

基于混沌系统与机器学习的医学图像加密算法

乔子轩¹, 谢雨桐¹, 姚苏眩¹, 朱晓强², 姚英英²

(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)

摘要: 随着医疗行业信息化进程的加速, 承载着患者隐私、临床数据等多方面敏感信息的医疗图像加密保护已成为业界关注的热点问题。目前学术界和工业界普遍采用像素置乱、混沌系统和机器学习等方法对医疗图像进行加密保护, 但这些方法仍存在算力资源浪费、加密密钥缺乏保护、加密速率低、密钥空间小等问题。为解决以上问题, 提出一种基于混沌系统及神经网络的新型图像加密算法——MCBS算法。该算法首先利用S盒及循环移位对医疗图像进行置乱, 然后使用经混沌系统加密后的由神经网络和宽度学习网络输出的矩阵密钥与置乱后的图像进行异或运算, 实现图像的像素扩散, 最后利用数字签名技术为医疗图像的传输过程提供保护。在安全性能分析实验中, 将MCBS算法与RIE-RID、CCAES和FOLS算法进行了比较, 结果表明, 该算法在相关性值和PSNR等方面均处于领先水平。

关键词: 混沌系统; 机器学习; 医学图像; 图像加密

DOI: 10.11907/rjdk.251353

扫描二维码阅读全文:



中图分类号: TP309

文献标识码: A

文章编号: 1672-7800(XXXX)0XX-0001-12

Medical Image Encryption Algorithm Based on Chaotic Systems and Machine Learning

QIAO Zixuan¹, XIE Yutong¹, YAO Suxuan¹, ZHU Xiaoliang², YAO Yingying²

(1. School of Software, Beijing Jiaotong University;

2. School of Cyberspace Science and Technology, Beijing Jiaotong University, Beijing 100091, China)

Abstract: With the acceleration of informatization process in the medical industry, the encryption protection of medical images, which carry sensitive information such as patient privacy and clinical data, has become a hot issue in the industry. At present, pixel disruption, chaotic system and machine learning are commonly used in academia and industry to encrypt and protect medical images, but these methods still have problems such as waste of arithmetic resources, lack of protection of encryption key, low encryption rate, and small key space. In order to solve the above problems, this paper proposes a new image encryption algorithm based on chaotic system and neural network, MCBS algorithm, which firstly utilizes the S-box and logical chaotic system to disrupt the medical images; and then uses the matrix key encrypted by chaotic system and outputted from neural network and width learning network to perform a heterosynthesis operation with the disrupted image. Then the matrix key output from the neural network and the width learning network encrypted by the chaotic system is used to carry out the different-or operation with the disordered image to realize the pixel diffusion of the image; finally, the digital signature technology is used to provide protection for the transmission process of medical images. In the security test, this paper compares the MCBS algorithm with the mainstream RIE-RID, CCAES and FOLS algorithms. The results show that the MCBS algorithm outperforms the others in terms of correlation and PSNR.

Key Words: chaotic system; machine learning; medical image; image encryption

收稿日期: 2025-06-30

基金项目: 国家自然科学基金项目(62401037); 国家重点研发计划项目(2023YFB2703702); 中国博士后科学基金会项目(GZC20230224, 2024M750166); 北京交通大学人才基金项目(2023XKRC016)

作者简介: 乔子轩(2004-), 女, 北京交通大学软件学院学生, 研究方向为机器学习; 谢雨桐(2004-), 女, 北京交通大学软件学院学生, 研究方向为隐私保护; 姚苏眩(2004-), 女, 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, 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; 姚英英(1994-), 女, 博士, 北京交通大学网络空间安全学院助理教授, 研究方向为密码学。本文通讯作者: 朱晓强。

0 引言

随着物联网(Internet of Things, IoT)技术的快速发展,在医疗领域,每日有着海量的医疗图像产生,这些图像涉及患者的个人隐私和医疗状况等多方面敏感信息。因此,针对此类图像加密算法的研究具有重要意义。当前的主流加密方法主要分为置乱和扩散两个关键过程。置乱过程通过改变像素元素的位置或顺序来破坏原始像素结构,从而隐藏原始图像特征;扩散过程则通过改变像素值或位置的方式,使明文图像信息分散到整个密文图像中。这些过程涉及的核心算法包括像素置乱、盲源分离、神经网络及混沌系统等^[1]。

在各类加密技术中,混沌系统因其具有的随机性而被广泛应用于图像加密算法的置乱过程中。自1989年Matthews^[2]首次提出混沌密码学理论以来,该技术得到了迅速发展。目前,应用于加密图像领域的混沌系统主要分为连续型和离散型两大类。在离散混沌映射研究方面,Alawida^[3]提出混沌映射增强算法(Enhanced Logistic Map, ELM)。相较于经典的Logistics混沌映射,该算法不仅增强了Logistics混沌系统加密的安全性,而且扩展了混沌范围,提高了遍历率并优化了算法性能。另一方面,在高维混沌系统研究方面,Wei等^[4]设计的新型分数阶3D洛伦兹混沌系统被运用于图像加密,并由此提出了MIEA-FCSM(Multi-image Encryption Algorithm Based on the New Fractional-order 3D Lorenz Chaotic System and 2D-SCPM)算法。实验结果证明,新型3D洛伦兹混沌系统不仅扩大了密钥空间,而且增强了加密算法的安全性,且MIEA-FCSM算法的加密时间缩减至0.150 4 s,有着显著的效率优势。该算法相比低维混沌系统安全性更高,又比高维混沌系统计算负担更小,且像素变化率(the Number of Pixels Change Rate, NPCR)达到了99.757%^[5]。

除上述置乱过程外,扩散过程在图像加密中也是不可或缺的一部分。扩散步骤能够将明文图像中的信息分散到整个密文中,使得每个像素的变化都影响到全局,以此来抵抗选择明文攻击和已知明文攻击。传统的扩散方式包括超混沌系统驱动扩散、交叉扩散、双向扩散等。近年来,利用DNA编码的扩散方法和基于机器学习的扩散方法也得到了迅猛发展。Chen等^[6]将2D Hénon-Sine映射与DNA编码相结合,通过DNA随机编码及异或操作实现扩散,不仅具有优良的安全性能,而且拓宽了DNA编码在图像加密领域的应用范围。Wang等^[7]提出的基于改进Logistics映射和双图混合的加密算法,通过明文关联置乱和混沌扩散,显著扩大了满映射时控制参数的取值范围,提升了系统抵抗差分攻击的能力。Shao^[8]提出一种结合4D混沌系统的并行彩色图像加密方法,通过三通道同时加密,将加密时间压缩至1 s内。Ding等^[9]提出的DeepKey-

GenA (Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption)利用对抗网络将密钥空间扩大至 $(2^8)^{196\ 608}$,同时实现了高达7.98的信息熵和极高的敏感性。

虽然现有图像加密算法在置乱与扩散阶段已实现了较高的安全性能,但仍存在算力资源浪费、计算效率和安全性难以兼顾及密钥缺少保护等问题。Yousif等^[10]提出一种结合扫描技术、El-Gamal公钥密码体制和混沌系统的鲁棒性图像加密算法(以下简称RIE-RID算法),该算法利用EL-Gamal加密算法完成置乱过程,扩散过程则由Lorenz和Rössler两类混沌系统完成。RIE-RID算法大幅提高了密钥空间的复杂度,但在加密耗时和计算效率方面均有所欠缺。Khan等^[11]提出的分数阶Lorenz-Stenflo(Fractional Order Lorenz-Stenflo, FOLS)算法基于新型五维Lorenz-Stenflo混沌系统和忆阻器特性进行图像加密,该算法的置乱与扩散阶段皆由混沌系统实现,成功地将加解密时间压缩至0.12 s,但也导致了加密安全性下降。在神经网络图像加密领域,Man等^[12]提出一种双图像加密算法,该算法将图像特征作为卷积神经网络的卷积核,使得双图加密效率相比单图串行处理有着明显提升,但也导致了单张有效图像加密时算力资源的浪费。Zhu等^[13]将卷积神经网络(Convolutional Neural Network, CNN)和宽度学习(Broad Learning System, BLS)相结合提出一种高效深度与广度学习加密网络(Efficient Deep and Broad Learning-Based Encryption Network, EDBNet),该网络在医学图像加密方面有着很高的加密速率,但其CNN矩阵密钥较为直接,存在与原图特征重合的可能性,进而导致CNN密钥易被破译。

为了解决以上问题,本文提出MCBS(Multi-Chaotic System Algorithm Based on CNN and BLS with S-box)算法。该算法采用S盒(Substitution-box)和Logistics混沌系统进行图像置乱操作,利用卷积神经网络和宽度学习生成的两种矩阵密钥,并结合Lorenz混沌系统加密和异或运算实现像素扩散,最后将数字签名作为传输保护措施融入图像加密算法。该算法在增强安全性的同时,降低了计算复杂度,是一种高效的图像加密策略。本文的主要贡献如下:

(1)对EDBNet进行改进,引入S盒对医疗图像进行加密。该算法以其独特的混淆和扩散特性,能够有效打乱医疗图像的像素值分布,从而极大地提升医疗图像在存储和传输过程中的保密性。

(2)对卷积神经网络进行修改,将SHA3-256和洛伦兹混沌系统用于CNN架构中,将CNN的特征进行置乱加密,为CNN的矩阵密钥提供有效保护,进而抵御各类针对特征数据的攻击。

(3)在信息传输方面采取数字签名技术,通过对加密后图像的哈希值进行签名处理,接收端能够准确验证数据在传输过程中是否被篡改,同时确认数据来源的可靠性,

为医疗图像信息在不同设备间的传输提供保障。

1 本文算法

1.1 概述

本节将概述 MCBS 算法的加密过程, 图 1 展示了加密流程的整体框架。该加密过程包括置乱、扩散以及添加数字签名认证, 以确保加密后的图像具有高度的安全性。

(1) 置乱。本阶段采用双通道混淆机制实现像素级置乱。首先引入动态 S 盒替换策略, 该策略基于椭圆曲线和莫比乌斯变换生成非线性替换表, 对原始像素值进行双向非线性映射, 消除图像统计的相关性。随后使用洛伦兹和逻辑混沌系统分别生成两个混沌序列作为移位密钥, 对图像块执行双向循环移位操作, 破坏图像空间的相关性。

(2) 扩散。本阶段采用双流加密, 联合卷积神经网络和宽度学习系统构建双特征驱动扩散器。首先使用混沌序列生成 CNN 的一个卷积核, 通过预训练 CNN 提取图像的边缘特征矩阵形成第一个矩阵密钥, 随后采用广度学习微调模型获得第二个特征矩阵密钥。最后通过异或运算对置乱后的图像进行扩散。该设计利用 CNN 的局部特征捕获能力与 BLS 的快速全局关联特性, 显著提升了密钥的敏感性与扩散效率。混沌系统的引入也对密钥进行了有效保护。

(3) 数字签名认证。在加密终端引入 RSA 算法 (Rivest-Shamir-Adleman) 对加密图像哈希值进行签名处理。此步骤在加密完成后执行, 并随加密图像一同传输。该机制不仅可验证数据的完整性, 而且可通过公钥验证实现身份溯源, 为传输安全提供保障。

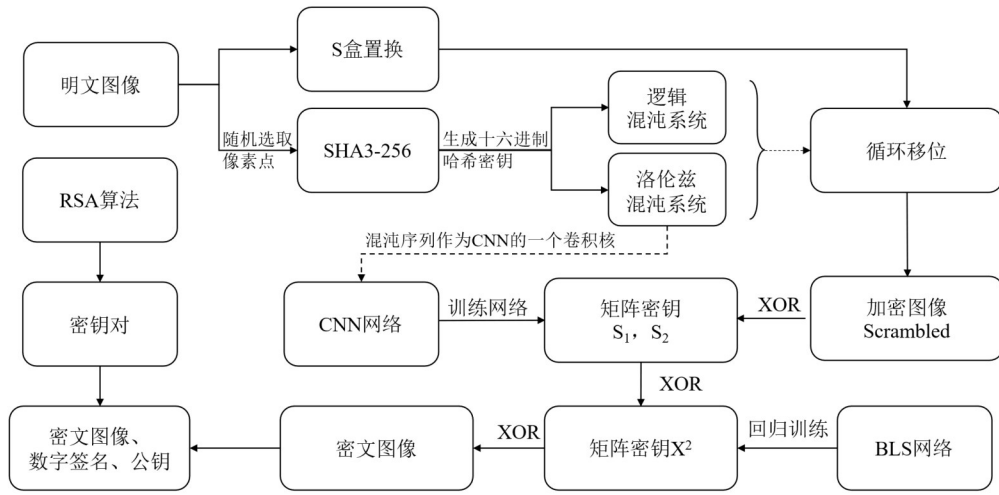


Fig. 1 Image encryption flow

图 1 图像加密流程

1.2 算法实现过程

1.2.1 置乱

本节将详细描述置乱阶段所使用的 S 盒和循环移位的加密流程, 该双层置乱结构有效提升了算法对差分攻击与相关性分析的抵抗能力。

首先, 介绍所使用的 S 盒生成算法及其加密流程。该算法由 Bilal 等^[14]开发, 使用了两个代数结构: 椭圆曲线 EC 和伽罗瓦域上的莫比乌斯变换, 以生成具有高非线性度的 S 盒。根据射影一般线性群 $PGL(2, GF(x))$ 对伽罗瓦域 $GF(x)$ 的作用规则, 本文定义莫比乌斯变换形式如下:

$$\begin{cases} T: PGL(2, GF(x)) \times GF(x) \rightarrow GF(x) \\ T(z) = \frac{\alpha z + \beta}{\gamma z + \eta} \end{cases} \quad (1)$$

本文将选取一个椭圆曲线 $E_{p,0,b}$, 提取该曲线上所有点的纵坐标, 据此构造两组整数 C_1 和 C_2 。莫比乌斯变换 $T(z)$ 的参数 β 和 η 从集合 C_1 与 C_2 中动态选择, 而参数 α 和 γ 从集合 $\{011...12^m - 1\}$ 中随机选择。构建长度为 M 的 S 盒

步骤如下: ①要获得一个长度为 M (即 2^m) 的 S 盒, 首先选择一个素数 $p > 2^m$ 和一个随机的整数 $b \in [1, p-1]$, 构建一个椭圆曲线 $E_{p,0,b}$ 。并且, 该素数 p 满足条件: 若素数满足 $p \equiv 2 \pmod{3}$, 则椭圆曲线 $E_{p,0,b}$ 上所有点对应的纵坐标共计 $p+1$ 个, 且取值均不重复; ②取 $E_{p,0,b}$ 上前 2^m 个点的 y 坐标构成一个集合 A ; ③生成两个随机整数集合 B_1 和 B_2 , 其中 $B_i \subseteq [0, 2^m - 1]$ $|B_i| = 2^m$ ($i = 1, 2$), 并基于二者构建集合 C_1 和 C_2 。对于 $i = 1, 2$, $C_i = (A + B_i) \bmod 2^m$; ④对于莫比乌斯变换 $T(z) = \frac{\alpha z + \beta}{\gamma z + \eta}$, 首先选择参数 $\beta \in C_1$ 和 $\eta \in C_2$, 再随机选择参数 $\alpha, \gamma \in \{0, 1, \dots, 2^m - 1\}$ 。为避免奇点, 需注意额外条件 $\alpha\eta - \beta\gamma \neq 0$ 和 $\gamma z + \eta \neq 0$; ⑤对于输入 $z = 0, 1, \dots, 2^m - 1$, 莫比乌斯变换 $T(z) = \frac{\alpha z + \beta}{\gamma z + \eta}$ 的输出即为所需的 S 盒。

S 盒生成算法的伪代码如下:

算法 1 S 盒生成算法

Input: Choose the parameters $p > 2^m$, where $m = \log_2 M$ and $b \in [1, p-1]$.

Output: The required S-box.

Begin

Make sure $p \equiv 2 \pmod{3}$;

Calculate the points on the EC $\mathbb{E}_{p,0,b}$;

From the EC points, choose the first 2^m elements of the y-coordinate and design a set A;

Select two random sets of integers s.t. $B_i \subseteq [0, 2^m - 1]$ and $|B_i| = 2^m$ for $i = 1, 2$;

Compute the two sets C_1 and C_2 : $C_i = (A + B_i) \pmod{2^m}$ for $i = 1, 2$;

Choose the parameters α, γ from $O = \{0, 1, \dots, 2^m - 1\}$, and β, η from C_1 and C_2 respectively;

Let $x = 0; 2^m - 1$;

Galois field $z = GF(m)$;

Initialize set $S_1 = []$;

for $j = 1$ to 2^m do

$$f_1 = \alpha(j) \times z(j) + \beta(j);$$

$$f_2 = \gamma(j) \times z(j) + \eta(j);$$

if $\alpha(j) \times \eta(j) - \beta(j) \times \gamma(j) \neq 0$ and $\gamma(j) \times z(j) + \eta(j) \neq 0$ then

$$S_2 = \frac{f_1}{f_2};$$

$$S_1 = [S_1, S_2];$$

End if

End for

End

下面介绍如何应用动态 S 盒加密算法。S 盒加密算法主要包括两个阶段:扩散阶段和置乱阶段。在扩散阶段,生成随机数用于扩散明文图像,以增加图像中的随机性,使其能够抵御差分攻击。之后,采用 S 盒对扩散后的图像像素进行置换。在置乱阶段,生成两个 S 盒分别用于置换图像的行和列。该加密方案不同阶段的详细步骤如下:

(1) 选择一个椭圆曲线 $\mathbb{E}_{p',0,b'}$, 使得 $p' \equiv 2 \pmod{3}$, 且 $p > w \times h$ 。

(2) 用扩散排序打乱 $\mathbb{E}_{p',0,b'}$ 上的点。若 (x_1, y_1) 和 (x_2, y_2) 是椭圆曲线上的两个点, 则扩散排序定义如下:

$$(x_1|y_1)O(x_2|y_2) \Leftrightarrow \begin{cases} \text{either } x_1 + y_1 < x_2 + y_2, \text{ or} \\ x_1 + y_1 = x_2 + y_2, \text{ and } x_1 < x_2 \end{cases} \quad (2)$$

(3) 将 $\mathbb{E}_{p',0,b'}$ 上点的 y 坐标构建成为一个大小为 $w \times h$ 的集合 K_1 , 作为按 y 坐标升序排列时的索引向量。

(4) 对于一个大小为 $w \times h$ 的图像 I , 将图像 I 转换为大小为 $1 \times wh$ 的行向量 K_2 。为使用集合 K_1 扩散图像 I 的像素, 需要构建 $K_3 = (K_1 + K_2) \pmod{256}$, 再将行向量 K_3 重塑为大小为 $w \times h$ 的中间图像 K_4 。

(5) 使用算法 1 生成长度为 w 和 h 的两个不同的 S 盒

σ 和 λ , 分别用于打乱图像 K_4 的行和列, 以减少图像 K_4 像素间的相关性。

(6) 图像 K_4 经过 S 盒 σ 和 λ 的置乱后, 得到加密图像 C 。

在使用 S 盒算法进行置乱后, MCBS 算法需要使用循环移位操作对图像进行第二次置乱。

以下介绍循环移位的加密流程, 本文利用两种混沌系统生成循环移位所需的置乱索引。首先, 从明文图像中随机选取一个像素值, 利用字符串“980aFs09f”构造哈希函数生成器, 采用 SHA3-256 算法得到 64 位十六进制哈希密钥“9eb544472bae67d6e554edbe37a99b2e7cdaa6aa7dbceac9dae63d541f7f67e6”。之后, 根据公式(3)进行分割, 得到洛伦兹混沌系统的 3 个初始值。

$$initKey = \frac{\text{int}(\text{hashKey}[n:n+4], 16)}{w \times h} \pmod{1}, n = 1, 6, 11 \quad (3)$$

3 个初始值将通过如公式(4)所示的洛伦兹混沌方程进行多轮迭代:

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dy}{dt} = x(\rho - z) - y \\ \frac{dz}{dt} = xy - \beta z \end{cases} \quad (4)$$

其中, 将混沌系统的参数 σ, ρ, β 分别设置为 10、40、8/3。当 ρ 为 40 时, 该混沌系统的随机性更强。鉴于需要为明文图像的每一行分配混沌扰动参数, x 将依据公式(5)迭代 w 次。行混沌置乱索引的计算方法如公式(6)所示:

$$x_{i+1} = x_i + dx_i \times 0.01 \quad (5)$$

$$row_i = \text{round}(\text{abs}(x_i) \times 10^6) \% w \quad (6)$$

其中, $x_0 = initKey$, $\text{abs}(\cdot)$ 表示绝对值, $\text{round}(\cdot)$ 表示向下取整。每一轮的 x 将加入混沌序列尾部, 最后得到长度为 w 的序列 Seq_c 。

对于列置乱, 通过逻辑混沌系统生成另一个混沌序列, 以增强所提出密码系统的不确定性。同样地, 需要为明文图像每一列分配一个混沌扰动参数。因此, y 将根据公式(7)迭代 h 次。列混沌置乱索引的计算方法如公式(8)所示:

$$y_{j+1} = 3.6789 \times y_j \times (1 - y_j) \quad (7)$$

$$col_j = \text{round}(\text{abs}(y_j) \times 10^6) \% h \quad (8)$$

其中, $y_0 = (row_w / (w \times h)) \pmod{1}$ 。然后, 根据 row_i 和 col_j 对加密图像 C 实施二次置乱处理。通过两个索引 row_{arg} 、 col_{arg} 分别对图像 C 同一行和同一列的元素进行右循环移位与左循环移位, 最终得到置乱后的加密图像 $Scrambled$ 。

1.2.2 扩散

本节将详细介绍 MCBS 算法中, 通过卷积神经网络和

宽度学习获得两种矩阵密钥并进行像素扩散的过程。

(1) 卷积神经网络矩阵密钥获取。本文主要采用 CO-VID-CT-Dataset 开展 MCBS 算法的加密性能测试, 该数据集由两类标签的肺部图像构成^[15]。基于数据集特征, 本文设计了三层卷积层以生成两个矩阵密钥, 从而根据标签属性进行图像加密。除结合数据集特征外, 本文还通过设计精简的 5 层架构实现了更高的训练效率和较好的图像特征提取能力, 具体架构如图 2 所示。

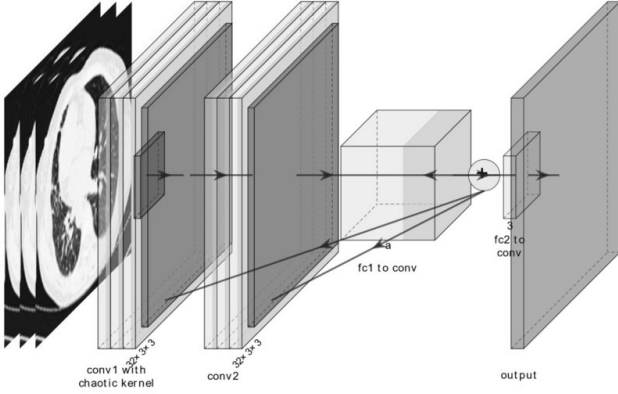


Fig. 2 The architecture of convolutional neural network

图 2 卷积神经网络架构

为提升 MCBS 算法在不同医学数据集上的适应性和泛化性, 其卷积神经网络架构设计会根据数据集标签数量调整卷积层层数, 从而生成更丰富且与标签数量形成对应关系的卷积神经网络矩阵密钥。不同标签的图像在经过后续“利用异或操作实现扩散”部分所述的映射判断后, 与不同的矩阵密钥进行异或加密。对于复杂数据集, 通过生成更多矩阵密钥以提升密钥复杂度, 进而防止密钥被破译, 提升密钥的安全性。在卷积核结构上, 相较于边缘检测中使用水平梯度和垂直梯度的卷积核进行卷积计算, MCBS 使用置乱章节循环位移部分的混沌序列 Seq_c 进行填充, 通过 $w \times h$ 维度的矩阵重塑操作, 将其作为第一卷积层的卷积核 K_{seq} 。卷积计算如公式(9)所示。该设计通过混沌序列的随机性有效保护了矩阵密钥, 避免了 MCBS 算法的神经网络结构被直接破解。同时, 与图像维度一致的卷积核尺寸可确保医学图像的重要细节信息被保留, 避免局部特征丢失。第二层卷积核进行垂直梯度值计算, 如公式(10)所示。其中, (i, j) 表示像素坐标, $I(i + m, j + n)$ 表示强度值。此外, 使用填充以确保图像大小的统一。

$$G_{seq}(i, j) = \sum_{m, n} I(i + m, j + n) \cdot K_{seq}(m, n) \quad (9)$$

$$G_y(i, j) = \sum_{m, n} I(i + m, j + n) \cdot K_y(m, n) \quad (10)$$

本文使用 ReLU 函数作为所有卷积层的激活函数。在卷积层后的池化层中, 用最大池化来降低特征图维数, 而在全连接层和最后的输出层中, 本文设计了前向传播来优化各层卷积权重。使用肺炎图像集进行训练时, 通过梯度

下降算法最小化目标函数。目标函数及梯度下降算法如公式(11)、公式(12)所示。

$$L = - \sum_{i=1}^n (y_i \log(p_i) + (1 - y_i) \log(1 - p_i)) \quad (11)$$

$$\theta = \theta - \alpha \nabla L(\theta, x_i, y_i) \quad (12)$$

其中, y 是真实标签, p 是真实类别的预测概率。获得混沌序列训练神经网络进而获得加密密钥的算法流程如算法 2 所示。最终该算法将会得到与加密图像大小一致的矩阵密钥 S_1 和 S_2 。

算法 2 卷积神经网络密钥生成算法

Input: target image($w \times h$), data set X

Output: matrix S_1 , matrix S_2

Begin

$x, y, z \leftarrow$ get initial Lorenz paraments;

for $i \leftarrow 1$ to w :

Update dx, dy, dz by Eq.4;

Update x by Eq.5;

Add x into chaotic sequence;

End for

Reshaping chaotic sequence into convolution layer1 kernel ma-

trix;

for i in n do:

Train CNN model with filters by Eqs.(9, 10);

Use SGD to minimize the loss function by Eqs.(11, 12);

End for

Reshape convolution layer 1 weights into matrix $S_1(w \times h)$;

Reshape convolution layer 2 weights into matrix $S_2(w \times h)$;

End

由卷积神经网络生成的矩阵密钥主要基于卷积层的裁剪模式生成, 攻击者需要通过模型输出逆向推导卷积核的裁剪模式。基于混沌序列构建卷积核, 再结合卷积核裁剪模式的随机性, 有效提升了逆向推导难度。此外, 复杂数据集具备数量更丰富的卷积核, 卷积核数量的增加也显著提升了密钥熵的理论值。

(2) 宽度学习矩阵密钥获取。尽管 MCBS 算法的 CNN 采取了精简的架构以获得更快的训练速度, 但在大规模数据集下, 其计算成本依旧很高。Chen 等^[16]提出宽度学习算法, 不同于深度学习对于神经层深度的扩展, 宽度学习主要探索每层神经元宽度的增加, 具有快速学习的特性。这一特性也较好地解决了计算成本高、训练速度慢的问题。

宽度学习的核心在于快速构建特征节点和增强节点, 并利用伪逆直接求解输出权重, 以避免传统深度学习的迭代训练过程。特征节点的生成包含 3 步: 首先使用随机权重 W_{f_i} 和偏置 β_{f_i} 对训练集 X 进行线性变换, 然后通过非线性激活函数 φ 处理变换结果, 最后的输出即为特征节点 F_i 。具体函数参考算法 3 中的特征节点 F_i 生成部分。增强节点 E_m 由特征节点矩阵 F_n 经随机线性变换(权重 W_{em} 、偏

置 β_{em})后,再通过非线性激活函数 ξ 生成。具体函数参考算法3中的增强节点 E_m 生成部分。最后基于岭回归求解目标函数得到权重 W^* ,将权重 W^* 重塑为 $w \times h$ 大小,即为所需的宽度学习密钥矩阵。

算法3 宽度学习密钥生成算法

Input: dataset (X, y), Number of feature nodes N_f , Number of enhancement nodes N_e , Shrinkage coefficient s, Ridge penalty term λ

Output: matrix $X_s^2(w \times h)$

Begin

Normalize data set X;

Initialize weights and biases for feature nodes and enhancement nodes β_{fi}

for i in n do

Compute feature mappings: $F_i = \varphi(XW_{fi} + \beta_{fi}), i = 1, \dots, n$, φ is activation function;

Get features by $E_m = \xi(F^n W_{en} + \beta_{en}), F^n = [F_1, \dots, F_n]$ while using N_e ;

Minimize the loss by ridge regression ;

$$W^* = \arg \min_w \|HW - y\|^2 + \lambda \|W\|_2^2, H = [F_n | E_m];$$

End for

$X_s^2 = \text{Reshape}(W^*)$;

Return X_s^2 ;

End

不同于卷积神经矩阵密钥的灵活性与普适性,宽度学习矩阵密钥的生成取决于训练过程的随机性和数据集的多样性。权重分布随机性越强,神经元数量越多,宽度学习矩阵密钥的密钥熵相应越高,其抗暴力破解能力也随之增强。双通道矩阵的设计融合了二者优势,在确保MCBS算法对不同复杂程度数据集具备更强适应性的同时,显著提升了算法的抗暴力破解能力。

(3)利用异或操作实现扩散。使用 COVID-CT-Dataset 训练 CNN 和 BLS 模型,该数据集的医学图像按肺部是否患病分为两类,其中标签为0表示健康肺部,标签为1表示患病肺部^[15]。在扩散的最后阶段,MCBS算法将医学图像标签与混沌序列 Seq_e 最后一位的十六进制值相加后进行模2运算。若取余结果为0,则将置乱后的图像与 S_1 矩阵密钥和 X_s^2 矩阵密钥进行异或运算;若取余结果为1,则将置乱后的图像与 S_2 矩阵密钥和 X_s^2 矩阵密钥进行异或运算。通过将混沌序列与数据集标签相结合,有效防范了标签判断条件被直接破解,以避免攻击者推断出卷积神经网络矩阵密钥与标签的映射关系而造成信息泄露。经上述异或操作后便可得出最终的加密图像。

以下给出MCBS算法中实现扩散过程的完整步骤:

首先,使用 Lorenz 混沌系统生成的混沌序列构造 CNN 的部分卷积核,并使用医疗图像数据集完成 CNN 的训练,保存训练所得的 CNN 模型。对模型的两个卷积层权重进行填充与裁剪,以获得与加密图像大小一致的矩阵密钥

S_1 和 S_2 。

其次,训练 BLS,将保存的 BLS 模型中的权重 W^* 进行填充与裁剪,以获得与加密图像大小一致的矩阵密钥 X_s^2 。

再次,根据以下公式获取判断标签:

$$selector = (\text{int}(Seq_e[16]) + label) \% n, n = num_{label} \quad (13)$$

其中, n 为标签个数, $label$ 为当前加密图像的标签值。在使用 COVID-CT-Dataset 进行训练时, n 为 $2^{[15]}$ 。

最后,根据以下公式对置乱后的图像进行异或运算:

$$\begin{cases} \text{Scrambled Image XOR } S_1 \text{ XOR } X_s^2, & \text{if } selector = 0 \\ \text{Scrambled Image XOR } S_2 \text{ XOR } X_s^2, & \text{if } selector = 1 \\ \text{Scrambled Image XOR } S_3 \text{ XOR } X_s^2, & \text{if } selector = 2 \\ \dots\dots\dots \\ \text{Scrambled Image XOR } S_n \text{ XOR } X_s^2, & \text{if } selector = n - 1 \end{cases} \quad (14)$$

在使用 COVID-CT-Dataset 进行训练时,置乱公式如下:

$$\begin{cases} \text{Scrambled Image XOR } S_1 \text{ XOR } X_s^2, & \text{if } selector = 0 \\ \text{Scrambled Image XOR } S_2 \text{ XOR } X_s^2, & \text{if } selector = 1 \end{cases} \quad (15)$$

经异或运算后,即得到了加密后的医学图像。

1.2.3 数字签名

前文已介绍了如何通过置乱和扩散操作加密图像数据,以确保加密过程的安全性和复杂性。为进一步保证加密数据在传输过程中的完整性与真实性,本文使用 RSA 对最终加密图像的哈希值进行数字签名。

数字签名过程使用 RSA 算法生成数字签名密钥对 (PK, SK),其中私钥 SK 主要用于生成加密图像的签名,公钥 PK 则用于验证签名。生成密钥对的具体步骤如下:

(1)加密方随机选择两个 1 024 位的大素数 p 和 q , 计算其乘积 $n = p * q$, 模数 n 作为公钥和私钥的共同部分。

(2)计算欧拉函数值 $\varphi(n) = (p - 1) \times (q - 1)$, 该值表示小于 n 且与 n 互质的正整数个数。

(3)任选一个公钥指数 e , 满足 $\gcd(e, \varphi(n)) = 1$, 确保 e 与 $\varphi(n)$ 互质。

(4)计算私钥指数 d , 满足 $e \times d \equiv 1(\text{mod } \varphi(n))$, 即 e 和 d 的积关于模 $\varphi(n)$ 同余。

使用 SHA-256 算法计算加密图像的哈希值,并使用私钥 SK 对哈希值加密,生成数字签名。数字签名生成的伪代码如下:

算法4 数字签名生成算法

Input: message, private key(n, d)

Output: signatureBegin hash_value $\leftarrow$ SHA256(message);

$m \leftarrow \text{convert_to_integer}(\text{hash_value});$

signature $\leftarrow \text{powmod}(m, d, n);$

Return signature;

End

图3展示了RSA算法在图像数据处理中的应用过程。首先,发送方生成RSA密钥对,其中私钥用于生成数字签名,公钥通过互联网传输给接收方。签名结束后,数字签

名、公钥与加密图像将一同发送给接收方。在接收端处理过程中,接收方首先针对接收到的加密图像 C' 计算哈希值 $H_1(C')$, 然后使用发送方的公钥 PK 对数字签名进行解密, 从而获得原始的哈希值 $H_2(C')$ 。若 $H_1(C') = H_2(C')$, 则表明加密图像未被篡改, 数字签名验证成功, 可继续解密过

程。若验证失败, 则表明数据可能已在传输过程中被篡改或签名无效, 此时接收方应丢弃该数据, 不再进行后续解密操作, 以避免矩阵密钥等内容泄露。数字签名机制在 MCBS 算法中用于保障传输中密文的完整性和来源的真实性, 而不直接参与 MCBS 核心加密密钥的保护。

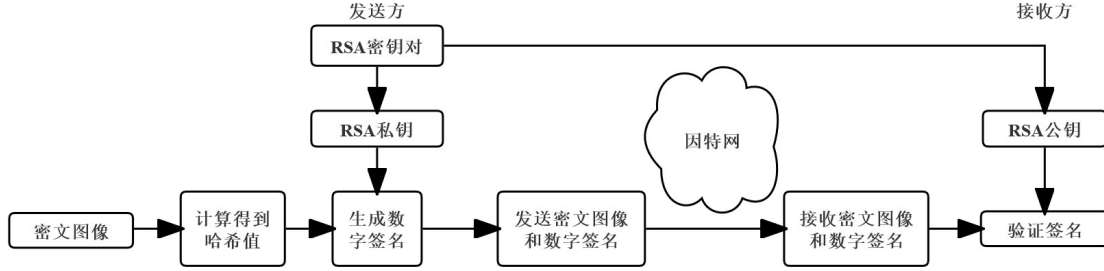


Fig. 3 Application process of digital signature

图3 数字签名应用过程

2 性能分析

本节采用遮挡攻击测试、敏感性分析、统计分析、加密质量分析等多种方法分析 MCBS 算法的性能, 同时与 AES^[17]、RIE-RID^[10] 以及 FOLS^[11] 3 种算法进行详细对比。性能分析采用 COVID-CT-Dataset, 测试环境为配备 16 GB 内存的 Apple M3 CPU, 算法使用 Python 3.12 实现。COVID-CT-Dataset 加密和解密图像如图 4 所示, 从左至右依次

为 No.1 - No.10 图像的加解密结果, 从上至下依次为明文图像、密文图像和解密后的图像。尽管本文实验主要基于 COVID-CT 数据集的 CT 图像完成, 但 MCBS 算法在设计上具有通用性, 也可应用于其他医学图像模态。为验证 MCBS 算法的普适性, 本文另外采用 IXI-Dataset 中的 T1 加权脑部 MRI 图像开展加解密实验与性能测试^[18]。IXI-Dataset 加密与解密图像如图 5 所示, 从左至右依次为 No.11-No.20 MRI 图像的加解密结果, 从上至下依次为明文图像、密文图像和解密后的图像。

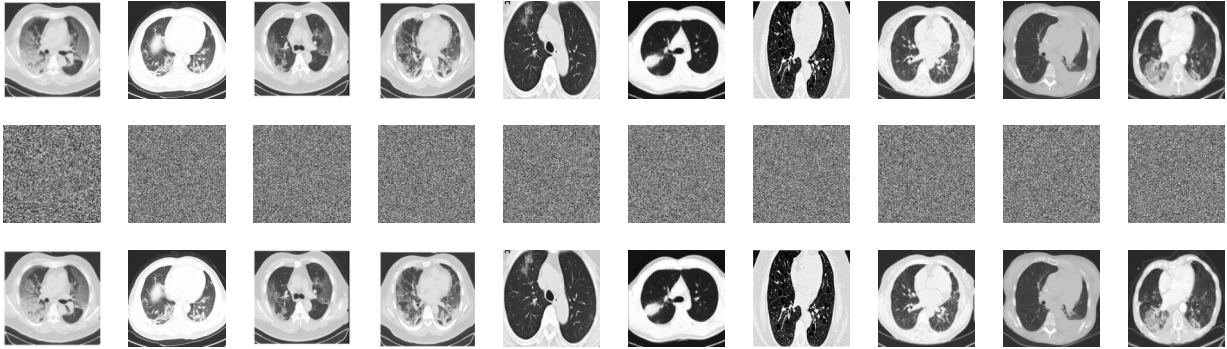


Fig. 4 Encryption and decryption experimental results using COVID-CT-Dataset

图4 COVID-CT-Dataset 加密与解密实验结果

2.1 敏感性分析

差分攻击是评估密码算法安全性的一种常见方法, 常用于检验算法抵御差分攻击能力的两个指标是像素变化率 (the Number of Pixels Change Rate, NPCR) 和统一平均变化强度 (Unified Average Changing Intensity, UACI)。计算公式分别如公式 (16)、公式 (17) 所示:

$$NPCR = \frac{1}{w \times h} \times \sum_{i,j} D(i,j) \times 100\% \quad (16)$$

$$UACI = \frac{1}{w \times h} \times \sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{255} \times 100\% \quad (17)$$

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, C' 分别为原始与修改后明文的加密结果。

较高的 NPCR 和较低的 UACI 表明加密算法对输入变化更敏感, 从而能更好地抵御差分攻击。本文对图 4 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, 实验结果如表 1 所示。结果表明, 大多数测试用例的 NPCR 与 UACI 接近期望值 99.609 4% 和 33.463 5%。因此, 本文提出的 MCBS 算法对明文图像敏感, 并且在抵抗差分攻击方面表现出色。

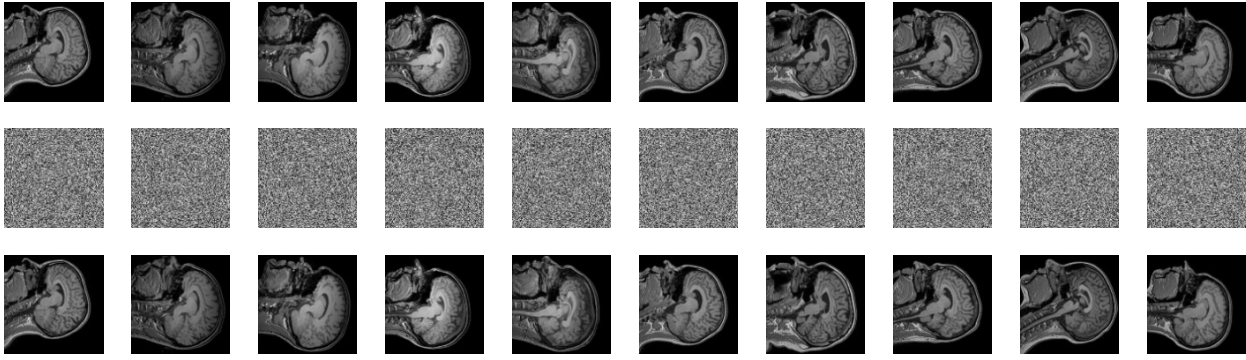


Fig. 5 Encryption and decryption experimental results using IXI-Dataset

图5 IXI-Dataset加密与解密实验结果

Table 1 Comparison of different metrics for plaintext and ciphertext images

表1 明文与密文图像不同指标比较

测试图像	NPCR/%	UACI/%	明文熵	密文熵	PSNR	加密时间/s	解密时间/s
No.1	99.620	33.463	7.0354	7.9973	6.331	2.993	1.051
No.2	99.609	33.458	6.2896	7.9974	6.328	2.931	1.082
No.3	99.571	33.272	7.0427	7.9970	7.395	4.282	1.389
No.4	99.608	33.367	6.9612	7.9972	7.430	3.089	1.147
No.5	99.634	33.525	6.9109	7.9970	7.169	3.318	1.258
No.11	99.606	33.287	6.2454	7.9970	6.918	1.627	1.598
No.12	99.600	33.441	6.3435	7.9973	6.556	1.636	1.581
No.13	99.619	33.594	5.9371	7.9975	6.955	1.603	1.652
No.14	99.609	33.423	6.4332	7.9972	6.844	1.633	1.648
No.15	99.619	33.447	5.6488	7.9971	7.010	1.649	1.614
平均	99.610	33.428	6.4848	7.9972	6.894	2.476	1.402

2.2 统计分析

2.2.1 直方图分析

直方图作为图像安全性分析的重要工具,能够直观反映各灰度级的像素分布频率。在理想情况下,密文图像的直方图应均匀分布。本文实验选取图4中前3幅明文图像及其经MCBS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。其中,图(a)—图(c)是第1~3个明文的直方图,图(d)—图(f)是对应密文的直方图。实验数据显示,相较于明文图像中呈现的显著的灰度聚集现象,密文直方图各灰度级的频次分布趋于相对均衡。该可视化结果表明,MCBS算法通过非线性扩散有效打破了明文图像的统计相关性,使得密文直方图符合均匀分布的随机性标准,从而显著增强了系统抵御统计攻击的能力。

2.2.2 相邻像素相关性分析

在分析图像加密算法时,普遍会通过相邻像素之间的相关性来识别加密图像中的结构。相关性值可以表明加密算法在打乱像素值和引入随机性方面的有效性。为了

分析相邻像素之间的相关性,本文计算了水平、垂直和对角线方向的相关性值。本文实验从图4 No.1的明文图像及其密文图像中随机选取3 000组相邻像素对,其相关性分布如图7所示。其中,图(a)—图(c)分别表示第一个明文的水平、垂直和对角线相关性,图(d)—图(f)是第一个密文的对应分析结果。数值结果如表2所示。统计结果显示,密文图像相邻像素的相关系数降至 0.7500 ± 0.004 ,说明加密后密文图像中相邻像素之间的相关性较弱。以上量化分析证明了本文提出的加密算法能够有效地打乱像素值,并抵抗统计分析或暴力破解等攻击。

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,反映图像的灰度值是否分布均匀,可用于评估密文图像中的随机性和安全性水平。信息熵的定义如下:

$$H = -\sum_i p_i \log_2 p_i \quad (18)$$

其中, p_i 是第*i*个灰度级的概率。若某个灰度级没有出现在图像中,即 $p_i = 0$,则对应的项在求和时应被忽略。对于256级灰度医学图像而言,最大理论信息熵为8比特/像素,这对应于完全均匀的像素分布状态。在加密算法分析中,信息熵指标能够有效量化密文图像的统计随机性水平。数值越接近理想值8,表明加密过程对原始医学数据的混淆程度越高,抵御统计攻击的能力越强。

表1对图4 No.1~No.5医学图像的明文和密文信息熵进行了对比。实验结果表明,5组测试医学图像的明文信息熵分布在6.2~7.1之间,经过MCBS加密算法处理后,密文信息熵提升至7.94~7.98,与理想值的绝对偏差不超过0.06 bit,证明其具有高度的随机性和安全性。

2.3 鲁棒性分析

为了评估本文算法的抗干扰能力,采用遮挡攻击测试

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

表2 明文和密文的水平、垂直与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	0.996 4	0.997 0	0.996 5	0.996 0	0.995 9	0.996 0	0.993 6	0.993 5	0.993 2
密文	0.751 9	0.753 8	0.751 2	0.752 8	0.741 7	0.751 4	0.756 1	0.747 0	0.747 0

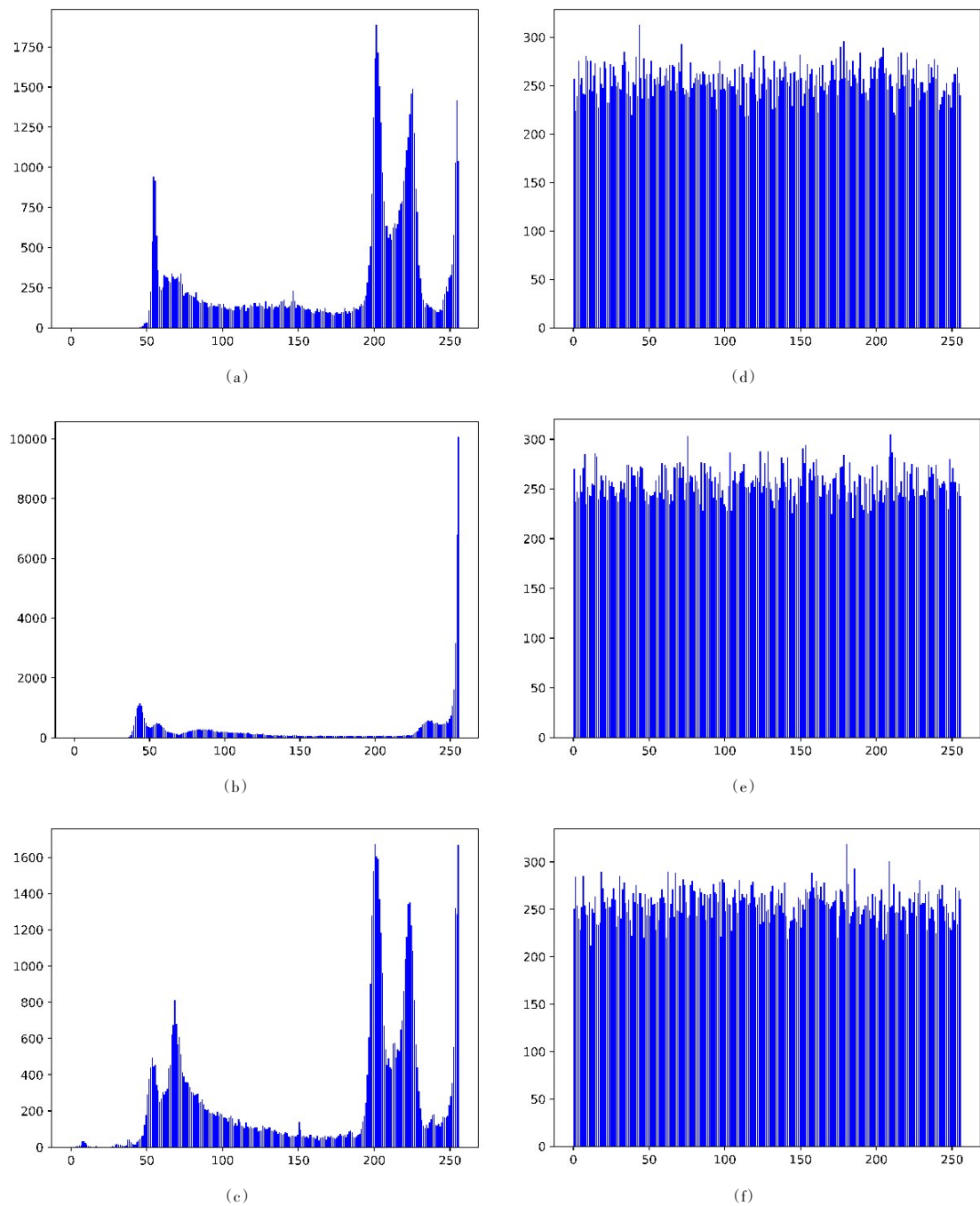


Fig. 6 Comparison of image histograms

图 6 图像直方图对比

和峰值信噪比(Peak Signal To Noise Ratio, PSNR)分析两种方法,系统验证了该算法在信息安全传输领域的抗攻击性能。

(1)遮挡攻击测试。攻击者通常通过移除或修改图像的部分像素,试图破坏其完整性,从而影响解密后的图像质量和信息完整度。高鲁棒性的加密算法应能有效扩散和隐藏原图的局部特征,使得即使加密图像遭受部分裁剪或遮挡,仍能恢复出大部分原始图像信息。为验证本文算法的抗遮挡能力,在加密图像中随机选择3个大小为50×80像素的矩形区域,并将该区域的像素值全部置零,以模

拟数据传输过程中信息丢失的情况。随后,本文使用正确的解密方式对遭受遮挡攻击的加密图像进行解密处理。实验结果如图8所示。该结果表明,即使加密图像遭受了较大面积的遮挡攻击,解密后仍能恢复绝大部分原始图像信息,且加密图像中缺失的像素区域并未导致解密图像中的对应区域出现大规模信息缺失。这一现象充分证明了本文算法对原始图像信息进行了有效的扩散处理,具备出色的加扰性能和抗遮挡攻击能力。

(2) PSNR 值分析。峰值信噪比(PSNR)是图像处理领域广泛应用的质量评估指标,通过计算均方误差(Mean-

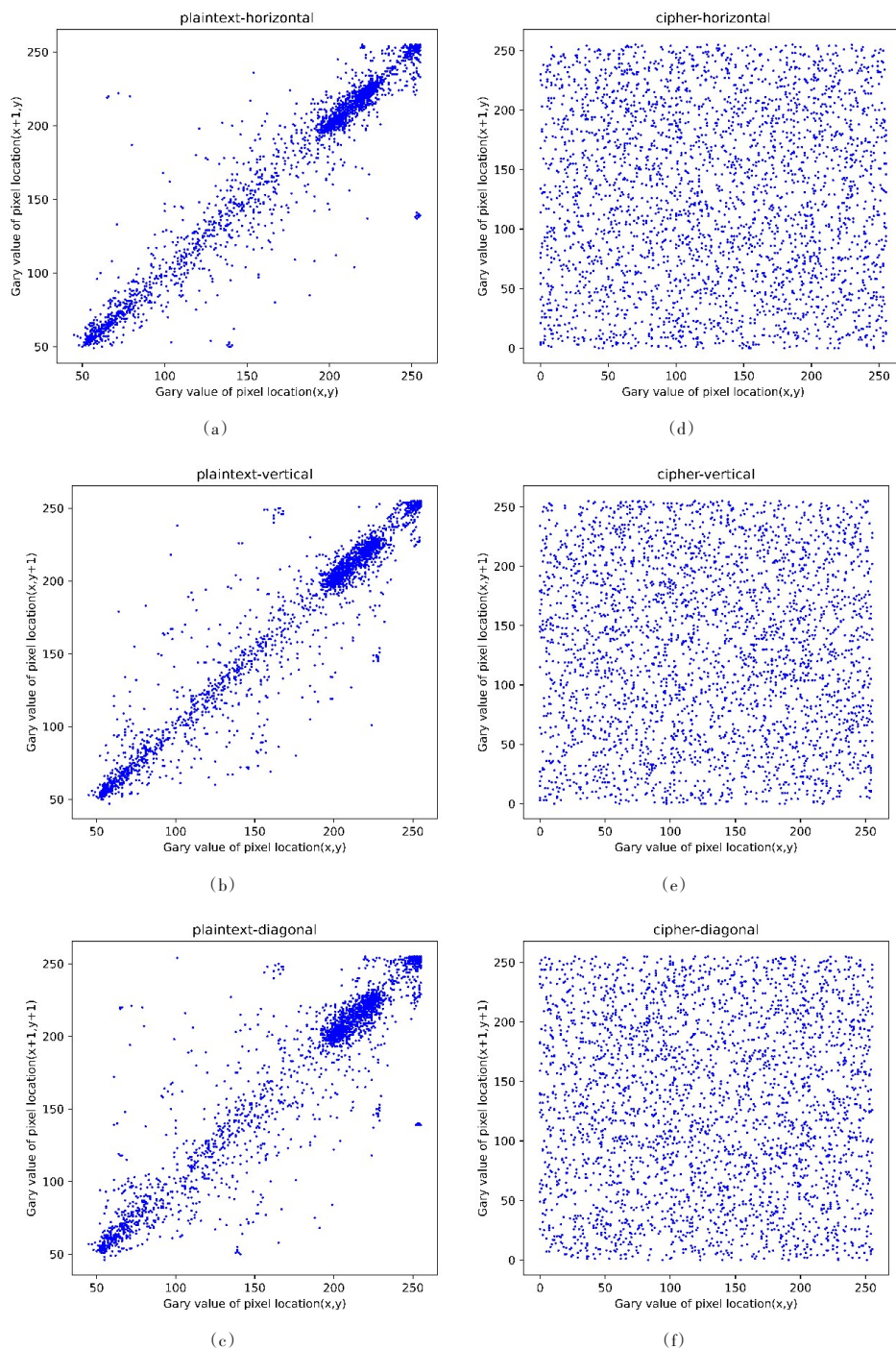


Fig. 7 Correlation analysis

图7 相关性分析

Square Error, MSE)来量化原始图像与处理后图像之间的像素差异,并进一步计算图像像素最大可能值与MSE的比例。在图像加密领域,PSNR值越低,表示原图与加密图像差异越大,加密效果越好。本文仍然使用图4中的图像进行PSNR值分析,实验结果如表1中的PSNR列所示。数据显示,经MCBS算法处理后,原图与加密图像的平均PSNR值约为6.931 dB,远低于图像处理领域普遍认可的可接受阈值(通常为30 dB以上)。这一结果充分表明,加密后的图像与原始图像之间几乎不存在可视相关性,验证了

MCBS算法的有效性。同时,不同图像样本的PSNR值波动范围较小(标准差仅为0.427),证明了本文算法对不同图像类型和内容具有良好的适应性与稳定性。

2.4 对比实验

为验证本文提出的图像加密算法的有效性,本节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^[10]、CCAES^[17]和FOLS^[11])进行了对比实验,实验结果如图9、表3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、随机性、鲁棒性以及计算效率等

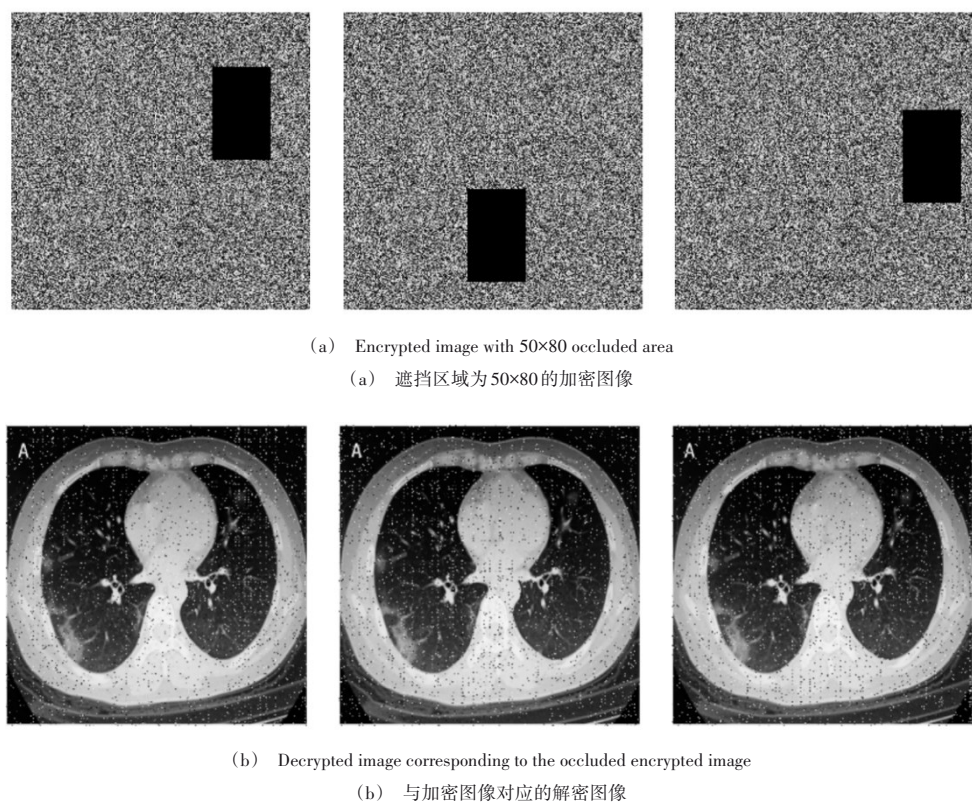


Fig. 8 Occlusion test

图 8 遮挡测试

Table 3 Comparison with different algorithms

表 3 不同算法的比较

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	99.620	33.463	7.997 3	6.331	2.993	1.051	0.000 8	0.003 1	0.003 4
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 ^[10]	99.632	33.634	7.997 2	7.440	19.236	19.500	0.012 6	0.033 3	0.012 2
FOLS ^[11]	99.678	30.806	7.676 7	7.409	0.248	0.078	0.004 3	0.033 5	0.017 2

多个方面。

RIE-RID 算法结合了扫描技术、EL-Gamal 公钥加密算法和混沌系统^[10]。该算法通过锯齿变换和螺旋扫描对图像像素重新进行排列,并使用 EL-Gamal 加密算法对置乱后的图像进行加密。最后使用 Lorenz 系统和 Rössler 系统对图像进行混淆与扩散。虽然 RIE-RID 算法通过高维混沌系统增加了密钥空间的复杂度,但是复杂的算法结构导致计算效率降低。从表 3 可以看出,该算法在加密时间和解密时间上耗时均接近 20 s,无法满足实际需求。

CCAES 算法通过 Arnold 混沌序列生成加密密钥,结合改进后的 AES 算法对原始图像进行加密^[17]。该方法在保持 AES 算法安全性的同时,借助混沌系统增强了算法的扩散能力,使得加密图像具备较强的差分攻击抵抗能力。然而,从表 3 的数据可以得出,CCAES 算法的密文熵值明显低于其他算法,表明其加密结果存在一定的可预测性,因而易受到统计攻击。此外,其垂直方向的相关系数值高达 0.261 2,说明算法在消除图像相关性方面存在缺陷。这可能是因为算法的 Arnold 混沌序列存在周期性,以及行列移

位操作存在缺陷,导致图像加密的随机性不足。

FOLS 算法基于分数阶 Lorenz-Stenflo 模型引入一种新型五维混沌系统,并结合磁通量控制的忆阻器实现图像加密^[11]。其利用分数阶混沌系统的高敏感型和不可预测性生成伪随机序列,实现高效的图像置乱和扩散。该算法简化了分数阶 Logistic 映射运算,具有极高的加密和解密速度。然而,这种高效率牺牲了安全性能。表 3 的数据结果表明,FOLS 算法的 UACI 值显著低于理想值,说明该算法对图像的扰动不均匀,抵抗差分攻击的能力较弱。

本文提出的 MCBS 算法在保持较低计算开销的同时,显著提高了加密图像的安全性。本文采用多阶段加密策略,使用 S 盒置换图像,并且利用混沌序列进行图像行列移位。同时,使用 CNN 特征提取和 BLS 回归进行异或扩散,对生成的加密图像附加数字签名。结合混沌系统、机器学习和密码学,有效提高了加密图像的安全性和不可预测性。实验以及与相关算法的对比结果表明,MCBS 算法具有较强的敏感性与较好的统计特性,同时保证了较高的运行速度和复杂度。

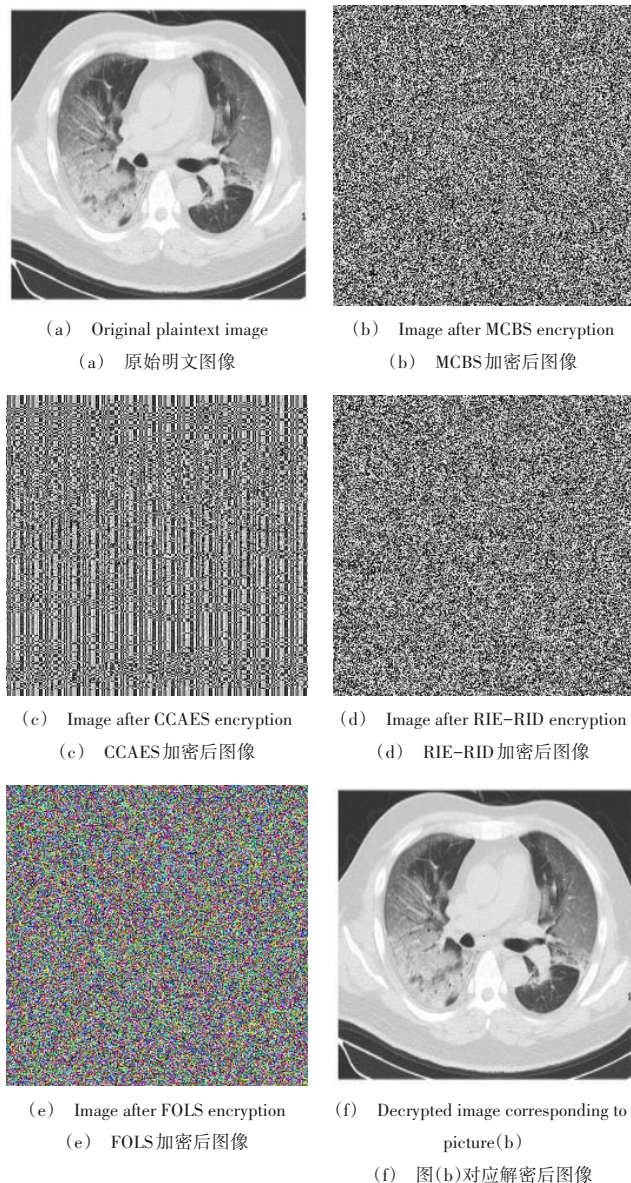


Fig. 9 Encryption results of different encryption algorithms

图9 不同加密算法的加密结果

3 结语

本文提出的MCBS算法解决了医疗图像加密场景下算法的安全性和效率两大问题,可为患者提供良好的隐私保护措施。该算法通过将SHA3-256和洛伦兹混沌系统应用于CNN架构中,加强了对密钥矩阵的保护,并通过广度学习微调模型,获取两个特征矩阵密钥实现双流加密。同时,利用椭圆曲线和莫比乌斯变换生成具有高非线性度的S盒对明文图像置乱,大幅提升了信息的不确定性。通过COVID-CT数据集进行评估,结果表明,本文算法在多个方面优于几种先进算法,同时具有高效性,是医疗图像保护场景下的理想选择。相较于传统加密算法,MCBS算法因引入神经网络和多次混沌迭代,在资源受限的计算设备上,

运行效率仍存在一定的提升空间,对此方面的优化将是未来工作的重点。

参考文献:

- [1] WEN C C, WANG Q, MIAO X N, et al. Digital image encryption: a survey[J]. Computer Science, 2012, 39(12): 6-9, 24.
文昌辞,王沁,苗晓宁,等. 数字图像加密综述[J]. 计算机科学, 2012, 39(12): 6-9, 24.
- [2] MATTHEWS R. On the derivation of a "chaotic" encryption algorithm[J]. Cryptologia, 1989, 13(1): 29-42.
- [3] ALAWIDA M. Enhancing logistic chaotic map for improved cryptographic security in random number generation[J]. Journal of Information Security and Applications, 2024, 80: 103685.
- [4] WEI F, WANG Q W, LIU H, et al. Exploiting newly designed fractional-order 3D Lorenz chaotic system and 2D discrete polynomial hyper-chaotic map for high-performance multi-image encryption[J]. Fractal and Fractional, 2023, 7(12): 887.
- [5] POURASAD Y, RANJBARZADEH R, MARDANI A. A new algorithm for digital image encryption based on chaos theory[J]. Entropy, 2021, 23(3): 341.
- [6] CHEN J X, CHEN L, ZHOU Y C. Cryptanalysis of a DNA-based image encryption scheme[J]. Information Sciences, 2020, 520: 130-141.
- [7] WANG Q, XU G T. An encryption algorithm based on improved logistic mapping and dual-image blending[J]. Netinfo Security, 2022, 22(12): 76-86.
- [8] SHAO Y. A parallel color image encryption algorithm using chaos for colour image encryption[C]// 2024 3rd International Conference on Electronics and Information Technology, 2024: 595-600.
- [9] DING Y, TAN F Y, QIN Z, et al. DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption[J]. IEEE Transactions on Neural Networks and Learning Systems, 2021, 33(9): 4915-4929.
- [10] YOUSIF S F, ABBOD 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.
- [11] 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, 2022, 98(1): 014002.
- [12] 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.
- [13] 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]// 2024 IEEE International Conference on Smart Internet of Things, 2024: 51-58.
- [14] BILAL M, MURTAZA G, DEMIR B, et al. An efficient algorithm to generate dynamic substitution-boxes and its applications in image encryption[J]. Alexandria Engineering Journal, 2025, 116: 214-231.
- [15] HE X, YANG X, ZHANG S, et al. Sample-efficient deep learning for COVID-19 diagnosis based on CT scans[DB/OL]. <https://www.medrxiv.org/content/10.1101/2020.04.13.20063941v1.full.pdf>.
- [16] CHEN C L P, LIU Z. Broad learning system: an effective and efficient incremental learning system without the need for deep architecture[J]. IEEE Transactions on Neural Networks and Learning Systems, 2018, 29(1): 10-24.
- [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] XU Y, JOVICICH J. IXI dataset[EB/OL]. <http://brain-development.org/ixi-dataset/>.

(责任编辑:黄健)