, "Security analysis of the image encryption algorithm based on a two-dimensional infinite collapse map," *Entropy*, vol. 24, no. 8, p. 1023, 2022.
[36] S. Wang, Q. Peng, and B. Du, "Chaotic color image encryption based on 4d chaotic maps and dna sequence," *Optics & Laser Technology*, vol. 148, p. 107753, 2022.
[37] M. Blaimer, F. Breuer, M. Mueller, R. M. Heidemann, M. A. Griswold, and P. M. Jakob, "Smash, sense, pils, grappa: how to choose the optimal method," *Topics in Magnetic Resonance Imaging*, vol. 15, no. 4, pp. 223–236, 2004.
[38] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on mixed image element and chaos," *Computers & Electrical Engineering*, vol. 62, pp. 401–413, 2017.
[39] A. Jolfaei, X.-W. Wu, and V. Muthukkumarasamy, "On the security of permutation-only image encryption schemes," *IEEE transactions on information forensics and security*, vol. 11, no. 2, pp. 235–246, 2015.
[40] T. M. Hoang and H. X. Thanh, "Cryptanalysis and security improvement for a symmetric color image encryption algorithm," *Optik*, vol. 155, pp. 366–383, 2018.
[41] G. Hu, D. Xiao, Y. Wang, and X. Li, "Cryptanalysis of a chaotic image cipher using latin square-based confusion and diffusion," *Nonlinear Dynamics*, vol. 88, pp. 1305–1316, 2017.
[42] L. Chen, B. Ma, X. Zhao, and S. Wang, "Differential cryptanalysis of a novel image encryption algorithm based on chaos and line map," *Nonlinear Dynamics*, vol. 87, pp. 1797–1807, 2017.
[43] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. A. Del Campo, "A rgb image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, vol. 109, pp. 119–131, 2015.
[44] Z. Parvin, H. Seyedarabi, and M. Shamsi, "A new secure and sensitive image encryption scheme based on new substitution with chaotic function," *Multimedia Tools and Applications*, vol. 75, pp. 10 631–10 648, 2016.
[45] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.
[46] L. Li, Y. Yao, and X. Chang, "Plaintext-dependent selective image encryption scheme based on chaotic maps and dna coding," in *2017 International Conference on Dependable Systems and Their Applications (DSA)*. IEEE, 2017, pp. 57–65.
[47] H. Fan, M. Li, D. Liu, and K. An, "Cryptanalysis of a plaintext-related chaotic rgb image encryption scheme using total plain image characteristics," *Multimedia Tools and Applications*, vol. 77, pp. 20 103–20 127, 2018.
[48] B. Norouzi and S. Mirzakuchaki, "Breaking an image encryption algorithm based on the new substitution stage with chaotic functions," *Optik*, vol. 127, no. 14, pp. 5695–5701, 2016.
[49] P. Sneha, S. Sankar, and A. S. Kumar, "A chaotic colour image encryption scheme combining walsh–hadamard transform and arnold–tent maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 1289–1308, 2020.
[50] G. Wang, X. Ye, and B. Zhao, "A novel remote sensing image encryption scheme based on block period arnold scrambling," *Nonlinear Dynamics*, vol. 112, no. 19, pp. 17 477–17 507, 2024.
[51] K. Jithin and S. Sankar, "Colour image encryption algorithm combining arnold map, dna sequence operation, and a mandelbrot set," *Journal of Information Security and Applications*, vol. 50, p. 102428, 2020.
[52] V. Subashini and S. Poornachandra, "A new transformation for chaotic image encryption based on the arnold cat map," *Applied Mathematics & Information Sciences An International Journal*, vol. 12, no. 4, pp. 797–805, 2018.
[53] T. ul Haq and T. Shah, "Algebra-chaos amalgam and dna transform based multiple digital image encryption," *Journal of Information Security and Applications*, vol. 54, p. 102592, 2020.
[54] G. Qi, M. A. van Wyk, B. J. van Wyk, and G. Chen, "On a new hyperchaotic system," *Physics Letters A*, vol. 372, no. 2, pp. 124–136, 2008.
[55] M. Suryadi, Y. Satria, and L. N. Prawadika, "An improvement on the chaotic behavior of the gauss map for cryptography purposes using the circle map combination," *Journal of Physics: Conference Series*, vol. 1490, no. 1, p. 012045, 2020.
[56] C. Leith, "Stochastic models of chaotic systems," *Physica D: Nonlinear Phenomena*, vol. 98, no. 2-4, pp. 481–491, 1996.
[57] L. Huang, S. Cai, M. Xiao, and X. Xiong, "A simple chaotic map-based image encryption system using both plaintext related permutation and diffusion," *Entropy*, vol. 20, no. 7, p. 535, 2018.
[58] J. Wu, J. Shi, and T. Li, "A novel image encryption approach based on a hyperchaotic system, pixel-level filtering with variable kernels, and dna-level diffusion," *Entropy*, vol. 22, p. 5, 12 2019.
[59] H. Shen, X. Shan, M. Xu, and Z. Tian, "A new chaotic image encryption algorithm based on transversals in a latin square," *Entropy*, vol. 24, no. 11, p. 1574, 2022.
[60] X. Chai, J. Zhang, Z. Gan, and Y. Zhang, "Medical image encryption algorithm based on latin square and memristive chaotic system," *Multimedia Tools and Applications*, vol. 78, pp. 35 419–35 453, 2019.
[61] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on dna encoding and chaotic system," *Multimedia Tools and Applications*, vol. 78, pp. 7841–7869, 2019.
[62] N. Iqbal, M. A. Khan, and S.-W. Lee, "Multi-image cipher based on the random walk of knight in a virtual 3d chessboard," *Multimedia Tools and Applications*, pp. 1–33, 2023.
[63] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the lss chaotic map and single s-box," *IEEE Access*, vol. 8, pp. 25 664–25 678, 2020.
[64] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37 855–37 865, 2021.
[65] S. Bhuvaji, A. Kadam, P. Bhumkar, S. Dedge, and S. Kanchan, "Brain tumor classification (mri)," 2020. [Online]. Available: https://www.kaggle.com/dsv/1183165
[66] L. Visuña, D. Yang, J. Garcia-Blas, and J. Carretero, "Computer-aided diagnostic for classifying chest x-ray images using deep ensemble learning," *BMC Medical Imaging*, vol. 22, no. 1, p. 178, 2022.

Quanjun Li is currently pursuing his undergraduate studies at the School of Advanced Manufacturing, Guangdong University of Technology, Guangzhou, China. His research interests encompass computer vision, image encryption, multimodal learning, and deep learning.

Qian Li is currently pursuing the degree in communication engineering with Wuyi University, with a focus on computer science. Her research interests include deep learning and image encryption.

Bingo Wing-Kuen Ling received the B.Eng. (Hons) and M.Phil. degrees in Electronic and Computer Engineering from the Hong Kong University of Science and Technology in 1997 and 2000, and the Ph.D. degree in Electronic and Information Engineering from the Hong Kong Polytechnic University in 2003. He has held academic positions at King's College London, the University of Lincoln, and currently serves as a Full Professor at Guangdong University of Technology. He is a Fellow of the IET, Senior Member of the IEEE, and a Distinguished Professor under China's National Young Thousand-Talent and University Hundred-Talent programs. He is active in multiple IEEE technical committees and has received best reviewer awards from the IEEE Instrumentation and Measurement Society. He has also guest-edited special issues for leading journals and is an associate editor for several prestigious publications.

Chi-Man Pun received his Ph.D. degree in Computer Science and Engineering from the Chinese University of Hong Kong in 2002. He was the Head of the Department of Computer and Government Information Science from 2014 to 2019. Dr. Pun is currently a Professor of Computer and Information Science and in charge of the Image Processing and Pattern Recognition Laboratory at the Faculty of Science and Technology of the University of Macau. His research interests include Image Processing and Pattern Recognition; Multimedia Information Security, Forensic and Privacy; Adversarial Machine Learning and AI Security, etc. He is also a senior member of theIEEE.

Guoheng Huang received the Ph.D. degree in software engineering from the University of Macau, Macao, China, in 2017. He is CCF Member and Associate Professor for computer science with Guangdong University of Technology, Guangzhou, China. His research interests include Computer Vision, Pattern Recognition, and Artificial Intelligence.

Xiaochen Yuan received the Ph.D. degree in software engineering from the University of Macau, Macao, China, in 2013. She is currently an Associate Professor with the Faculty of Applied Sciences of the Macao Polytechnic University, Macao. Her research interests include digital multimedia processing, digital watermarking, multimedia forensics, tampering detection and self-recovery, acoustic processing and diagnosis, and deep learning techniques and applications. She is a senior member of theIEEE.

Guo Zhong received the Ph.D. degree in computer science from the University of Macau, Macao, China. He is currently an Associate Professor with the School of Information Science and Technology, Guangdong University of Foreign Studies, Guangzhou, China. His research interests include machine learning and its applications, such as pattern recognition, data mining, and information retrieval.

Sarra Ayouni received the M.S. degree from the Faculty of Sciences of Tunis (FST) and the Ph.D. degree in computer science from the University of Montpellier 2, France. She is currently an Assistant Professor with the Department of Information Systems, College of Computer and Information Sciences (CCIS), Princess Nourah bint Abdulrahman University (PNU), where she is also a Coordinator of Distance Education. Her main research interests include data science, artificial intelligence, fuzzy datamining, and e-learning.

Jianwu Chen* received his Bachelor of Medicine degree from Fujian Medical University in 1991 and his doctorate degree from Paris VI University in 2004. Since 2013, he has been the director of the Affiliated Union Hospital of Fujian Medical University. His research interests include radiation therapy, combination of basic and chemoradiotherapy, standardized treatment of cancer pain, etc.