基于分数阶超混沌与条件GAN的可逆水印医学图像加密算法

曹 棪[1],章步峰[1],徐 滔[1],朱晓强[2],刘 源[3]

(1. 北京交通大学 软件学院;2. 北京交通大学 网络空间安全学院,北京 100091;
3. 天津大学 软件学院,天津 300350)

摘 要: 随着医疗行业信息化进程的加速发展,医学图像作为承载患者隐私和关键诊断信息的载体,其加密保护已成为当前研究与应用领域的热点。然而,现有图像加密方法普遍面临安全性不足、加密效率低下以及功能单一等挑战。为解决上述问题,提出了一种名为FGC-RDH的新型医学图像加密算法。首先,该算法融合哈希算法与分数阶4DChen超混沌系统构建统一伪随机数(PRN)生成机制,驱动动态分数阶S盒及空间填充曲线置换,从而实现高效的像素置乱;其次,在扩散阶段,提取明文的混沌哈希特征向量作为约束条件,利用混沌引导条件生成对抗网络(GAN)生成基础扩散密钥,并结合自适应混沌精炼来实现区域增强扩散;最后,通过集成明文域可逆水印技术,使算法具备了可靠的数据溯源功能。通过与RIE-RID、CCAES和MCBS等算法进行对比实验,结果表明,该算法在密文熵、NPCR、UACI和密钥敏感性等性能上显著提升,其中,NPCR值达到99.616%、密文熵达到7.999 1。实验结果充分证明,该算法具有极高的安全性和抗攻击能力,能够为远程医疗数据的高效安全传输提供强有力的技术保障。

关键词: 可逆水印;图像加密;机器学习;医学图像

DOI: 10. 11907/rjdk. 261092 扫描二维码阅读全文:

中图分类号: TP301 **文献标识码:** A **文章编号:** 1672-7800(2026)007-0072-12

Medical Image Encryption Algorithm Based on Fractional-Order Hyperchaos, Conditional GAN, and Reversible Watermarking

CAO Yan[1], ZHANG Bufeng[1], XU Tao[1], ZHU Xiaoqiang[2], LIU Yuan[3]

(1. *School of Software*, *Beijing Jiaotong University*; 2. *School of Cyberspace Science and Technology*, *Beijing Jiaotong University*, *Beijing* 100091, *China*; 3. *School of Software*, *Tianjin University*, *Tianjin* 300350, *China*)

Abstract: With the rapid advancement of healthcare informatization, medical images, which serve as essential carriers of patient privacy and critical diagnostic information, have become a focal point in encryption research and application. However, existing image encryption methods generally face challenges such as insufficient security, low efficiency, and limited functionality. To address these issues, this paper proposes a novel medical image encryption algorithm named FGC-RDH. Specifically, the algorithm first integrates a hash algorithm with a fractional-order 4D Chen hyperchaotic system to construct a unified pseudo-random number (PRN) generation mechanism, which drives dynamic fractional-order S-boxes and space-filling curve permutations to achieve efficient pixel scrambling. Second, in the diffusion phase, chaotic hash feature vectors are extracted from the plaintext as constraints to guide a Conditional Generative Adversarial Network (GAN) in generating a base diffusion key, which is then refined through adaptive chaotic processes for regionally enhanced diffusion. Finally, by incorporating plaintext-domain reversible watermarking technology, the algorithm enables reliable data traceability. Comparative experiments with algorithms such as RIE-RID, CCAES, and MCBS demonstrate that the proposed method significantly improves performance in terms of ciphertext entropy,

收稿日期: 2026-03-24

基金项目: 中央高校基本科研业务费专项(2026JBMC063);国家自然科学基金项目(62401037);中国博士后科学基金会项目(GZC20230224, 2024M750166)

作者简介: 曹棪(2004-),男,北京交通大学软件学院学生,研究方向为机器学习、图像加密;章步峰(2005-),男,北京交通大学软件学院学生,研究方向为混沌密码学、隐私保护;徐滔(2005-),男,北京交通大学软件学院学生,研究方向为网络安全;朱晓强(1992-),男,博士,CCF专业会员,北京交通大学网络空间安全学院助理教授,研究方向为物联网、机器学习、隐私保护;刘源(1996-),女,天津大学软件学院博士研究生,研究方向为数据中心网络。本文通讯作者:朱晓强。

NPCR, UACI, and key sensitivity. Notably, the NPCR reaches 99.616% and the ciphertext entropy achieves 7.999 1. These results prove that the algorithm possesses high security and robust anti-attack capabilities, providing strong technical support for the efficient and secure transmission of remote medical data.

Key Words: reversible watermarking; image encryption; machine learning; medical image

0　引言

当前,物联网、大数据与云计算等前沿技术已广泛应用于医疗系统,CT、MRI、X-ray等医疗影像数据已成为临床诊断与疾病管理的核心依据。随着这些医疗技术的发展,越来越多的医疗图像被生成。然而,医疗图像承载着患者的敏感隐私信息,包括个人身份、病史甚至潜在的基因数据,一旦这些数据被篡改或恶意泄露,将导致十分严重的后果。因此,构建强有力的图像数据加密防护机制以保障数据安全,已成为医疗领域的刚需。为应对上述医疗图像数据安全防护的挑战,本文深入研究并提出了一种新型医学图像加密算法,旨在提供更为安全、高效、智能且功能全面的解决方案。

在图像加密领域,传统图像加密技术主要分为置乱和扩散两个关键过程,通过破坏图像像素间固有的强空间相关性和像素分布规律来实现加密[1]。在置乱方面,其核心是打破原始图像像素间的空间相关性;在扩散方面,其核心目标是将图像中单个像素的灰度值变化扩散到多个像素上,以此打破像素灰度值之间的统计关联性。近年来的研究致力于通过融合多项技术来突破单一加密算法在安全性与效率上的瓶颈。在提升安全性方面,Fan等[2]利用分数阶超混沌系统结合位级置乱与DNA级扩散,实现了高安全性的图像加密。Meng等[3]提出了一种基于分数阶保守忆阻超混沌系统和扩展Z字变换的彩色图像加密算法,显著提升了密文的不可预测性。Yu等[4]则通过设计一种具有隐藏动力学和多卷吸引子的新型分数阶系统,验证了其在抵御相空间重构攻击方面的优势。在提升处理效率方面,引入深度学习模型辅助密钥生成已成为新趋势。Singh等[5]对基于深度学习的图像加密技术进行了系统综述,分析了利用神经网络建立非线性特征映射,从而降低计算延时的可行性。Huang等[6]针对医学影像提出了具备可学习特性的加密方案,实现了模型训练效率与隐私保护的有效平衡。此外,现有的加密研究多关注数据机密性,忽略了医学影像对临床溯源的需求。为此,Asif等[7]探讨了利用深度神经网络优化可逆数据隐藏(Reversible Data Hiding, RDH)性能的方法,旨在解决密文传输过程中的数据确权难题。

然而,这些方法在某些应用场景下仍然暴露出一些弊端。乔子轩等[8]提出的MCBS算法,通过引入S盒和Logistics混沌系统进行像素置乱,并利用卷积神经网络(Convolutional Neural Network, CNN)和宽度学习(Broad Learning System, BLS)生成的矩阵密钥进行异或扩散,最终辅以数字签名技术。然而,在密钥生成环节中,由于置乱后图像的像素空间相关性已被大幅破坏,机器学习模型难以捕捉到有效的特征差异,这使得该算法在密钥敏感性方面存在明显的局限。同时,其S盒的构造较固定,与分数阶超混沌源相比仍有提升空间。Yousif等[9]提出的RIE-RID算法结合扫描技术、ElGamal公钥密码、Lorenz及Rössler两类混沌系统,通过多层置乱和混沌扩散提高了密钥空间复杂度。然而,RIE-RID算法因其多层扫描等操作,导致加密解密耗时显著增加,难以适配医学图像临床应用场景下的实时处理要求。Khan等[10]提出的FOLS算法基于新型五维Lorenz-Stenflo混沌系统与忆阻器特性实现了图像加密,旨在压缩加解密时间。虽然FOLS算法优化了加解密耗时问题,但其置乱与扩散过程完全依托混沌系统生成的伪随机序列,单一的密钥生成源导致密钥空间的多样性不足,在面对针对混沌系统的差分攻击时,加密方案的安全性易出现短板。在神经网络与混沌系统的融合方面,Man等[11]提出了一种双图像加密算法,该算法将图像特征作为CNN的卷积核,提升了双图加密效率。然而,这种方法主要关注多图并行处理的效率,其单张图像的加密时算力资源浪费问题仍未有效解决。此外,Zhu等[12]提出的EDBNet网络将CNN和BLS结合,实现了极佳的加密速率。然而,EDBNet的CNN矩阵密钥生成方式较为直接,存在与原图特征重合的风险,导致CNN密钥易被破译。

为了克服现有图像加密技术在安全性和效率等方面的挑战 ,本文提出的FGC-RDH算法通过多技术融合实现了性能均衡。该算法构建了高效且对明文和用户密钥敏感的统一伪随机数(Pseudo-Random Number, PRN)生成器,该生成器不仅具备高效的运算特性,还对原始明文信息与用户密钥呈现出高度敏感性。基于此生成器,算法进一步构建了动态S盒,并借助PRN驱动的Hilbert空间填充曲线完成像素位置置换,最终实现像素级的置乱操作。在扩散阶段,通过混沌引导的条件生成对抗网络(Generative Adversarial Network, GAN)生成基础扩散密钥,同时,该GAN结合二次混沌精炼,实现了扩散密钥生成。此外,本算法还集成了明文域可逆数字水印。通过上述技术手段的协同运作,算法在安全性和功能性上得到了进一步的提升。本文的主要贡献如下:

(1)改进传统随机数(PRN)生成方式,融合SHA-256哈希算法与分数阶4D Chen超混沌系统,从而构建混沌-哈希反馈迭代结构。该结构能够生成对明文和用户密钥极其敏感的PRN流,显著提升了PRN的高效复用与派生。

(2)优化明文域可逆数字水印嵌入方案,通过PRN驱

动的预测器优化与位置图压缩算法，在明文域嵌入预测误差扩展（Prediction Error Expansion，PEE）可逆水印，从而实现高容量、低失真且对密钥敏感的水印功能，确保了数据的无损恢复。

（3）构建融合几何重组与GAN的加密架构，采用PRN驱动的动态S盒与Hilbert空间填充曲线来实现置乱过程。首先，通过混沌引导的条件生成对抗网络（GAN）构建基础扩散密钥；其次，依据PRN驱动生成的区域强度图，对基础密钥进行区域差异化的强度调整。

1 本文算法

FGC-RDH加密新算法的加密过程，如图1所示。其具体包括PRN生成、置乱、扩散以及优化后的可逆数字水印集成，多环节协同，从而确保加密后的图像具有高度的安全性、智能化与功能性。

（1）PRN生成。本阶段构建统一的PRN源。算法融合哈希算法与分数阶4D Chen超混沌系统，形成混沌—哈希反馈循环机制，生成对明文和用户密钥敏感的PRN序列。该PRN序列作为子种子，通过高效复用与派生机制，为后续所有模块提供相应的子序列。

（2）置乱。本阶段首先利用PRN派生的随机数子序列为待加密的原始明文图像动态生成唯一的S盒，实现像素值的非线性转换。随后，采用PRN驱动的Hilbert空间填充曲线置换，彻底打乱像素位置，从而确保打乱后图像的空间相关性。

（3）扩散。本阶段采用区域感知密钥生成机制。首先，从原始图像中提取混沌哈希特征向量作为GAN的条件输入；其次，基于混沌哈希特征向量与混沌噪声，混沌引导的条件GAN生成基础扩散密钥；然后，依据PRN驱动生成的区域强度图，对基础密钥进行区域差异化的强度调整，产出最终扩散密钥；最后，将置乱后的图像与该密钥进行异或运算，实现像素扩散。

（4）数字水印。本算法优化了明文域可逆数字水印功能。采用PRN驱动的高效位置图压缩方案，将关键数据以无损方式嵌入明文图像，随后，连同加密流程一同进行保护。该功能不仅可以提供隐私信息保护和身份溯源，还确保了数据在医学场景中的无损恢复。

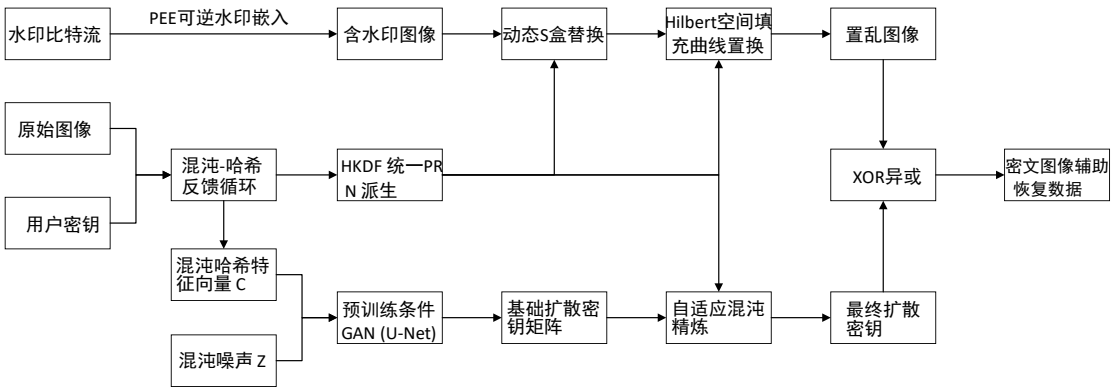


Fig. 1 The flowchart of image encryption

图1 图像加密流程图

1.1 PRN生成

伪随机数序列（PRN）生成方法将分数阶4维Chen系统的当前状态注入哈希输入中，通过SHA-256计算获得新的哈希值，再由该哈希值对混沌系统状态进行微扰并驱动下一步迭代，从而生成对明文与密钥高度敏感的PRN统一子种子字节流[13]。

1.1.1 PRN生成过程

首先，定义以下符号及输入、输出参数：①输入参数D：原始明文图像的哈希值；②输入参数K：用户提供的加密密钥；③输出R：生成的PRN字节序列，其长度为L，序列中每个字节的取值范围为0~255；④混沌系统状态S_t：表示分数阶4D Chen系统在第t轮迭代时的状态向量(x_t, y_t, z_t, w_t)，该向量由4个实数值构成；⑤系统参数θ：控制分数阶4D Chen系统行为的参数集，包括(a, b, c, d, α, t)，其中$\alpha \in (0,1]$为分数阶阶次，t为迭代步长。

本文选用的分数阶4D Chen超混沌系统是该算法的核心，其数学模型可描述为如下的分数阶微分方程组，如式（1）所示。

$$\begin{cases} D_t^{\alpha} x = a(y - x) \\ D_t^{\alpha} y = (c - a)x - xz + cy \\ D_t^{\alpha} z = xy - bz \\ D_t^{\alpha} w = x + d \end{cases} \tag{1}$$

其中，$\alpha \in (0,1]$表示系统的分数阶阶次。相较于传统的低维或整数阶混沌系统，分数阶4D Chen系统展现出更为复杂的超混沌动力学特性，其具有多个正的李雅普诺夫指数（Lyapunov exponents），意味着系统在多个维度上均具有极强的发散性和不可预测性。在PRN统一子种子生成前，需要确定系统的初始混沌状态。算法将D与密钥K进行字节拼接，并计算其SHA-256哈希值，作为混沌系统初始化的基础，如式（2）所示。

$$H_0 = SHA256(D \mathbin{/\!/} K) \tag{2}$$

随后，利用得到的 H_0 对分数阶 4 维 Chen 系统的初始状态进行调整。具体而言，取 H_0 的前 16 字节，将其解析为 4 个无符号的 32 位整数 u_1、u_2、u_3、u_4，再根据公式(2)将这些整数映射到区间 [−1，1]，以产生一个 4 维扰动向量 δ=(δ_1，δ_2，δ_3，δ_4)，如式(3)所示。

$$\delta_i = 2 \times \left(\frac{u_i}{2^{32} - 1} \right) - 1, \quad i = 1 \cdots 4 \tag{3}$$

给定预设的基础初始条件 $s_{base} = \left(x_0^{base}, y_0^{base}, z_0^{base}, v_0^{base} \right)$，系统的初始混沌状态设定为：$s_0 = s_{base} + \lambda \times \delta$。其中，λ 为一个权重常数(0.1)，用于控制扰动强度，保证数值稳定性。系统的初始混沌状态设定好后，PRN 生成器将利用此初始状态，进入一个高效的迭代循环，持续产出满足加密需求的伪随机数序列。迭代循环过程的伪代码如算法 1 所示。

算法 1　PRN 迭代循环

输入：D，K，θ，基本初始条件 s_{base}，输出长度 L

输出：PRN 字节序列 R(长度为 L)

$H_0 \leftarrow SHA256(D \| K)$;

$s_0 \leftarrow s_{base} + \lambda \cdot \delta(H_0)$;

R ←[ ], $H_{current} \leftarrow H_0, t \leftarrow 0$;

While length(R) < L *do*;

Encoding the four floating-point states into a 32-byte string:

$B(s_t) \leftarrow float\_state\_to\_bytes(s_t)$;

$X_t \leftarrow H_{current} \,//\, sep \,//\, B(s_t)$;

Calculate new hash: $H_{next} \leftarrow SHA256(X_t)$;

Hash-Driven Perturbation: $s_t' \leftarrow s_t + \lambda \cdot \delta(H_{next})$;

Fractional-order Chen system iteration:

$s_{t+1} \leftarrow F\_Chen\_alpha(s_t'; \theta)$;

Extract PRN bytes:

$R \leftarrow R \,//\, Take4(float\_state\_to\_bytes(s_{t+1}))$;

Update the current hash and count:

$H_{current} \leftarrow H_{next}$, $t \leftarrow t + 1$;

Return the first L bytes of R

End

1.1.2　PRN 的高效复用与派生

实验中，为每个模块重新生成 PRN 序列会大幅增加计算开销。为降低在多模块、多阶段场景下反复长序列生成的计算开销，本算法引入“主种子+上下文派生”机制，同时，确保派生出的 PRN 子序列具备高随机性、不可预测性与安全性。

令主种子长度为 S 字节，调用算法 1 生成长度为 S 的 PRN 序列作为统一主种子：$Seed \leftarrow PRNGen(D, K, \theta, S)$，子序列派生遵循 HKDF(HMAC-based Key Derivation Function)的 Extract-then-Expand 模式[14]。给定盐值 salt 与上下文信息 ctx，计算伪随机密钥 PRK，如式(4)所示。

$$PRK = HMAC\_SHA256(salt, Seed) \tag{4}$$

以 $info = ctx \,//\, counter$ 作为扩展信息，如式(5)所示。

$$PRN\_ctx = HKDF\_Expand(PRK, info, L_{ctx}) \tag{5}$$

其中，counter 是一个迭代计数器，用于在同一上下文下生成多个互不相同的子序列，用式(4)生成长度为 L_{ctx} 的子序列。具体流程如图 2 所示。

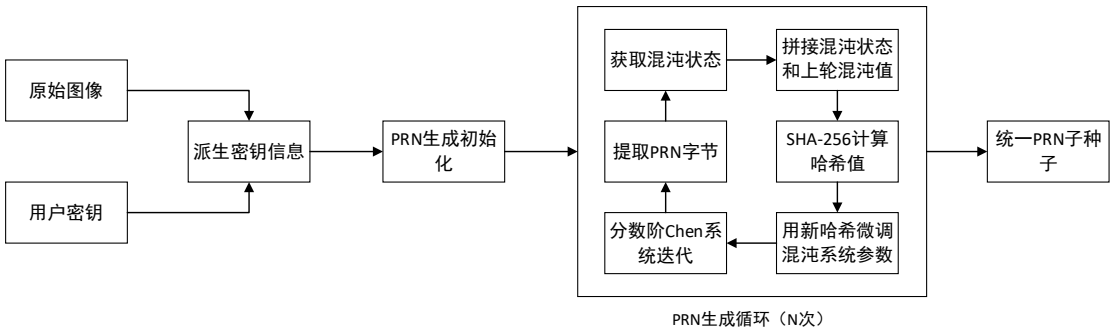


Fig. 2　The flowchart of PRN generation

图 2　PRN 生成流程图

1.2.　数字水印

数字水印作为一种有效的数据隐藏手段，通过在载体图像中嵌入特定的元数据(如患者信息、版权标识等)来实现身份认证与版权保护。该阶段将水印信息以可逆方式嵌入原始图像中，生成含水印图像作为后续置乱阶段的输入，从而为医学图像提供无损的版权保护与溯源功能。

1.2.1　预测误差扩展(PEE)水印嵌入

预测误差扩展(PEE)通过修改像素预测值的误差来实现信息的无损嵌入，其利用误差直方图的平移与扩展，在保障影像质量的前提下提供可观的嵌入容量。

首先，定义输入参数，具体包括：①输入图像 I：待嵌入水印的原始灰度图像，像素值 $I \in \{0, 1, \cdots, 255\}^{H \times W}$，尺寸为 H×W；②水印比特流 W：待嵌入的元数据，表示为 L 个比特 $W = (w_1, w_2, \cdots, w_L)$；③ 用户密钥 K：驱动 PRN 流生成的核心密钥；④扩展阈值 T：控制预测误差扩展的阈值。

对于图像像素 I(i，j)，采用 MED(Median Edge Detector)预测器来计算预测值 p(i，j)，如式(6)所示。

$$p(i,j) = median(left, top, left + top - top\_left) \tag{6}$$

其中，left、top、top_left 为邻域像素值，预测误差 e(i，j)定义为 $e(i,j) = I(i,j) - p(i,j)$。算法只对满足误差阈值限制($|e(i,j)| \leqslant T$)且不会因扩展而溢出的像素进行扩展。对于满足条件的像素，根据待嵌入的水印比特 $w \in \{0, 1\}$ 扩

展预测误差$e'(i,j)$,如式(7)—式(8)所示。

$$e'(i,j) = 2 \times e(i,j) + w(if\ e(i,j) \geqslant 0) \quad (7)$$

$$e'(i,j) = 2 \times e(i,j) - w(if\ e(i,j) < 0) \quad (8)$$

扩展后的新像素值$I_w(i,j)$为:$I_w(i,j) = p(i,j) + e'(i,j)$。算法记录所有被修改像素的位置,从而形成位置图 L。

1.2.2 PRN驱动的位置图压缩

本算法采用PRN驱动的位置图压缩方案。根据公式(4)由统一的PRN子种子中派生出位置图压缩的子PRN序列PRN_compression。本算法集成了RLE、差分编码结合霍夫曼编码等多种压缩方式。系统根据当前位置图的稀疏度,利用 PRN_compression序列辅助动态选择最优算法,生成压缩图 *L_compressed*。随后,将该压缩图与水印恢复所需的其他信息共同封装为辅助数据*Auxiliary_Data*,以供后续水印提取和图像恢复使用。

1.2.3 水印提取与原始图像恢复

首先,用 Auxiliary_Data 中的 PRN_compression 驱动解压缩恢复位置图L;其次,逆向计算原始预测误差e(i,j)和水印比特w;最终,恢复原始像素值$I(i,j) = p(i,j) + e(i,j)$。数字水印嵌入过程如算法2所示。

算法2 数字水印嵌入

输入:I,W,K,T,PRN 统一子种子P

输出:水印图像 Iout,辅助数据 Aux

1. L=zeros(H,W,dtype=bool)

2. Iw=I.copy(), bit_index=0

3. PRN←DerivePRN(P, ``watermark_compression'', L)

4. For i=1 to H-1, j=1 to W-1:

5. If bit_index≥len(W): break

6. p←MED_Predictor(Iw, i, j)

7. e←Iw(i,j)-p

8. w←W[bit_index]

9. e′←2×e+w (if e≥0) or e′←2×e-w (if e<0)

10. Iw(i,j)←p+e′,If 0≤Iw(i,j)≤255:

11. L(i,j)←True, bit_index←bit_index+1

12. Else Iw(i,j)←I(i,j)

13. Location Map Compression: Lcompressed←CompressLocationMapPRN(L, PRN)

14. Build auxiliary data:

15. Aux←{location_map_compressed: Lcompressed, watermark_length: len(W), …}

16. Return Iw, Aux

17. End

1.3 置乱

在置乱阶段,采用PRN驱动的动态S盒并结合Hilbert空间置换流程,有效提升了算法对明文和密钥的敏感性。

1.3.1 动态S盒构建

S盒是对称密码体制中实现非线性变换的核心组件,其主要作用是混淆明文与密钥之间的逻辑关系,从而抵御线性攻击与差分攻击。传统的S盒(如AES算法中的S盒)通常采用固定的置换表,虽然具备良好的密码学特性,但缺乏灵活性,这意味着对于不同的明文图像或同一图像的不同区域,替换逻辑始终保持一致。由于医学影像具有极强的空间冗余性和灰度聚集性,静态S盒难以彻底消除图像的统计特征,且容易受到已知明文攻击。为消除图像像素的统计特征,本文利用统一PRN子种子派生出的PRN_{sbox}序列来构造动态S盒。不同于固定S盒,该S盒随图像内容动态生成。首先,初始化序列$S = [0, 1, \cdots, 255]$,利用Fisher-Yates洗牌算法。随后,在第i次迭代中,用$r_i \in PRN_{sbox}$计算随机索引$j = (r_i\ mod(i+1))$并交换S[i]和S[j]的位置,生成的映射关系记为S_{box}。对图像I中的每个像素I(i,j)执行非线性替代,得到中间图像$I^{(1)}$,如式(9)所示。

$$I^{(1)}(i,j) = S_{box}[I(i,j)], \quad 0 \leqslant i < H,\ 0 \leqslant j < W \quad (9)$$

1.3.2 PRN-Hilbert空间置换

在像素值混淆的基础上,进一步采用Hilbert空间填充曲线与Fisher-Yates洗牌相结合的双层位置置乱策略。首先,从主种子派生独立序列PRN_k,先截取序列PRN_k的前16个字节,将其分为4组,每组4字节。随后,将每组字节按大端序重组为32位无符号整数$u_m(m = 1, 2, 3, 4)$,通过线性映射将整数域上的离散值投影至连续区间[-1,1],如式(10)所示。

$$\begin{cases} u_m = \sum_{j=0}^{3} PRN_k[4(m-1)+j] \cdot 2^{8(3-j)} \\ \{x_k, y_k, z_k, w_k\}_m = \dfrac{u_m}{2^{32}-1} \times 2 - 1 \end{cases} \quad (10)$$

其中,$PRN_k[i]$表示序列中的第i个字节,映射结果依次记为$x_k, y_k, z_k, w_k \in [-1, 1]$(分别对应m=1, 2, 3, 4)。上述参数提供了充足的数值精度,用于驱动后续Hilbert曲线阶数、旋转与翻转的随机化。Hilbert曲线的阶数$order_k$、旋转角度$rotate_k$和反转状态$flip_k$的计算如式(11)所示。

$$\begin{cases} order_k = \lceil \log_2(\max(H, W)) \rceil + \Delta(x_k, y_k) \\ rotate_k = \lfloor |z_k \times 1\,000| \rfloor \bmod 4 \\ flip_k = (w_k - \lfloor w_k \rfloor) > 0.5 \end{cases} \quad (11)$$

其中,值x_k, y_k用于计算动态扰动项$\Delta(x_k, y_k)(\Delta(x_k, y_k) = \lfloor |x_k + y_k| \times C \rfloor$,C为调节常数),从而引入随机扰动。基于上述参数构建一维Hilbert路径$Path_k$,首先,将图像中的二维像素映射为一维序列Y_k;其次,利用PRN_k生成置换索引π_k,Fisher-Yates洗牌算法对Y_k进行二次乱序得到Y'_k;最后,按$Path_k$逆映射回二维空间,重组得到最终置乱图像*Scrambled_Image*。置乱过程如算法3所示。

算法3 动态S盒与Hilbert置乱算法

输入:I, K, θ, PRN统一子种子P

输出:置乱图像S_{img}

1. PRN ← DerivePRN(P, ''sbox'', L)

2. S ← GenDynamicSBox(PRN_{sbox}),For$i$ = 1to$H$, j = 1to$W$:

3. $I^{(1)}(i,j) \leftarrow S[I(i,j)]$

4. $\mathrm{PRN}_{\mathrm{hilbert}} \leftarrow \mathrm{DerivePRN}(\mathrm{P}, ``hilbert'', L)$

5. $\{x, y, z, w\} \leftarrow \mathrm{ExtractNormParams}(\mathrm{PRN}_{\mathrm{hilbert}})$

6. $\mathrm{Path} \leftarrow \mathrm{BuildHilbertPath}(H, W, x, y, z, w)$

7. $V \leftarrow \mathrm{ExtractPixels} = (I^{(1)}, \mathrm{Path})$

8. $V' \leftarrow \mathrm{FisherYatesShuffle}(V, \mathrm{PRN}_{\mathrm{hilbert}})$

9. $S_{img} \leftarrow \mathrm{MapBack}(V', \mathrm{Path})$

10. Return S_{img}.

11. End

1.4　扩散

传统的扩散往往依赖于简单的低维混沌映射生成的密钥流进行异或操作，虽然具有较高的计算效率，但在密钥生成的复杂度和与明文的关联性上存在局限。为了解决上述问题，本文采用一种基于混沌引导的条件生成对抗网络（GAN）与自适应混沌精炼相结合的新型扩散方法。该方法首先从原始明文图像中提取其混沌哈希特征向量（Chaotic-Hash Feature Vector，CHFV），指导GAN智能生成基础扩散密钥，随后，通过混沌系统驱动生成的区域强度图进行自适应的精炼过程。

1.4.1　混沌哈希特征向量提取

为了让生成的扩散密钥既具有随机性又与特定的明文图像高度绑定，本算法提取原始图像的混沌哈希特征向量。相较于传统方案直接提取图像的边缘、纹理等语义特征，容易导致明文信息泄露，本文采用混沌—哈希迭代方式替代。将原始图像I的哈希值与用户密钥K结合，输入分数阶4D Chen系统进行多轮“哈希-混沌”反馈迭代。首先，由式（2）和式（3）计算得到分数阶4D Chen系统的初始状态S_0，系统进入$N = 30$轮的迭代过程，每一轮迭代t进行如下操作：

将上一轮混沌状态$\mathrm{S_{t-1}}$序列化为字节$\mathrm{B_{t-1}}$，与上一轮哈希值拼接，计算新哈希$\mathrm{H_t}$：$H_t = SHA256(H_{t-1} \| B_{t-1})$。同时，利用Ht的部分比特生成微扰量Δ，更新系统状态，从而实现了哈希对混沌的反向控制，使得明文微小差异能迅速改变混沌轨迹，如式（12）所示。

$$S'_{t-1} = S_{t-1} + \Delta(H_t) \tag{12}$$

在微调后的状态基础上，利用分数阶微分方程数值解法迭代计算下一状态：$S_t = FractionalChenStep(S'_{t-1})$。经过N轮迭代后，系统收敛到一个高度敏感的状态。本文从最终的混沌状态中提取并量化出一个128维的浮点向量C，如式（13）所示。

$$C = ExtractFingerprint(S_N, H_N) \tag{13}$$

最终，得到的C便是原始文图像的混沌哈希特征向量。该向量在数学上满足单向不可逆性，可防止反向重构原始图像，从而保障了特征安全性。此外，凭借其极强的扩散引导能力，C为GAN提供了针对当前加密任务的唯一标识。

1.4.2　混沌引导的条件GAN生成基础扩散密钥

本文使用条件生成对抗网络（GAN）来生成扩散密钥。其中，生成器G采用经典的U-Net结构，利用其编码器—解码器结构及跳跃连接，将原始明文图像中提取的特征向量C映射为高维的图像级矩阵。判别器D采用了PatchGAN架构，同样接收特征向量C作为条件输入，确保了生成的密钥与图像特征之间的关联性。本算法的训练数据选自公开的COVID-CT-Dataset数据集，共筛选出约346张CT切片，并结合不同用户密钥构造出1 038组混沌哈希特征向量—噪声—理想密钥训练三元组[15]。该数据集以8∶1∶1的比例划分为训练集、验证集和测试集。所有图像经去标识化后统一转换为灰度图像，调整分辨率至256×256，并归一化至[-1，1]，优化器选用Adam，生成器与判别器的初始学习率分别设为1×10^{-4}和5×10^{-6}，Batch size设为8，总计训练35个Epoch，此时生成器的损失函数趋于平稳。训练生成器G采用的复合损失函数如式（14）所示。

$$\mathrm{L_G} = \lambda_{\mathrm{adv}}\mathrm{L_{adv}} + \lambda_{\mathrm{crypto}}(\mathrm{L_{entropy}} + \mathrm{L_{corr}}) \tag{14}$$

其中，$\mathrm{L_{entropy}}$=0.05为负熵损失，旨在迫使像素值趋向均匀分布；$\mathrm{L_{corr}}$为相关性惩罚，旨在消除相邻像素间的统计关联。同时，为了保证密钥的不可预测性，利用分数阶4D Chen系统生成的混沌噪声向量Z注入生成器中。生成器G接收条件C和噪声Z，输出一个与明文图像尺寸一致的浮点矩阵。由于GAN输出通常在[-1，1]区间，需将其映射量化至[0，255]，如式（15）所示。

$$K_{base} = \left\lfloor \frac{G(C,Z) + 1.0}{2.0} \times 255.0 \right\rfloor \tag{15}$$

其中，$\mathrm{K_{base}}$为基础扩散密钥矩阵。

1.4.3　自适应混沌精炼

为了消除神经网络输出可能存在的弱相关性，本文在GAN生成基础密钥$\mathrm{K_{base}}$后加入了精炼模块，在不改变图像语义的前提下，对密钥矩阵进行空间异构化处理。首先，利用统一PRN子种子派生的精炼模块子序列$\mathrm{P_{refine}}$驱动线性投影层映射至图像空间，生成一个随机的与原图等大的矩阵$\mathrm{W_{proj}}$。为了保证非线性特征，用Sigmoid函数进行归一化得到$\mathrm{M_{int}}$。随后，遍历基础密钥矩阵$\mathrm{K_{base}}$的每个像素点(i,j)，根据Mint(i, j)的数值决定该点的处理深度。本文设定了一个处理程度阈值$\mathrm{T_{refine}}$=0.3，该阈值经过大量实验测试选定，旨在平衡加密强度与计算负载，使算法能更好地强化处理图像。如果$\mathrm{M_{int}}(i, j) < \mathrm{T_{refine}}$，则不进行精炼；如果$\mathrm{M_{int}}(i, j) \geqslant \mathrm{T_{refine}}$，则启动精炼。精炼轮次计算如式（16）所示。

$$Rounds(i,j) = \begin{cases} 0, & if\ M_{int}(i,j) < T_{refine} \\ R_{\min} + \left\lfloor \dfrac{M_{int}(i,j) - T_{refine}}{1 - T_{refine}} \times (R_{\max} - R_{\min}) \right\rfloor, & if\ M_{int}(i,j) \geqslant T_{refine} \end{cases} \tag{16}$$

其中，$\mathrm{R_{min}}$=1，$\mathrm{R_{max}}$=5，最多精炼5次。

在具体的自适应精炼阶段，从专用伪随机流$\mathrm{P_{refine}}$中提取随机数值，对基础密钥像素执行多轮模加变换。像素值

加随机数后进行 mod256 运算，从而有效消除生成对抗网络在生成过程中可能残留的结构化统计特征，进一步提升密钥的随机性。

1.4.4 最终扩散合并

将置乱图像 S_{img} 与精炼后的密钥矩阵进行异或合并 $Ciphertext = S_{img} \oplus K_{refined}$，扩散与密钥生成流程如算法 4 所示。

算法 4 扩散与密钥生成

输入：置乱图像 S_{img}，生成器 G，I，K，PRN 统一子种子 P

输出：最终密文 C_{out}

```
H0←SHA256(SHA256(I)//K)
S0←Init_Chaos_State(H0,θ)
For t=1 to Nf do:
  Ht←SHA256(Ht-1//Serialize(St-1))
  St←Fractional_Chen_Step(St-1,Ht)
C←Quantize(SNf,HNf)
Z←P.derive(P,"noise_z",100)
Kraw←G(C,Z)
Kbase←⌊(Kraw+1)×127.5
PRNproj←P.derive(p,"proj_matrix",100)
Mint←Sigmoid(Reshape(PRNproj·C))
Krefined←Kbase.copy()
PRNref←P.derive(p,"refine_stream",100)
For each pixel (i,j) in Krefined do:
  If Mint(i,j)≥Tthreshold then:
    r←Rmin+⌊Mint(i,j)-Trefine1-Trefine×(Rmax-Rmin)
    For k=1 to r do:
      p←PRNref.next_byte()
      Krefined(i,j)←(Krefined(i,j)+p)
    EndFor
  End
End
Cout←Simg⊕Krefined
Return Cout
End
```

2 性能分析

本文针对提出的 FGC-RDH 加密算法进行全面的安全性评估与性能测试。实验环境基于 Python3.12 开发，硬件配置如下：处理器为 Intel Core i9；内存为 16 GB；显卡为 NVIDIA GeForce RTX 3060。测试数据涵盖了 COVID-CT-Dataset[15] 和 Retinal OCT[16]。其中，COVID-CT-Dataset 是实验的核心数据集，主要用于算法的基础性能测试与网络训练。该数据集包含丰富的肺部 CT 切片。此类 CT 图像具有极其典型的医学影像特征以及高度聚集的内部组织纹理，在空间上存在极强的冗余度与统计相关性，极易遭受统计分析攻击。实验中，所有测试图像均统一预处理为 256×256 尺寸的 8 位灰度图。图 3 展示了部分 COVID-CT 影像。

Retinal OCT 数据集相较于肺部 CT，视网膜 OCT 影像在灰度分布上呈现出截然不同的层状纹理与高频散斑噪声特征。该数据集用来验证本文算法在面对不同医学成像模态下的跨模态泛化能力。图 4 展示了部分视网膜 OCT 影像。

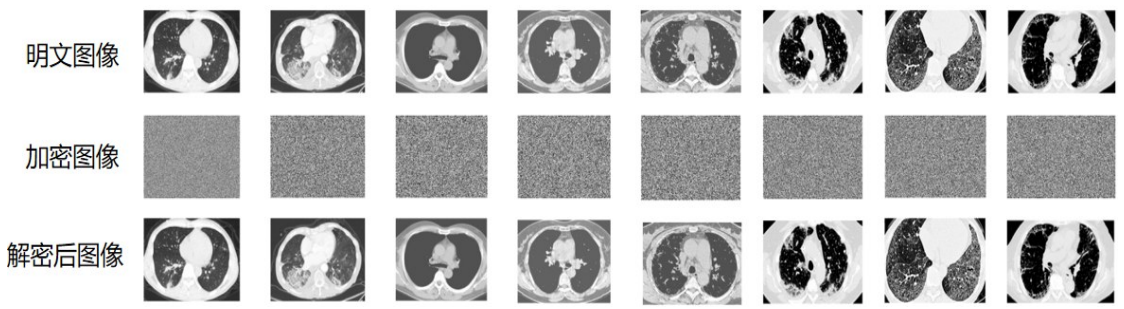


Fig. 3 Encryption and decryption experiments of COVID-CT from C-1 to C-8

图 3 COVID-CT 的加密和解密实验 C-1 至 C-8

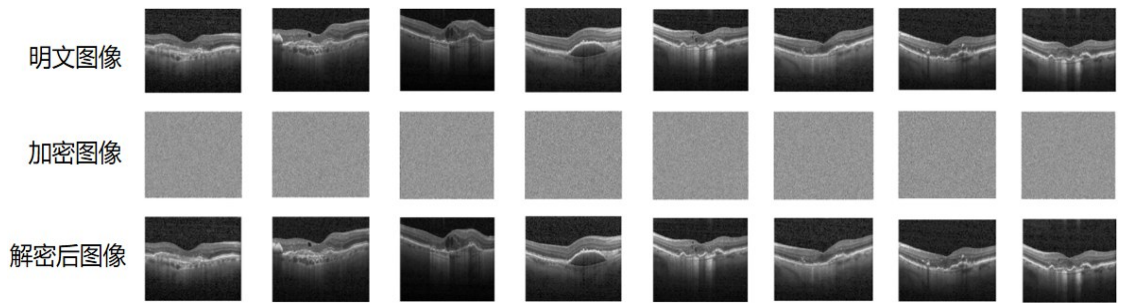


Fig. 4 Encryption and decryption experiments of Retinal OCT images from R-1 to R-8

图 4 Retinal OCT 视网膜图像的加密和解密实验 R-1 至 R-8

2.1　差分攻击与敏感性分析

差分攻击是密码分析者常用的手段，通过观察明文微小差异在密文中产生的波动来推测密钥。评估该特性的核心指标是像素变化率（the Number of Pixels Change Rate，NPCR）和统一平均变化强度（Unified Average Changing Intensity，UACI）。其计算公式分别如式（17）—式（18）所示。

$$NPCR = \frac{1}{w \times h} \times \sum_{i,j} D(i,j) \times 100\% \tag{17}$$

$$UACI = \frac{1}{w \times h} \times \sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{255} \times 100\% \tag{18}$$

其中，$D(i,j)$ 为差异指示函数，当两幅密文图像在 (i,j) 处像素值不同时取 1，否则取 0。$w \times h$ 为图像总像素数，C 和 C′ 分别为原始与修改后明文的加密结果。

2.1.1　明文敏感性测试

在实验中，对原始医学图像随机选取坐标为 (x,y) 的像素点，施加单位级灰度扰动（±1），保持加密密钥不变。通过像素变化率（NPCR）与统一平均变化强度（UACI）来进行量化评估。若指标显著低于理论理想值，说明算法对输入的微小改变缺乏足够的扩散能力。对图 3 中前 5 个明文样本随机修改一个像素点，并记录对应密文的统计特性变化，实验统计结果汇总如表 1 所示。数据显示，FGC-RDH 算法在多组测试图像上的 NPCR 均值超越了 99.60%，UACI 值稳定在 33.50% 左右。相比于传统加密算法，FGC-RDH 算法对明文图像敏感，并且在抵抗差分攻击方面表现出色。

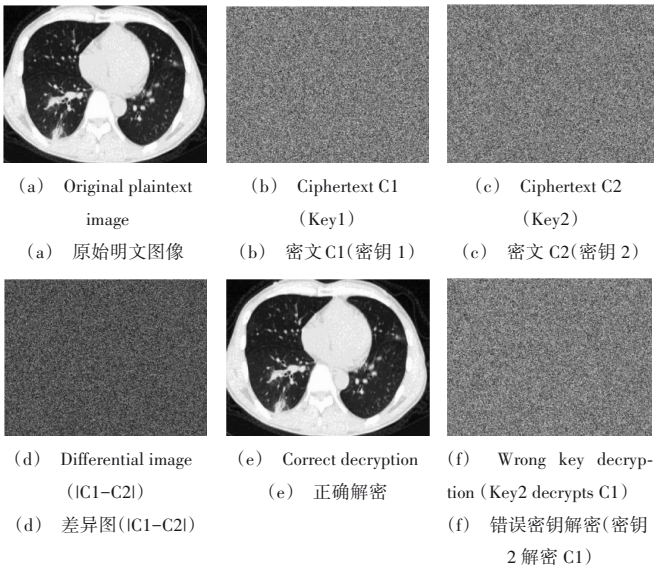
Table 1　Comparison of different metrics for plaintext and ciphertext images

表 1　明文和密文图像不同指标的比较

测试图像	NPCR /%	UACI /%	明文熵	密文熵	PSNR	加密时间/s	解密时间/s
C-1	99.611	33.439	6.873 4	7.999 3	6.741	4.993	3.336
C-2	99.612	33.441	7.110 9	7.998 3	7.298	4.891	3.483
C-3	99.068	33.485	6.788 9	7.998 8	6.362	6.087	4.043
C-4	99.609	33.452	6.905 9	7.998 0	6.544	4.535	1.453
C-5	99.620	33.427	6.402 6	7.998 9	7.169	3.614	2.377
R-1	99.607	33.485	6.245 4	7.997 0	6.918	4.627	3.568
R-2	99.607	33.464	7.052 2	7.997 6	6.667	4.432	3.592
R-3	99.598	33.490	7.107 4	7.997 7	6.955	3.603	2.552
R-4	99.615	33.414	6.593 1	7.997 4	6.873	4.753	3.748
R-5	99.619	33.388	6.593 2	7.997 1	6.989	4.649	3.574
平均	99.611	33.448	6.767 3	7.998 0	6.852	4.620	3.619

2.1.2　密钥敏感性

加密方案必须保证在密钥空间内任意 1 bit 的差异均能产生完全不相关的加密结果。实验对 480 bit 主密钥中的随机一位执行翻转操作。首先，使用原始密钥 Key1 生成密文 C1；其次，通过随机翻转 Key1 中的任意一个比特位构造微偏密钥 Key2，并使用 Key2 对同一原图进行加密得到 C2。密钥敏感性测试结果如图 5 所示。通过对比 C1 与 C2 产生的差异图，其像素差异率 NPCR 达到 99.64%，变化强度 UACI 为 33.53%。上述指标均极度逼近密码学理想值，这表明加密阶段对密钥是非常敏感的。当尝试使用错误密钥 Key2 解密由 Key1 生成的密文时，解密结果呈现出彻底的噪声化特征，完全无法辨识原始结构和信息。



(a) Original plaintext image　(b) Ciphertext C1 (Key1)　(c) Ciphertext C2 (Key2)

(a) 原始明文图像　(b) 密文C1(密钥 1)　(c) 密文 C2(密钥 2)

(d) Differential image (|C1−C2|)　(e) Correct decryption　(f) Wrong key decryption (Key2 decrypts C1)

(d) 差异图(|C1−C2|)　(e) 正确解密　(f) 错误密钥解密(密钥 2 解密 C1)

Fig. 5　Key sensitivity test

图 5　密钥敏感性测试

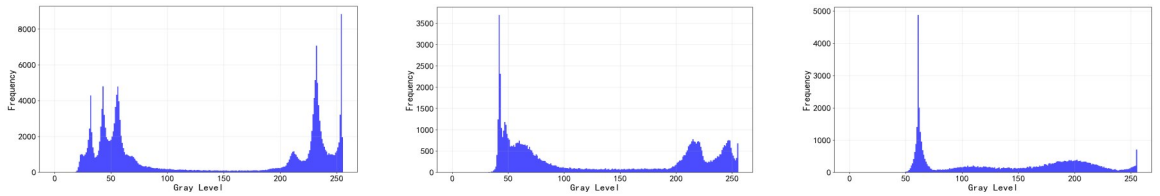
2.2　统计分析

2.2.1　灰度直方图评估

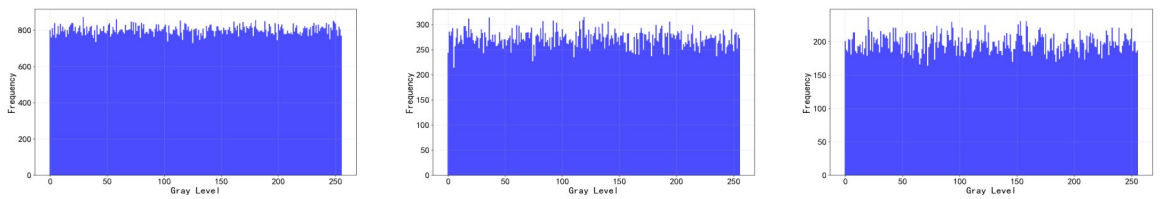
医学图像（如 CT 影像）通常包含大量的背景噪声抑制和组织聚集区，其直方图表现出极强的不平衡性和尖锐的波峰。统计攻击正是利用密文像素值的频率分布或空间关联性来破译原始信息。鉴于医学影像具有极强的结构特征，若加密算法不能彻底消除其统计分布特征，攻击者极易通过分析像素频率规律获取敏感的诊断隐私。实验选取图 3 中第 1、第 2 和第 5 张明文图像以及其经 FGC-RDH 算法加密后的密文图像进行对比分析，其直方图分布如图 6 所示。加密前的明文图像具有明显的灰度偏好；而经过 FGC-RDH 算法处理后，密文直方图转变为极度平滑的矩形分布。这表明密文像素分布在统计上达到了均匀分布。

2.2.2　相邻像素的相关性分析

原始医学影像在空间维度上存在极强的冗余度，其相邻像素关联度通常较高。若加密后仍存在强相关性，攻击者可利用空间冗余进行纹理重组或轮廓提取。为评估算法对空间相关性的破坏能力，本实验在密文图像的水平、垂直及对角线 3 个方向随机采样 5 000 对相邻像素。其相关性分布如表 2 所示。实验数据表明，加密后的相关系数由明文的 0.95 以上（最高达 0.997 0）显著下降至 0.004 以下。此外，其相关性散点图如图 7 所示，直观展示了这一转变：明文像素点紧密围绕 45° 对角线分布，而密文像素点均匀充斥于 255×255 的二维相平面，证明空间关联已被彻底剥离。



（a） Plaintext histogram（image 1）
（a） 明文直方图(图像1)
（b） Plaintext histogram（image 2）
（b） 明文直方图(图像2)
（c） Plaintext histogram（image 5）
（c） 明文直方图(图像5)



（d） Ciphertext histogram（image 1）
（d） 密文直方图(图像1)
（e） Plaintext histogram（image 2）
（e） 密文直方图(图像2)
（f） Plaintext histogram（image 5）
（f） 密文直方图(图像5)

Fig. 6 Histograms

图 6 直方图

Table 2 Correlation values of plaintext and ciphertext in horizontal, vertical and diagonal directions

表 2 明文和密文的水平、垂直和对角线方向的相关性值

图像	水平			垂直			对角线		
	R	G	B	R	G	B	R	G	B
明文	0.9964	0.9970	0.9965	0.9547	0.9567	0.9586	0.9936	0.9935	0.9932
密文	0.0025	0.0032	0.0027	0.0022	0.0019	0.0021	−0.0005	−0.0011	−0.0008

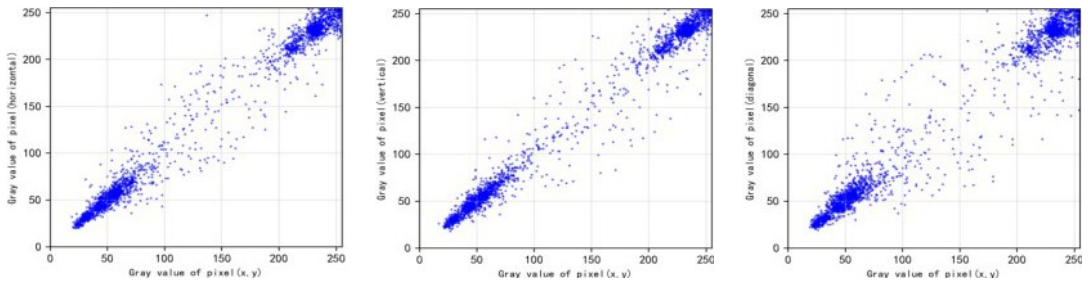
2.2.3 信息熵分析

信息熵是评估加密算法安全性的重要指标之一，用来反映图像的灰度值是否分布均匀，定义如式(19)所示。

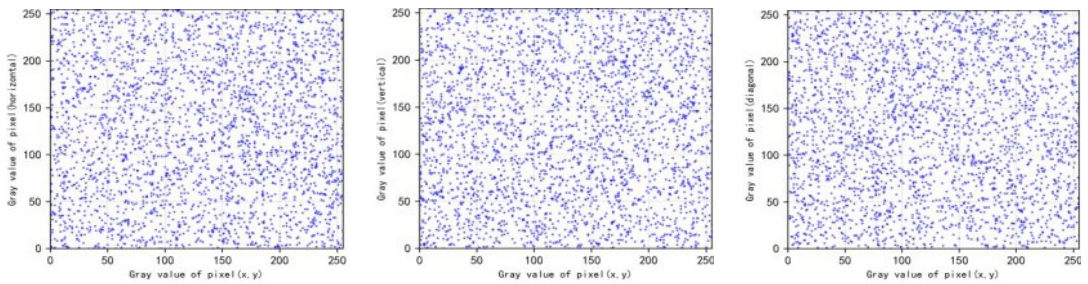
$$H = -\sum_i p_i \log_2 p_i \tag{19}$$

其中，p_i是第i个灰度级的概率。256级灰度医学图像的理论最大信息熵为8比特/像素，该值是评估密文图像随机性与安全性的重要指标。其值越接近8，表明加密对原始医学数据的扰乱越彻底，抗统计攻击的能力也越强。

图4中C-1至C-5医学图像的明文和密文的信息熵如表3所示。所测医学图像的明文图像信息熵分布范围为



（a） Plaintext Horizontal Correlation
（a） 明文水平相关性
（b） Plaintext Vertical Correlation
（b） 明文垂直相关性
（c） Plaintext Diagonal Correlation
（c） 明文对角线相关性



（d） Ciphertext Horizontal Correlation
（d） 密文水平相关性
（e） Ciphertext Vertical Correlation
（e） 密文垂直相关性
（f） Ciphertext Diagonal Correlation
（f） 密文对角线相关性

Fig. 7 Correlation analysis

图 7 相关性分析

6.4~7.1，经过FGC-RDH加密算法处理后得到的密文图像信息熵分布范围为7.998~7.999。结果表明，其对原始医学数据的扰乱较为彻底，具有高度安全性。

Table 3　Comparison of different performance metrics for plaintext and ciphertext of images C-1 to C-5 in Fig.4

表 3　图4 中C-1至C-5图像明密文不同性能指标的比较

测试图像	NPCR /%	UACI /%	明文熵	密文熵	PSNR	加密时间/s	解密时间/s
C-1	99.611	33.439	6.873 4	7.999 3	6.741	4.993	3.336
C-2	99.612	33.441	7.110 9	7.998 3	7.298	4.891	3.483
C-3	99.068	33.485	6.788 9	7.998 8	6.362	6.087	4.043
C-4	99.609	33.452	6.905 9	7.998 0	6.544	4.535	1.453
C-5	99.620	33.427	6.402 6	7.998 9	7.169	3.614	2.377

2.3　可逆数字水印（RDH）的功能性验证

医学影像具有极高的诊疗价值和法律严肃性。该实验旨在验证算法在确保数据机密性的同时，是否具备数据溯源与完整性校验的能力。针对医学诊断对影像数据完整性的严苛要求，并兼顾医学图像的版权保护与完整性校验需求，FGC-RDH算法集成了可逆水印模块。衡量水印性能的核心指标为峰值信噪比（Peak Signal-to-Noise Ratio，PSNR），是图像处理领域评价信号质量常用的客观标准。PSNR通过计算原始图像与嵌入水印后图像之间的均方误差（MSE），以实现对图像失真程度的量化表征。其单位为分贝（dB），数值越大，表示两幅图像在像素层面的差异越小，图像的保真度越高。实验选取CT等典型医学影像为测试样本，当嵌入5 000 bit元数据时，前后的视觉效果与残差分析结果如图8所示。由图8可知，明文图像的PSNR仍保持在45 dB以上，当PSNR高于40 dB时，人眼几乎无法察觉图像的细微改动。嵌入水印后的载体图像在视觉上与原始图像保持了高度一致，并且从放大20倍后的残差图可以观察到，水印信号呈类噪声分布。此外，在解密流程，算法能以100%的准确率提取元数据，并还原原始明文。

（a）Original image
（a）原始图像

（b）Watermarked image（PSNR=45.21dB，SSIM=0.988 0）
（b）含水印图像（峰值信噪比=45.21分贝，结构相似性=0.988 0）

（c）Residual image（×20）
（c）残差图像（放大20倍）

Fig. 8　Experimental results of function of verification reversible digital watermarking

图 8　验证可逆数字水印功能实验结果

2.4　跨模态泛化能力验证

为验证本文离线预训练的GAN扩散密钥生成网络是否具备在未见数据和不同成像模态下的泛化能力，避免模型对训练集（COVID-CT数据集）产生过拟合，本文选取了未经网络训练的Retinal OCT数据集进行了跨模态泛化测试[16]。R-1至R-5五幅视网膜OCT图像的测试结果如表4所示。尽管视网膜影像在组织纹理、灰度分布与背景噪声特征上与肺部CT图像存在巨大差异，但本文算法生成的密文信息熵依然稳定在7.997 0~7.997 7；在抵抗差分攻击的性能上，NPCR值稳定在99.598%~99.619%，UACI值约为33.388%~33.490%，均达到了密码学的理想安全标准。上述指标与在COVID-CT同源测试集上的结果高度一致，这充分证明了训练得到的生成器实质上学习到了由混沌哈希特征驱动的强扩散密码学映射规律，而非仅记住了特定影像的表观特征。

Table 4　Comparison of different performance metrics for plaintext and ciphertext of images R-1 to R-5 in Fig. 4

表 4　图4 中R-1至R-5图像明密文不同性能指标的比较

测试图像	NPCR /%	UACI /%	明文熵	密文熵	PSNR	加密时间/s	解密时间/s
R-1	99.607	33.485	6.245 4	7.997 0	6.918	4.627	3.568
R-2	99.607	33.464	7.052 2	7.997 6	6.667	4.432	3.592
R-3	99.598	33.490	7.107 4	7.997 7	6.955	3.603	2.552
R-4	99.615	33.414	6.593 1	7.997 4	6.873	4.753	3.748
R-5	99.619	33.388	6.593 2	7.997 1	6.989	4.649	3.574

2.5　算法理论分析与多分辨率性能测试

本文从理论层面系统评估了FGC-RDH算法的安全性与执行效率。在安全性方面，根据现代密码学的安全准则，为了有效抵抗穷举暴力破译，加密算法的理论密钥空间应至少达到2^{128}。本算法采用SHA-256算法生成256 bit外部主密钥K，奠定2^{256}的基础安全等级；分数阶4D Chen超混沌系统的4个初始状态值(x_0, y_0, z_0, w_0)、4个系统参数(a, b, c, d)及分数阶阶次α，在10^{-15}计算精度下形成约2^{448}的浮点参数空间（$\log_2(10^{135}) \approx 448$）。综上，算法理论总密钥空间$S$突破$2^{700}$，远超安全阈值，表明其可在高性能计算环境下有效抵御各类穷举攻击。

在执行效率方面，算法的设计充分权衡了安全强度与运行速度。基于分数阶混沌的PRN派生、可逆水印嵌入及双层置换操作均为像素级遍历计算。然而，智能扩散模块基于训练架构，在线加密仅需执行单次前向推理。因此，算法整体的时间复杂度保持在$O(H \times W)$级别。为了验证这一理论推导并评估算法在不同临床模态下的适用性，实验选取了从128×128到1 024×1 024四种分辨率进行测试，结果如表5所示。

Table 5　Comparison of performance and security under different image resolutions

表5　不同图像分辨率下的性能与安全性对比

图像尺寸	加密时间/s	解密时间/s	密文信息熵	NPCR/%	UACI/%
128×128	1.145 0	0.714 3	7.997 2	99.61	33.50
256×256	4.824 0	2.938 2	7.998 1	99.59	33.38
512×512	15.630 3	10.392 7	7.999 4	99.61	33.48

由表5可知，随着图像像素总数以4倍的倍率增长，加解密耗时同步呈现线性增长趋势，这与前述 $O(H \times W)$ 复杂度分析吻合。同时，无论图像尺寸如何变化，密文信息熵均稳定在7.99以上，NPCR与UACI等差分攻击指标也始终保持在理想阈值附近。这表明，FGC-RDH算法能够实现在不同尺寸医学影像处理中的性能伸缩与安全稳定性。

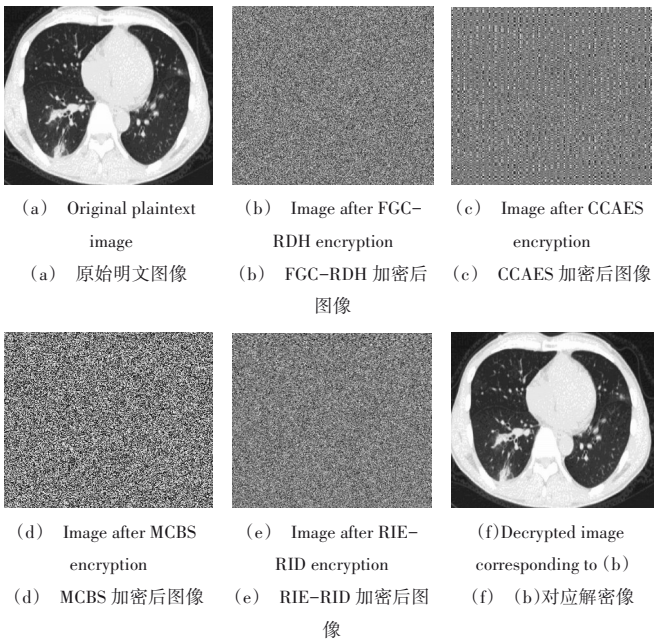
2.6 对比实验

为系统验证所提加密算法的综合性能，本文对算法进行了综合性能评估，并与当前主流的图像加密方法（RIE-RID[9]、CCAES[17]、FOLS[10]和MCBS[10]）进行了对比实验，实验结果如表6所示。评估指标涵盖了加密算法的关键性能维度，包括敏感性、统计特性、执行效率以及功能扩展性等多个方面。上述各加密算法的加密结果如图9所示。实验测得的NPCR与UACI等关键指标均极度逼近理论理想值，这与近年针对高维分数阶系统的安全性评估结论相一致[18]。

Table 6 Comparison with other algorithms

表 6 与其他算法的比较

算法	NPCR/%	UACI/%	密文熵	PSNR	加密时间/s	解密时间/s	水平	垂直	对角线
本文算法	99.616	33.443	7.999 1	6.331	4.824	2.938	0.001 7	0.001 1	0.000 2
CCAES[17]	99.596	33.926	7.977 9	7.537	5.013	4.369	−0.066 4	0.290 6	0.039 7
RIE-RID[9]	99.632	33.634	7.997 2	7.440	19.236	19.50	0.012 6	0.033 3	0.012 2
FOLS[10]	99.678	30.806	7.676 7	7.409	0.428	0.078	0.004 3	0.033 5	0.017 2
MCBS[8]	99.620	33.463	7.997 3	6.331	2.993	1.051	0.000 8	0.003 1	0.003 4



(a) Original plaintext image (a) 原始明文图像
(b) Image after FGC-RDH encryption (b) FGC-RDH 加密后图像
(c) Image after CCAES encryption (c) CCAES 加密后图像
(d) Image after MCBS encryption (d) MCBS 加密后图像
(e) Image after RIE-RID encryption (e) RIE-RID 加密后图像
(f) Decrypted image corresponding to (b) (f) (b)对应解密像

Fig. 9 Encryption results of different encryption algorithms

图 9 不同加密算法的加密结果

RIE-RID算法结合了扫描技术、El-Gamal公钥加密算法和混沌系统[9]。该算法虽然通过多层置乱机制提升了逻辑复杂度，但从表6可以直观发现，该算法的运算开销极大，加密耗时高达19.236 s，难以满足医学影像实时处理的需求。同时，其采用像素级公钥处理方式，在消除图像空间相关性方面的表现同样平庸，难以适配高敏感医疗数据的防护要求。这种高复杂度带来的高延迟在多层置乱架构中普遍存在，使得该类算法在临床应用中受到限制[19]。

CCAES算法利用Arnold混沌序列生成加密密钥，结合改进后的AES结构进行加密[17]。实验结果显示，该算法在统计安全性上存在明显短板：其密文信息熵仅为7.977 9，显著低于本文算法，且其垂直方向的相关系数高达0.290 6。这表明，Arnold机制在处理高冗余医学图像时存在固有缺陷，导致密文随机性不足，极易遭受统计分析攻击。

FOLS算法基于分数阶Lorenz-Stenflo模型并结合忆阻器特性实现加密[10]。该算法的优势在于极高的运算速度（耗时仅0.248 s），但这种效率是以牺牲安全性为代价的。实验数据显示，FOLS算法的UACI为30.806%，显著低于理想理论值，这说明该算法对图像像素的扰动强度不足且分布不均，抵抗差分攻击的能力较弱。

MCBS算法通过卷积神经网络（CNN）与宽度学习系统（BLS）动态生成扩散密钥，并利用S盒及循环移位机制执行图像置乱[8]。实验结果显示，该算法在NPCR与UACI等敏感性指标上表现良好，但其置乱逻辑主要依赖于线性的行/列循环移位。这种方式对像素间空间关联性的破坏深度有限，导致其在处理高冗余医学影像时，对角线方向的相关系数（0.003 4）显著高于本文算法。

相比之下，本文提出的FGC-RDH算法在安全性与执行效能之间取得了较优的平衡。在统计随机性方面，算法的密文信息熵达到了7.999 1，不仅高于上述3种算法，也超越了MCBS（7.997 3），展现了极致的伪随机分布特性。在空间去相关化维度，其对角线方向的相关系数低至0.000 2，较MCBS（0.003 4）也有降低，证明了FGC-RDH算法在破坏图像空间结构方面效果较为显著。由于引入了条件GAN生成器、分数阶超混沌迭代以及可逆数字水印等多种新技术，导致加解密时间有所上升，但相较于牺牲安全性以换取极速的FOLS算法，这种时间开销的增加是实现安全提升与数据溯源功能所必需的成本权衡[10]。当与具备同等高安全性的算法相比，RIE-RID算法加密耗时高达19.236 s，难以满足现代医疗系统的实时性需求，而FGC-RDH算法的加密耗时仅约为其1/4。本文方案在保证医疗影像高度安全的同时，利用cGAN优化了扩散机制，

实现了安全强度与执行效率的深度权衡,符合当前医学图像加密技术的发展态势[20]。

3　结语

本文提出了FGC-RDH算法,针对医学影像加密场景中安全性和数据溯源性等问题,提供了一种高安全性的防护方案。该算法通过融合SHA-256哈希增强机制与分数阶4D Chen超混沌系统,构建了高强度的统一伪随机数生成机制,并以此驱动动态分数阶S盒与Hilbert空间填充曲线置换,实现了像素值与像素位置的深度重构,大大削弱了原始明文图像在空间与统计维度上的强相关性。在扩散阶段,算法创新性地利用混沌哈希特征向量引导条件生成对抗网络(cGAN)生成扩散密钥。除基本加密功能外,算法集成了明文域可逆数字水印技术,为图像数据提供了可靠的版权保护与溯源能力。通过在COVID-CT数据集上的实验验证表明,本文算法在信息熵、相关性以及明文/密钥敏感性等多项指标上均优于RIE-RID[9]、CCAES[17]和FOLS[10]等现有主流算法。结果表明,该算法能够有效抵御各类统计分析与差分攻击,是医疗影像保护场景下的理想选择。相较于传统算法,FGC-RDH算法由于引入了生成对抗网络(GAN)和复杂的分数阶混沌迭代,兼顾了计算开销与安全强度之间的平衡。未来的研究将重点探索AI模型的轻量化部署及硬件加速技术,以进一步提升在大规模实时医疗影像传输场景中的运行效能。

参考文献:

[1] HOSNY K M, ZAKI M A, LASHIN N A, et al. Multimedia security using encryption: a survey[J]. IEEE Access, 2023, 11: 43210-43235.

[2] FAN W, ZHANG D, WU J, et al. Color image encryption based on a fractional-order hyperchaotic system and cross-plane bit-level permutation and eight-base DNA-level diffusion[J]. Physica Scripta, 2025, 100(9): 095225.

[3] MENG F, WU G, ZHANG J. A novel color image encryption algorithm based on fractional-order conservative memristive hyperchaotic system and extended zig-zag transform[J]. Journal of King Saud University-Computer and Information Sciences, 2025, 37: 151.

[4] YU F, XU S, LIN Y, et al. Design and analysis of a novel fractional-order system with hidden dynamics, hyperchaotic behavior and multi-scroll attractors[J]. Mathematics, 2024, 12(14): 2227.

[5] SINGH O P, SINGH K N, SINGH A K, et al. Deep learning-based image encryption techniques: fundamentals, current trends, challenges and future directions[J]. Neurocomputing, 2025, 612: 128714.

[6] HUANG Q X, YAP W L, CHIU M Y, et al. Privacy-preserving deep learning with learnable image encryption on medical images[J]. IEEE Access, 2022, 10: 66345-66355.

[7] ASIF M, KUMAR L, SWAMI G, et al. High-capacity reversible data hiding using deep learning[C]//Proceedings of 2021 Asian Conference on Innovation in Technology (ASIANCON), 2021: 1-5.

[8] QIAO Z X, XIE Y T, YAO S X, et al. Medical image encryption algorithm based on chaotic systems and machine learning[J]. Software Guide, 2024, 23(8): 129-135.
乔子轩, 谢雨桐, 姚苏昡, 等. 基于混沌系统和机器学习的医学图像加密算法[J]. 软件导刊, 2024, 23(8): 129-135.

[9] YOUSIF S F, ABBOUD A J, RADHI H Y. Robust image encryption with scanning technology, the El-Gamal algorithm and chaos theory[J]. IEEE Access, 2020, 8: 155184-155209.

[10] KHAN N A, QURESHI M A, AKBAR S, et al. From chaos to encryption using fractional order Lorenz-Stenflo model with flux-controlled feedback memristor[J]. Physica Scripta, 2023, 98(1): 014002.

[11] MAN Z L, LI J Q, DI X Q, et al. Double image encryption algorithm based on neural network and chaos[J]. Chaos, Solitons & Fractals, 2021, 152: 111318.

[12] ZHU X Q, LIU J Q, ZHANG D L, et al. Enhancing patient privacy in IoT-enabled intelligent systems: a deep and broad learning-based efficient encryption network[C]//International Conference on Smart Internet of Things (SmartIoT), 2024: 51-58.

[13] ZHANG H B, LI C G, CHEN G R, et al. Hyperchaos in the fractional-order nonautonomous Chen's system and its synchronization[J]. International Journal of Modern Physics C, 2005, 16(5): 815-826.

[14] KRAWCZYK H, ERONEN P. HMAC-based extract-and-expand key derivation function (HKDF): RFC 5869[S]. Internet Engineering Task Force, 2010.

[15] HE X H, YANG X Y, ZHANG S H, et al. Sample-efficient deep learning for COVID-19 diagnosis based on CT scans[EB/OL]. https://www.researchgate. net/publication/340721185_Sample-Efficient_Deep_Learning.

[16] KERMANY D S, GOLDBAUM M, CAI W, et al. Identifying medical diagnoses and treatable diseases by image-based deep learning[J]. Cell, 2018, 172(5): 1122-1131.

[17] ARAB A, ROSTAMI M J, GHAVAMI B. An image encryption method based on chaos system and AES algorithm[J]. The Journal of Supercomputing, 2019, 75: 6663-6682.

[18] CAI S, SHU T, HUANG L, et al. A medical image encryption algorithm based on a 4D fractional-order hyperchaotic system and DNA sequence coding[J]. Scientific Reports, 2022, 12(1): 11442.

[19] WANG X, XU L, WANG S, et al. A multi-layered image encryption scheme using deep learning and chaos[J]. Expert Systems with Applications, 2023, 213: 119045.

[20] ZHOU N, LI H, WANG D, et al. Image encryption based on conditional generative adversarial network and hyperchaotic system[J]. Optics and Lasers in Engineering, 2021, 143: 106631.

(责任编辑:陈维捷)