2025 年 第 25 卷 第 4 期
2025, 25(4): 01529-11

科 学 技 术 与 工 程
Science Technology and Engineering

ISSN 1671—1815
CN 11—4688/T

DOI:10.12404/j.issn.1671-1815.2309557
引用格式:李佳文, 杨娜, 李萌萌, 等. 基于新四维混沌系统的医学图像加密[J]. 科学技术与工程, 2025, 25(4): 1529-1539.
Li Jiawen, Yang Na, Li Mengmeng, et al. Medical image encryption based on a new four-dimensional chaotic system[J]. Science Technology and Engineering, 2025, 25(4): 1529-1539.

基于新四维混沌系统的医学图像加密

李佳文, 杨娜, 李萌萌, 李珊珊*
(长安大学信息工程学院, 西安 710064)

摘 要 在当今数字化医疗环境中,医学图像的传输和共享已成为日常医疗工作的一部分。然而,由于医学图像内含患者隐私信息,若不加以保护,存在非法获取或泄露的风险,带来不必要的困扰。针对这一问题,提出一种基于 Zigzag 置乱和新四维超混沌系统的医学图像加密算法。首先利用 Zigzag 算法对图像进行一次置乱,大致隐藏图像的明显轮廓;再利用改进的猫映射算法对图像进行二次置乱,去除图像中明显的纹理特征;最后,将由明文图像生成的加扰因子应用于超混沌系统初始值的产生过程中,再将生成的超混沌序列转换为超混沌矩阵用于加密算法后续的扩散过程。仿真结果表明,所提算法能根据医学图像的特点有效隐藏明文信息,并能抵抗常见类型的攻击。所提算法在鲁棒性测试中表现良好,表明该算法可以解决远程医疗中图像易受干扰的问题。

关键词 医学图像加密; 超混沌系统; 猫映射; 置乱; 扩散
中图法分类号 TP309.7; **文献标志码** A

Medical Image Encryption Based on a New Four-dimensional Chaotic System

LI Jia-wen, YANG Na, LI Meng-meng, LI Shan-shan*
(School of Information Engineering, Chang'an University, Xi'an 710064, China)

[**Abstract**] In the contemporary digital healthcare setting, the dissemination and sharing of medical imagery are integral to routine medical operations. However, medical images often contain sensitive patient information, and without adequate protection, there is a risk of illegal acquisition or leakage, which brings unnecessary troubles. To address this issue, an encryption algorithm based on Zigzag scrambling and a new four-dimensional hyperchaotic system was proposed. Firstly, the Zigzag algorithm was used to scramble the image once, roughly hiding the obvious contours of the image. Then, an improved cat mapping algorithm was used to perform secondary scrambling on the image, removing obvious texture features. Finally, the scrambling factor generated from the plaintext image was applied to the initial value generation process of the hyperchaotic system. The generated hyperchaotic sequence was transformed into a hyperchaotic matrix for the subsequent diffusion process of the encryption algorithm. The simulation results show that the proposed algorithm can effectively conceal plaintext information based on the characteristics of medical images and resist common types of attacks. The robustness of the proposed algorithm has been demonstrated through testing, confirming its capability to address the issue of image interference in remote healthcare.

[**Keywords**] medical image encryption; hyperchaotic system; cat map; scrambling; diffusion

在数字化时代,图像作为信息传递的关键媒介,常包含丰富的个人、商业和敏感信息。在医疗领域中,医学图像包含如疾病诊断、病历记录和个人身份等敏感信息。医疗图像的泄露可能导致患者隐私泄漏。医学图像的篡改和伪造可能会导致错误的诊断和治疗,严重威胁患者的生命和健康。此外,鉴于医疗图像在不同医院、医生及研究机构间的频繁共享与远程访问需求,确保这些数据的安全性和保密性变得尤为关键。

中外学者都在积极探索各种医学图像加密算法[1],主要包括置乱、扩散以及两者的结合[2],两者结合能够同时改变像素位置及像素值本身,在经过严密的算法设计之后可以得到较为良好的加密效果。但是单一置乱与扩散的加密方案更容易被攻破。

混沌系统作为一种非线性、随机、敏感依赖初值的动力系统,具有高度不可预测性和复杂性。Fridrich[3]将混沌映射应用于图像加密,并讨论混沌

收稿日期: 2023-12-04; **修订日期**: 2024-11-05
第一作者: 李佳文(1999—),女,汉族,陕西宝鸡人,硕士研究生。研究方向:图像加密。E-mail:2022224067@chd.edu.cn。
* **通信作者**: 李珊珊(1982—),女,汉族,陕西商洛人,博士,副教授。研究方向:图像加密、图像理解与分析。E-mail:sputnik@126.com。

系统与密码系统之间的关系。通过将混沌系统引入图像加密过程,能够有效保护图像数据的安全,还能提高加密效率。

随着混沌系统的成熟,许多经典算法被应用到混沌系统中,如 DNA 编码、神经网络等[4-7],低维混沌系统结构简单,高维混沌系统往往具有更多的初始条件和更多的控制参数[8-9],文献[10]提出一种基于多混沌系统的多图像加密算法. 采用超混沌 Lorenz 系统生成四维混沌序列,利用其对置乱后的图像进行双向扩散和行列置乱,获得最终密文图像。文献[11]通过一类渐近稳定的标称线性系统和一致有界控制器的设计,构造在多个控制位置生成具有最大个数正李氏指数的高维超混沌系统。文献[12]提出一种基于 Lorenz 超混沌系统的量子图像加解密新方案。首先对洛伦兹超混沌系统得到的伪随机序列进行排序,然后对位置信息的行和列进行索引序列的加扰,最后混淆每个像素点的信息,一定程度提高了混沌系统安全性。为了改善其混沌性能和安全性,采用低维混沌系统的组合设计新的混沌系统。文献[13]首先通过耦合二维 Henon 混沌映射模型和 Sine 混沌映射模型,设计了一种新的三维混沌映射模型,解决了现有混沌映射模型的混沌空间小及混沌能力弱的问题。文献[14]提出了一种新的和改进的混沌图像加密系统,采用两个混沌映射来确保加密医学图像的混沌性能和安全性,以提高加密图像的随机性和安全性。

基于此,现提出一种基于 Zigzag 置乱和新四维超混沌系统的医学图像加密算法。采用明文信息直接参与密钥生成的方法设置加扰因子以提高加密算法对于明文的敏感性。在加密算法的置乱过程中,采用 Zigzag 算法和改进的猫映射对图像像素位置进行置乱。在扩散过程中,使加扰因子参与超混沌系统初值的生成过程,由于混沌系统对于初值的极端敏感性,明文信息的微小变化会造成混沌序列的剧烈变化,再将生成的混沌序列用于加密算法的扩散过程,一定程度上可以增强对像素值的扩散效果。所提加密算法扩散性能好、密钥敏感性强,且能够抵御差分、暴力、剪切、噪声等常见攻击。

1 基本原理

1.1 新四维超混沌系统

图像加密算法中应尽可能地采用对于初值极端敏感的混沌系统,以最大限度提高所产生混沌序列的不可预测性,越不可预测就越安全。文献[15-16]提出一个具有高度复杂性的四维超混沌系统,如式(1)所示。

$$\begin{cases}\dot{x} = a(y - x - w) + byz\\ \dot{y} = c(4x + y) - xz\\ \dot{z} = dx - ez + xy\\ \dot{w} = rx + f(3yz + y^2)\end{cases} \tag{1}$$

式(1)中:x、y、z、w 为混沌系统状态变量,$\dot{x}$、$\dot{y}$、$\dot{z}$、$\dot{w}$ 分别为其变化率;混沌系统的参数 $a=80$,$b=45$,$c=22$,$d=5$,$e=21$,$f=8$;r 为控制参数,用于调节混沌系统的整体动态特性 $60 \leqslant r \leqslant 322$。

当 $r=100$ 时,其 Lyapunov 指数为 LE1 = 25.620 6,LE2 = 11.240 1,LE3 = 1.717×10^{-5},LE4 = −115.033 6,可知 4 个 Lyapunov 指数中有 3 个都是大于 0 的,而且指数的值都偏大,说明此时系统不仅处于超混沌状态而且混沌程度很高,混沌系统在 $r=100$,且初始参数为(0, 0.5, 0.5, 0.5)时在二维相空间中的分布图如图 1 所示,可以看出,系统的动力学特征较为复杂且难以预测,满足加密算法的需求。

1.2 Zigzag 置乱

Zigzag 是一种形似中文汉字“之”的一种遍历方法[17],在操作中,从医学图像矩阵的第一个像素开始,以 Zigzag 特有的模式对随后的像素进行遍历,遍历过程将医学图像的每个通道矩阵拉伸为一维图像序列,具体路径如图 2 所示。以这种方式获得相对应的一维序列之后再经过一定规律的排布,便可完成对图像的初步置乱。

根据图 2 可以看出,采用 Ziazag 置乱对图像进行处理的过程中,对于图像的边界处置乱效果不佳。由于要维持“之”字形路径,对于处在边界处的像素点,在遍历过程中仍然保持相邻位置。但是对于医学图像来说,其数据量普遍较大,且其重点内容往往集中于图像的中心位置,所以采用这种置乱方法,很适用于医学图像加密。

1.3 改进的猫映射

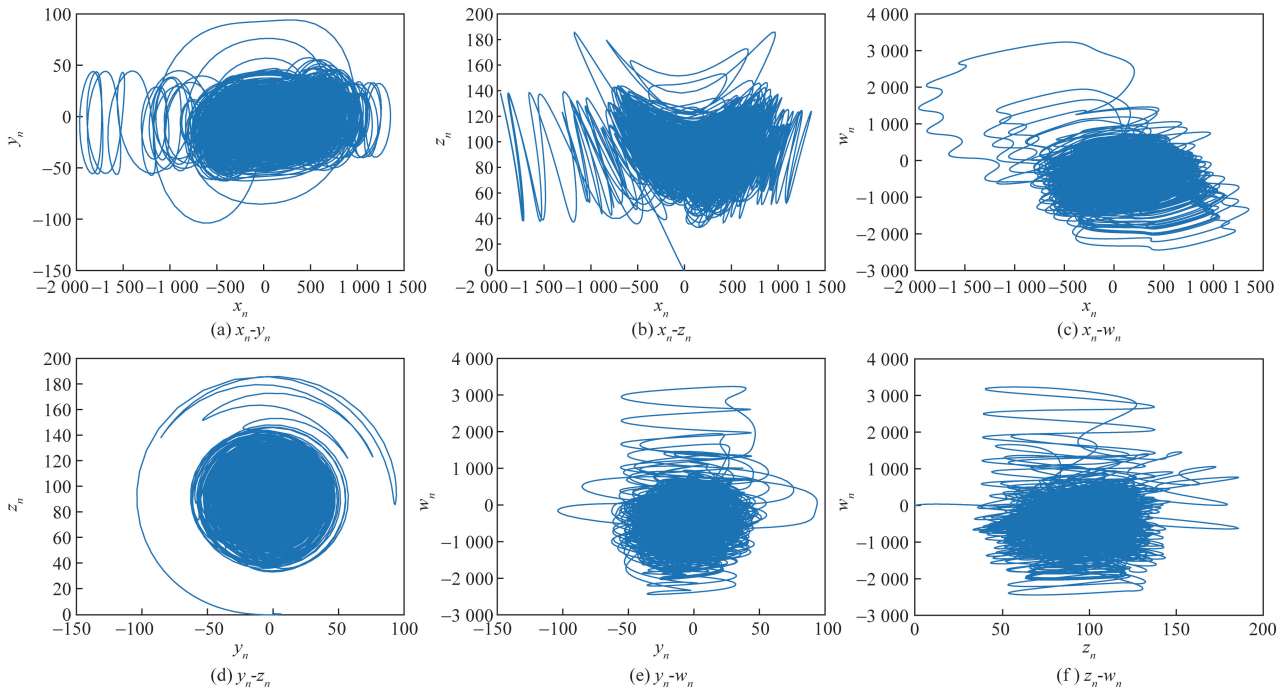
为了更好地隐藏医学图像的纹理特征,提高猫映射对于加密算法的置乱效果,对于猫映射进行非线性改进,可表示为

$$\begin{bmatrix}x_i\\ y_j\end{bmatrix} = \begin{bmatrix}1 & a\\ b & ab+1\end{bmatrix}\begin{bmatrix}x_{i-1}\\ y_{j-1}\end{bmatrix} + \begin{bmatrix}0\\ x_i^2\end{bmatrix} \bmod \begin{bmatrix}E\\ F\end{bmatrix} \tag{2}$$

式(2)中:(x_i, y_j) 为置乱图像的像素值;(x_{i-1}, y_{j-1}) 为明文图像的像素值;a 和 b 为正整数;$i \in [1, E]$,$j \in [1, F]$,E 和 F 分别对应图像矩阵的长和宽;mod(·)为取模运算。

1.4 Tent 映射

本文算法中密钥的生成部分需要借助 Tent 映射系统作为辅助[18]。Tent 映射又称帐篷映射,在数学中是指一种分段的线性映射,因其函数图像类似帐篷而得名,可表示为



x_n、y_n、z_n、ω_n为系统在第 n 步的状态变量

图 1　系统的二维空间分布图

Fig. 1　The two-dimensional spatial distribution of the system

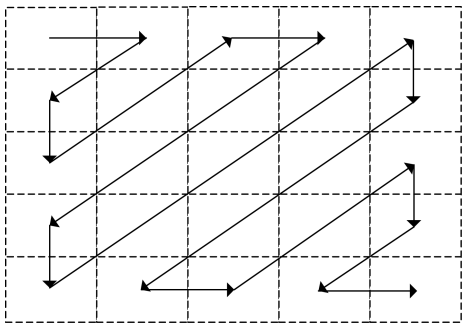


图 2　Zigzag 路径

Fig. 2　Zigzag path

$$x_{n+1}=f(x_n)=\begin{cases}\dfrac{x_n}{\alpha}, & x_n\in[0,\alpha)\\ \dfrac{1-x_n}{1-\alpha}, & x_n\in[\alpha,1]\end{cases} \tag{3}$$

帐篷映射在其参数范围内是一个二维混沌映射,并且具有均匀的分布函数和良好的相关性。其中,$0<\alpha<1$,在 α 的可取范围内,系统都处于混沌状态。尤其的,当 $\alpha=0.5$ 的时候,系统呈现短周期状态,因此一般不取 $\alpha=0.5$。

2　加密算法

本文加密算法的流程图如图 3 所示。其中超混沌序列的产生由以下 3 部分决定:用户输入的 5 个参数(x_0、y_0、z_0、w_0、r)、由二维 Tent 映射与明文信息共同产生的参数 h_1、h_2和由明文信息生成的加扰因子;进行猫映射置乱的所需参数由生成的超混沌序列、加扰因子和参数 h_1、h_2共同给出。

2.1　密钥的生成

步骤 1　由参数 α 和初始值 x_c生成 Tent 映射序列 L,其中 $\alpha\neq x_c$,否则系统将演化为周期系统。

步骤 2　由用户输入参数 u,选择序列 L 中的第 u 位对应的数值用作后续处理,正整数 u 的范围应当在序列长度以内。

步骤 3　选出所需数值以后,对其作出处理,可表示为

$$h=\mathrm{mod}\left\{\mathrm{floor}[L(u)10^4],\frac{1}{2}E\right\}+\frac{1}{4}E \tag{4}$$

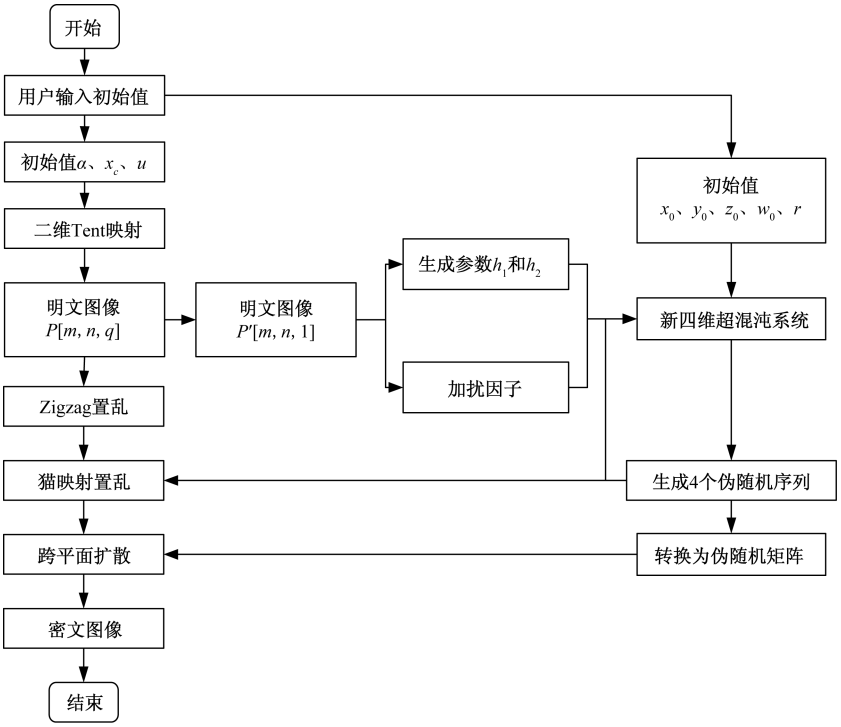
式(4)中:E 为图像矩阵的长。

作出以上处理的原因是考虑到医学图像的特点,因此将取值范围尽量限定在图片中间部分,从而保证后续得到的数据是有意义的。

步骤 4　随后将图像的 R 通道矩阵的第 h 行对应位置的像素点数进行累加记为 h_1,第 h 列对应位置的像素点数进行累加记为 h_2,可表示为

$$\begin{cases}h_1=\sum_{i=1}^{F}f(h,i)\\ h_2=\sum_{j=1}^{E}f(j,h)\end{cases} \tag{5}$$

式(5)中:$f(\cdot)$为待加密图像 R 通道中对应位置的像素值,图像的尺寸为 $E\times F$。



α、x_c、u 为用户输入的参数,其中 u 为正整数;$P[m,n,q]$ 为原始明文图像,其中,m 和 n 分别为图像矩阵的长和宽,q 为通道数,为减少计算负担,选择 $P[m,n,1]$ 表示 P 图像的第一通道生成加扰因子和特征信息

图 3 加密算法流程图

Fig. 3 Encryption algorithm flowchart

2.2 设置加扰因子

为了提高加密方案的明文敏感性,添加扰动因子,可表示为

$$\varphi = \frac{\sum_{i,j} f(i,j)}{EF} \tag{6}$$

式(6)中:$f(\cdot)$为待加密图像 R 通道中对应位置的像素值;$i \in [1, E]$且$j \in [1, F]$。

借助超混沌系统对初始参数的敏感性,通过将扰动因子加入超混沌系统初始参数的生成过程中,从而增加算法对于明文的敏感性。

2.3 超混沌序列的产生

结合上文以及所设置的加扰因子,计算混沌系统迭代时的最终初始值,可表示为

$$\begin{cases} x_0' = \mathrm{mod}(h_1 \times 2^{x_0}, r) + \varphi \\ y_0' = \mathrm{mod}(h_2 \times 2^{y_0}, r) + \varphi \\ z_0' = \mathrm{mod}(h_1 \times 2^{z_0}, r) + \varphi \\ w_0' = \mathrm{mod}(h_2 \times 2^{w_0}, r) + \varphi \end{cases} \tag{7}$$

将相关参数全部输入新四维混沌系统之中,将系统重复运行 $500 + E \times F \times 3$ 次,为了获得具有较好混沌特性的伪随机序列,每个伪随机序列都舍弃前 500 个迭代值,进而得到 4 个长度均为 $E \times F \times 3$ 的伪随机序列 $[x_x, y_y, z_z, w_w]$。

2.4 像素位置置乱

步骤 1 按照 RGB 平面的顺序对像素矩阵进行置乱,设原始明文图像 $\boldsymbol{O}$ 的每个平面尺寸为 $E \times F$,采用 1.2 节中 Zigzag 置乱方法将明文图像转换为一维序列 $\boldsymbol{O}_1$。

步骤 2 将一维序列 $\boldsymbol{O}_1$ 以列的方式进行重排,重新转换为二维矩阵,得到初始置乱后的加密图像 $\boldsymbol{O}_2$。

步骤 3 对 $\boldsymbol{O}_2$ 施加 30 轮猫映射置乱之后,得到半加密图像 $\boldsymbol{O}_3$,具体每一轮的猫映射过程如 1.3 节中所示。此过程中,猫映射的参数 a 和 b 由式(8)和式(9)给出。

$$\begin{cases} a' = \mathrm{mod}[h_1 \times \mathrm{floor}(\varphi), E \times F] \\ b' = \mathrm{mod}[h_2 \times \mathrm{floor}(\varphi), E \times F] \end{cases} \tag{8}$$

$$\begin{cases} a = \mathrm{floor}[x_x(a'+1) + y_y(b'+1)] \\ b = \mathrm{floor}[z_z(a'+1) + w_w(b'+1)] \end{cases} \tag{9}$$

式中:floor(·)表示对括号里的数值向下取整;x_x、y_y、z_z、w_w 为生成的伪随机序列,长度为 $E \times F \times 3$。

2.5 跨平面扩散

为了提供更高效的扩散操作,设计一种跨平面扩散,可以同时处理 3 个颜色平面中的所有图像像素。平面间的扩散可以导致一个像素到下一个像素的变化。

步骤 1 将利用混沌系统得到的 4 个伪随机序

列进行处理,可表示为

$$\begin{cases} X_{\mathrm{m}} = \mathrm{mod}\{\mathrm{floor}[x_x(i) \times 2^{16}], L\} \\ Y_{\mathrm{m}} = \mathrm{mod}\{\mathrm{floor}[y_y(i) \times 2^{16}], L\} \\ Z_{\mathrm{m}} = \mathrm{mod}\{\mathrm{floor}[z_z(i) \times 2^{16}], L\} \\ W_{\mathrm{m}} = \mathrm{mod}\{\mathrm{floor}[w_w(i) \times 2^{16}], L\} \end{cases} \tag{10}$$

式(10)中:$i \in [1, E \times F \times 3]$;$L = 256$ 为灰度级水平。

步骤 2　将得到的 4 个伪随机序列分别转换为 4 个三维混沌矩阵 $\boldsymbol{R}^{(1)}$、$\boldsymbol{R}^{(2)}$、$\boldsymbol{R}^{(3)}$、$\boldsymbol{R}^{(4)}$。

步骤 3　首先进行第一轮按行遍历扩散,使用 $\boldsymbol{R}^{(1)}$ 对置乱后的像素矩阵 $\boldsymbol{O}_3$ 进行扩散,得到扩散中间图像 $\boldsymbol{C}$。

步骤 4　第一轮按行遍历扩散完成后,依次使用 $\boldsymbol{R}^{(2)}$、$\boldsymbol{R}^{(3)}$、$\boldsymbol{R}^{(4)}$ 对扩散中间像素矩阵 $\boldsymbol{C}$ 接着进行按列遍历扩散,逆向按行遍历扩散,逆向按列遍历扩散,共 4 轮扩散操作,得到最终扩散的图像 $\boldsymbol{O}_4$。

以按行遍历扩散为例,具体操作如式(11)所示。在解密操作中,使用相同参数的逆操作可以得到置乱后的图像 $\boldsymbol{O}_3$。

图 4 描述了通过 $\boldsymbol{R}^{(1)}$ 矩阵对尺寸为 3 × 3 × 3 的彩色图像进行扩散的数字示例。例如,$\boldsymbol{O}_3(1,1,1)$ 是要处理的元素,$\boldsymbol{R}^{(1)}$ 与之对应坐标元素 $\boldsymbol{R}^{(1)}(1,1,1)$ 与 $\boldsymbol{O}_3(1,1,1)$ 异或得到扩散结果 $\boldsymbol{C}(1,1,1)$。除待扩散图像 $\boldsymbol{O}_3$ 的 R 通道第一行元素外,其余元素在 $\boldsymbol{O}_3$ 矩阵与 $\boldsymbol{R}^{(1)}$ 矩阵对应元素异或后仍需再异或 $\boldsymbol{C}$ 矩阵与 $\boldsymbol{O}_3$ 矩阵对应的上一行扩散后的元素。例如,$\boldsymbol{O}_3(3,2,1)$,$\boldsymbol{O}_3(1,1,2)$ 是要处理的元素,首先,它们分别要与 $\boldsymbol{R}^{(1)}$ 矩阵中对应坐标元素 $\boldsymbol{R}^{(1)}(3,2,1)$ 与 $\boldsymbol{R}^{(1)}(1,1,2)$ 异或,其次,还需分别异或上一行元素 $\boldsymbol{O}_3(2,2,1)$,$\boldsymbol{C}(2,2,1)$ 与 $\boldsymbol{O}_3(3,1,1)$,$\boldsymbol{C}(3,1,1)$。

$$\boldsymbol{C}_{i,j,k} = \begin{cases} \boldsymbol{O}_{3i,j,k} \oplus \boldsymbol{R}^{(1)}_{i,j,k}, & i = 1, k = 1, \\ \boldsymbol{O}_{3i,j,k} \oplus \boldsymbol{R}^{(1)}_{i,j,k} \oplus \boldsymbol{C}_{M,j,k-1} \oplus \boldsymbol{O}_{3M,j,k-1}, & i = 1, k \neq 1, \\ \boldsymbol{O}_{3i,j,k} \oplus \boldsymbol{R}^{(1)}_{i,j,k} \oplus \boldsymbol{C}_{i-1,j,k} \oplus \boldsymbol{O}_{3i-1,j,k}, & i \neq 1, \end{cases} \tag{11}$$

式(11)中:i、j、k 为图像中位于第 i 行、第 j 列的像素在第 k 个颜色通道的值;$\boldsymbol{C}$ 为过渡矩阵;$\boldsymbol{O}_3$ 为待扩散向量;$\boldsymbol{R}^{(1)}$ 为三维混沌矩阵。

2.6　解密过程

本文算法的解密过程中由于参数 h_1、h_2 和加扰因子 φ 的产生过程中涉及明文信息,所以在解密时,这些参数将经由安全性能更高的信道被传

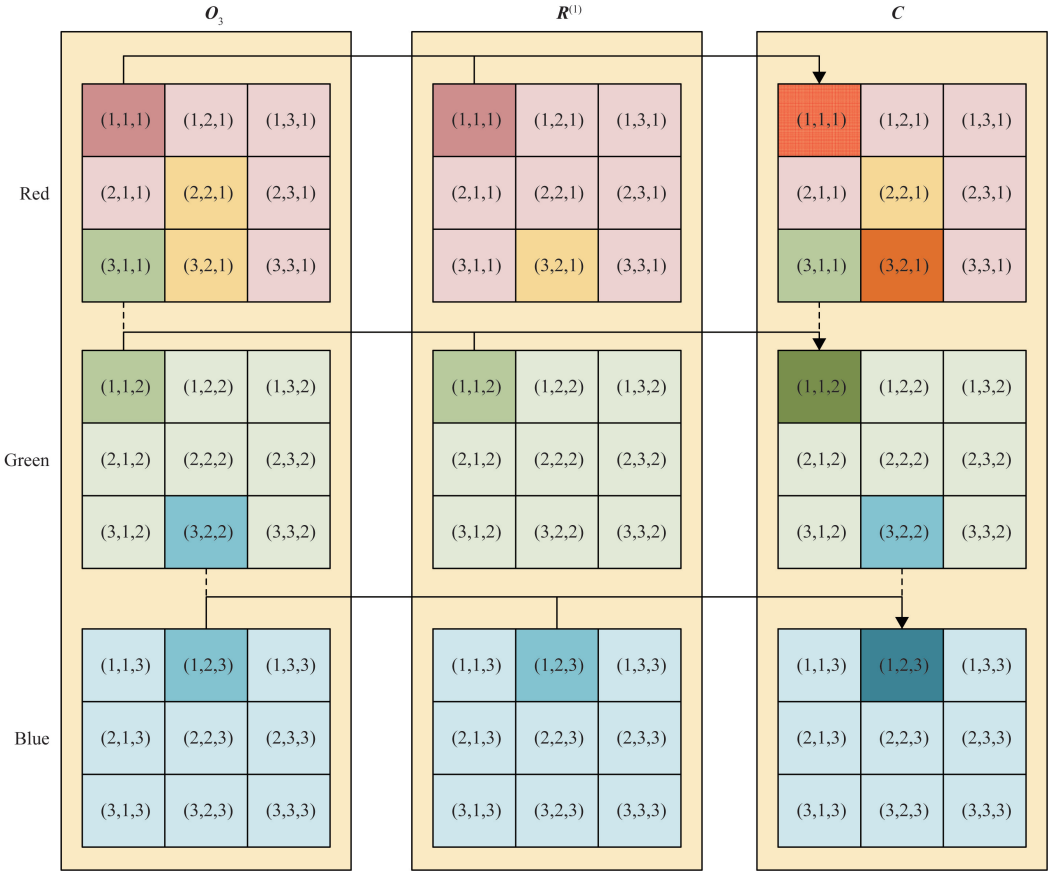


图 4　按行遍历跨平面扩散

Fig. 4　Cross plane diffusion through row traversal

输到解密端。所生成的混沌序列既用于逆扩散过程,也用于逆猫映射置乱的参数产生。具体过程如下。

步骤 1 输入参数 r 和混沌系统初始值 x_0、y_0、z_0、w_0。

步骤 2 将包含有明文信息的参数 h_1、h_2和加扰因子 φ 通过安全性能更高的信道传输到解密端,用于尺寸为 $E\times F\times 3$ 的密文图像 $\boldsymbol{O}_4$的解密。

步骤 3 利用伪随机数矩阵 $\boldsymbol{R}$,对图像 $\boldsymbol{O}_4$进行逆扩散操作,从而得到无重复置乱后的半加密图像 $\boldsymbol{O}_3$。

步骤 4 对 $\boldsymbol{O}_3$进行 30 轮猫映射置乱的逆过程,得到加密图像 $\boldsymbol{O}_2$。

步骤 5 对 $\boldsymbol{O}_2$进行 Zigzag 置乱还原,从而恢复出尺寸为 $E\times F\times 3$ 的明文图像 $\boldsymbol{O}$。

3 仿真及结果分析

为了验证算法的性能并且对方案进行对比性分析,测试选用了基准图像和医学图像进行相关实验:大小为 512×512×3 的 Lena 图像,大小为 512×512×3 的 Liver CT 图像。实验采用 MATLAB R2020a 软件进行软件测试,实验的主机环境为 Intel Core i5-8250U,具有 8 GB 内存,1.60 GHz 处理器,以及 64 位 Windows10 操作系统。

3.1 加解密效果及分析

测试图像的加密图像和解密图像以及对应的直方图如图 5 所示。可以看出,原始医学图像经加密处理,密文图像变成类似随机噪声分布的无意义图像,加密图像中不再包含明文图像中的相关信息,同时密文的直方图分布近似均匀,即所提算法具有较好的加密效果。其次,在输入相同的解密密

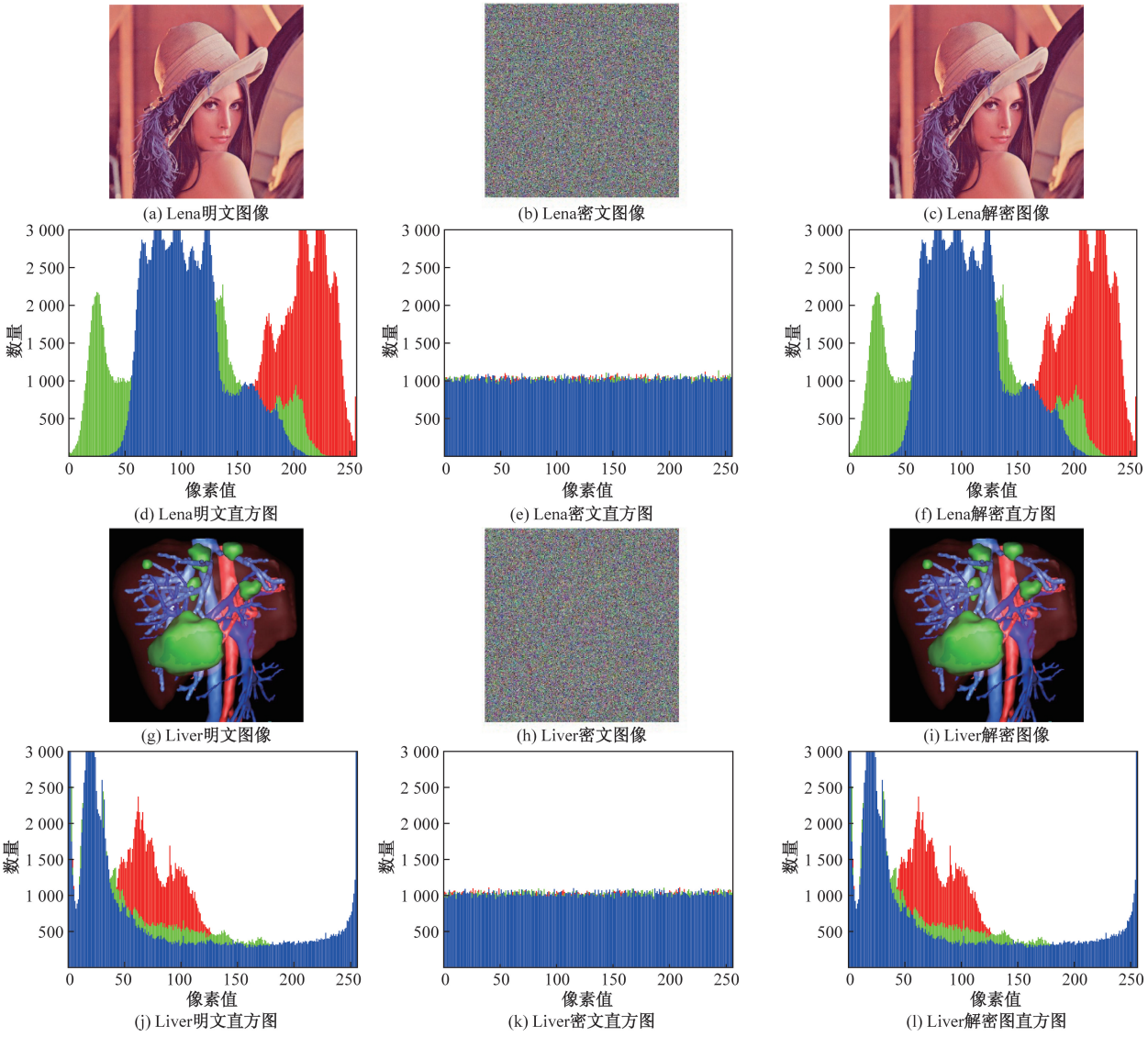


图 5 加解密结果

Fig. 5 Encryption and decryption results

钥且图像未受到篡改时,解密算法能够无失真还原出原始医学图像。

3.2　密钥分析

本文加密算法的密钥是由用户输入的参数 α、x_c、u 和 r、以及参与生成混沌系统迭代的初始参数 x_0、y_0、z_0、w_0 共同组成的。

由于是在双精度和 64 位 Windows10 操作系统下进行,根据《IEEE Standard for Floating-Point Arithmetic》(IEEE 754—2019)IEEE 浮点标准,64 位双精度计算精度为 10^{15}[19]。由此可以得出本文算法拥有的密钥空间大小为 $(10^{15})^8 = 10^{120}$,而能够抵御穷举攻击的最小密钥空间为 2^{100},本文算法远高于 2^{100},说明本加密算法面对穷举攻击具有足够的抵御能力。

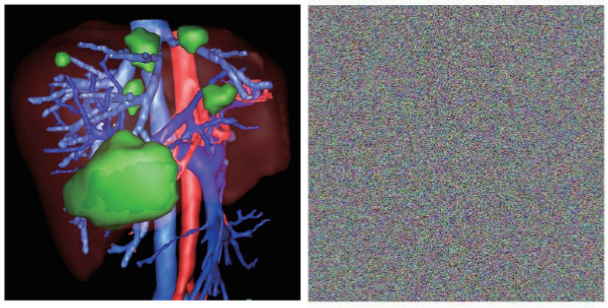
密钥敏感性是指当解密密钥发生微小变化时,却对密文图像的解密造成了非常严重的影响,此时我们认为加密算法对密钥有着极高的敏感性。由于混沌系统本身具有极高的初值敏感性,所以本实验选择通过影响新四维混沌系统的初始值生成过程,从而验证方案对于密钥的敏感性。

使用 512×512×3 的 Liver CT 图像作为测试图像,在对其进行正常加密之后得到密文图像。然而在解密时仅对新四维混沌系统的第一个初始值密钥进行更改,如式(12)所示,更改后的初始值密钥与原先的初始值密钥相差 1×10^{-8},如图 6 所示。

$$x_0' = \mathrm{mod}(h_1 \times 2^{x_0}, r) + \varphi + 0.000\ 000\ 000\ 1 \tag{12}$$

式(12)中:φ 为加扰因子。

最终验证结果如图 6 所示。



(a) 正确密钥的解密结果　　(b) 更改密钥后的解密结果

图 6　不同密钥的解密结果

Fig. 6　Decryption results of different keys

3.3　统计攻击

统计攻击是指基于医学图像中的统计特征或频率分布进行的攻击,其可以利用医学图像中的统计信息来获取有关原始图像内容。相关系数的计算公式[20]为

$$r' = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\ \sqrt{D(y)}} \tag{13}$$

$$\begin{cases} \mathrm{cov}(x,y) = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n}(x_i - E_x)(y_i - E_y) \\ D(x) = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n}(x_i - E_x)(y_i - E_y) \\ E(x) = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n}x_i \end{cases} \tag{14}$$

式中:$D(x)$、$D(y)$ 分别为 x、y 的方差;E_x、E_y 分别为 x、y 的数学期望;x_i、y_i 分别为 x、y 在第 i 个像素点上的观测值;n 为像素点的个数;$\mathrm{cov}(x, y)$ 为 x、y 的协方差;r' 为相关系数。

表 1 可以观察到明文图像中相邻像素之间的相关系数的绝对值接近 1,而密文图像中相邻像素之间的根相关系数的绝对值趋于 0。这表明明文图像中的相邻像素之间具有较高的相关性,而密文图像中的相邻像素之间几乎没有相关性。说明该算法在加密方面表现出良好的效果。

以 Liver CT 医学图像为例,在 liver 医学图像及其加密图像中分别从水平、垂直和对角方向上取 5 000对像素值做相邻像素相关性分析,结果如图 7 所示。

显然,平面像的像素对都分布在相空间的对角线上或靠近对角线,具有较高的相关性。相比之下,加密图像的所有像素对在整个相空间上是随机分布的,相关性较弱。这表明本文算法可以有效抵抗统计学攻击。

3.4　差分攻击

差分攻击攻击者收集一组已知的明文对和其对应的密文对,并观察它们之间的差异。然后,攻击者逐渐改变明文对的某一位或多位,并观察相应的密文对的变化。通过推测,攻击者可以获得一些关于密码算法中使用的密钥的有用信息。计算测试图像的 NPCR(number of pixel change rate)和 UACI(unified average changing intensity)值,如式(15)、式(16)所示,从而衡量本文加密方案的抗差分攻击能力,具体结果如表 2 所示。

$$\begin{cases} A_{\mathrm{R,G,B}}(i,j) = \begin{cases} 0, & C_{\mathrm{R,G,B}}(i,j) = C'_{\mathrm{R,G,B}}(i,j) \\ 1, & C_{\mathrm{R,G,B}}(i,j) \neq C'_{\mathrm{R,G,B}}(i,j) \end{cases} \\ \mathrm{NPCR}_{\mathrm{R,G,B}} = \dfrac{\displaystyle\sum_{i,j}A_{\mathrm{R,G,B}(i,j)}}{L} \times 100\% \end{cases} \tag{15}$$

$$\mathrm{UACI}_{\mathrm{R,G,B}} = \frac{1}{L}\left[\sum_{i,j}\frac{|C_{\mathrm{R,G,B}}(i,j) - C'_{\mathrm{R,G,B}}(i,j)|}{D-1}\right] \times 100\% \tag{16}$$

表 1 原始图像及其加密图像的相关系数

Table 1 The correlation coefficient between the original image and its encrypted image

算法	图像	方向	相关系数					
			原始图像			加密图像		
			R	G	B	R	G	B
本文算法	Lena（512×512×3）	水平	0.975 4	0.975 8	0.953 1	0.001 1	−0.000 8	0.002 3
		垂直	0.987 1	0.987 9	0.973 3	0.000 2	0.001 1	−0.000 9
		对角线	0.962 7	0.964 1	0.931 1	−0.001 2	0.002 0	−0.000 5
本文算法	Liver CT（512×512×3）	水平	0.986 1	0.9900	0.985 0	0.0025	−0.001 3	0.001 5
		垂直	0.987 6	0.989 3	0.985 0	0.001 0	0.002 5	−0.002 8
		对角线	0.975 5	0.981 1	0.9699	0.001 9	−0.002 0	−0.000 9
文献[21]	Lena（512×512×3）	水平	0.958 8	0.916 0	0.935 8	−0.019 6	−0.054 6	−0.014 5
		垂直	0.981 8	0.952 2	0.966 5	−0.016 2	−0.008 2	−0.018 4
		对角线	0.990 0	0.973 7	0.981 0	−0.007 8	−0.004 9	−0.001 2
文献[22]	Lena（512×512×3）	水平	0.964 2	0.982 2	0.962 2	0.000 6	−0.000 9	0.000 5
		垂直	0.961 8	0.974 9	0.962 2	−0.040 0	0.000 5	0.006 1
		对角线	0.960 3	0.965 4	0.924 6	0.003 0	−0.008 1	−0.007 5
文献[23]	Lena(512×512×3)	水平	0.979 8	0.969 1	0.932 8	0.003 6	0.003 3	0.001 7
		垂直	0.989 3	0.982 5	0.957 6	0.000 6	0.001 4	0.001 7
		对角线	0.969 7	0.955 5	0.991 8	0.003 0	0.004 9	0.000 1
文献[24]	Lena（512×512×3）	水平	0.989 0	0.984 0	0.957 0	0.000 7	−0.001 0	−0.000 6
		垂直	0.979 0	0.966 0	0.935 0	−0.015 0	−0.008 0	0.001 9
		对角线	0.967 0	0.952 0	0.918 0	−0.025 0	0.015 0	0.010 5

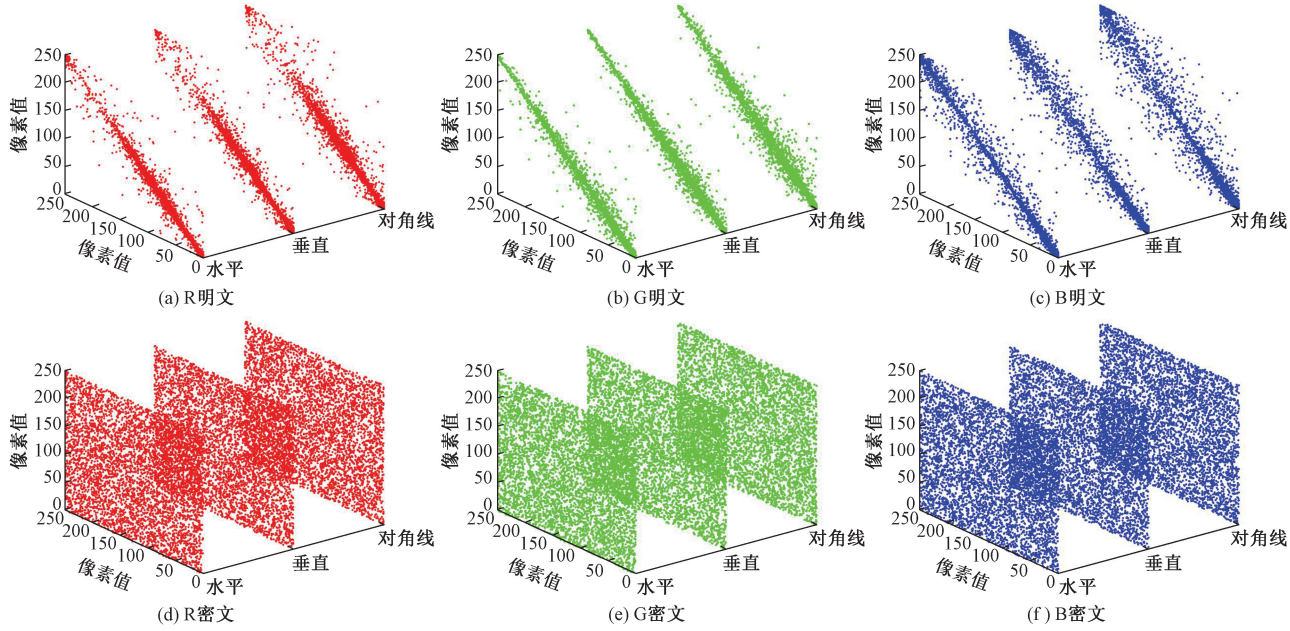


图 7 图像邻域像素值分布图

Fig. 7 Pixel value distribution map of image neighborhood

式中:L 为图像中的像素总数; $C_{R,G,B}$ 和 $C'_{R,G,B}$ 分别为原始医学图像对应的密文图像和改变一个像素灰度值后对应的密文图像; $A_{R,G,B}(i,j)$ 表示密文图像 $C_{R,G,B}(i,j)$ 和 $C'_{R,G,B}(i,j)$ 在同一位置的像素值是否发生变化; $NPCR_{R,G,B}$ 为像素变化率; $UACI_{R,G,B}$ 为密文图像 $C_{R,G,B}(i,j)$ 和 $C'_{R,G,B}(i,j)$ 之间像素值变化的平均强度; D 为图像的灰度等级。

如果得到的 NPCR 更接近理论值 99.609 4%, UACI 更接近理论值 33.463 5%,则认为图像加密算法具有较强的防御差分攻击的能力。通过表 2 中结果可知,本文算法的 NPCR 值 UACI 值均接近于理想值。这说明本文加密方案的抗差分攻击能力强,加密方案对于明文信息的变化十分敏感,攻击者无法通过篡改明文信息来攻破加密算法。

3.5 信息熵分析

通过式(17)分别计算测试图像在加密前和加密后的信息熵值,来衡量加密图像的随机性,具体结果如表 3 所示。

$$H(G) = \sum_{i=1}^{L} P(G_i) \log_2 \frac{1}{P(G_i)} \tag{17}$$

式(17)中:G_i为图像像素的灰度值;$P(G_i)$为图像中G_i出现的概率;L为灰度等级;$H(G)$为图像的信息熵。

由表3可知,所有待测图像在加密之后,其信息熵值均接近于理论值8,这说明经过本文加密算法处理所得到的加密图像具有一定的随机性,更不容易被攻破。

3.6　鲁棒性分析

为了衡量本文算法的鲁棒性,以尺寸为512×512×3大小的Liver CT医学图像为例,对其加密图像进行噪声攻击和剪切攻击。图8为Liver密文图像遭到强度为0.1的椒盐噪声,强度为0.01的高斯噪声,强度为0.01的斑点噪声攻击之后对应的解密图像;图9(a)、图9(c)为遭到不同程度剪切攻击之后的Liver密文图像,图9(b)、图9(d)分别为其对应的解密图像。

表2　NPCR和UACI值

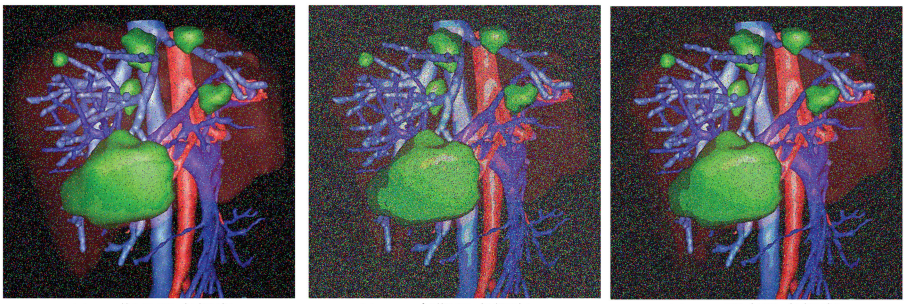
Table 2　NPCR and UACI values

算法	图像	NPCR/%			UACI/%		
		R	G	B	R	G	B
本文算法	Lena(512×512×3)	99.62	99.62	99.59	33.44	33.43	33.43
本文算法	Liver CT(512×512×3)	99.62	99.64	99.62	33.44	33.49	33.48
文献[21]	Lena(512×512×3)	99.68	99.68	99.69	33.83	33.69	34.03
文献[22]	Lena(512×512×3)	99.83	99.75	99.86	33.75	33.66	33.78
文献[25]	X-ray(400×300×3)	99.62	99.63	99.61	33.36	33.55	33.58
文献[23]	Lena(512×512×3)	99.62	99.62	99.60	33.56	33.46	33.42

表3　测试图像的信息熵结果

Table 3　Information entropy results of test images

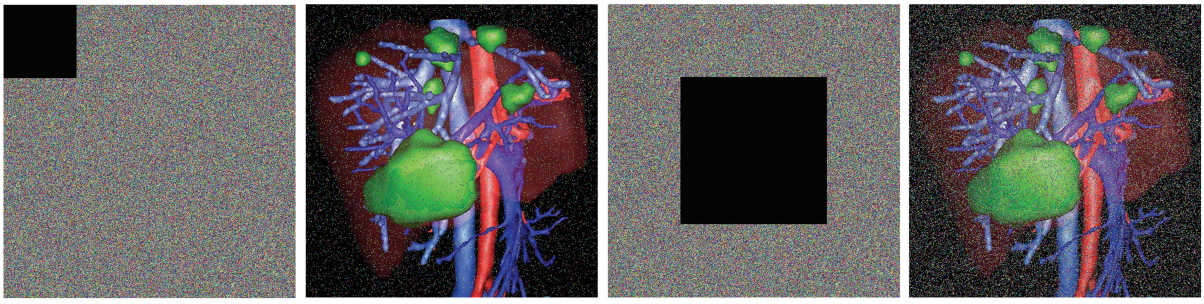
算法	图像	明文			密文		
		R	G	B	R	G	B
本文算法	Lena(512×512×3)	7.268 2	7.590 1	6.995 1	7.999 4	7.999 5	7.999 2
本文算法	Liver CT(512×512×3)	5.893 4	5.866 5	5.962 5	7.999 3	7.999 4	7.999 1
文献[26]	Average(512×512×3)	—	—	—	7.999 3	7.999 3	7.999 2
文献[23]	Lena(512×512×3)	—	—	—	7.999 3	7.999 2	7.999 3
文献[27]	a(256×256×3)	6.958 1	6.894 5	6.136 5	7.999 2	7.999 3	7.999 3



(a) 0.1椒盐噪声解密　(b) 0.01高斯噪声解密　(c) 0.01斑点噪声解密

图8　噪声攻击检测

Fig. 8　Noise attack detection



(a) 1/16剪切攻击　(b) 1/16剪切攻击　(c) 1/4剪切攻击　(d) 1/4剪切攻击

图9　剪切攻击检测

Fig. 9　Cut attack detection

经过以上分析可知,不同类型的噪声对密文图像进行攻击之后,解密图像会有不同程度的失真,但是仍能保留大部分明文信息,能够较好地恢复原始明文图像,这说明在进行远距离传输时,噪声对于加密算法的影响是处在可控范围内的;当对密文图像进行不同程度的剪切攻击时,解密后即使会损失一部分有效信息,但仍能较大程度的恢复原始图像,原图的轮廓依然清晰可见,说明在传输过程中即使发生了一定数量的数据丢失,却仍然能够得到一部分明文信息。综上,本算法具有良好的鲁棒性。

4 结论

提出一种基于 Zigzag 遍历和新四维超系统的医学图像加密方法。该方法基于传统的置乱扩散方法对图像进行加密。该算法主要包括密钥的生成、超混沌序列的生成、图像像素点位置扰乱以及图像像素值扩散等方面。加密方案充分结合了各项技术与医学图像的自身特点,更着眼于明文图像本身,并将加扰因子参与到混沌系统初始值的生成过程中从而增加方案的抗差分攻击能力。仿真结果及性能分析表明,本文算法能够抵御差分、穷举、剪切、噪声等常见攻击,可应用于图像信息的加密和传输。

参 考 文 献

[1] Ping P, Zhang X J, Yang X H, et al. A novel medical image encryption based on cellular automata with ROI position embedded [J]. Multimedia Tools and Applications, 2022, 81(5): 7323-7343.

[2] Anwar S, Meghana S. A pixel permutation based image encryption technique using chaotic map[J]. Multimedia Tools and Applications,2019, 78(19): 27569-27590.

[3] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps[J]. International Journal of Bifurcation and Chaos, 1998, 8(6): 1259-1284.

[4] Lin J Y, Zhao K N, Cai X, et al. Animage encryption method based on logistic chaotic mapping and DNA coding[C]//MIPPR 2019, Remote Sensing Image Processing, Geographic Information Systems, and Other Applications. New York: International Society for Optics and Photonics, 2020: 335-365.

[5] 袁涛, 曲强, 姜青山. 基于混沌系统和喷泉码的 DNA 加密编码方法[J]. 集成技术, 2024, 13(3): 4-24.
Yuan Tao, Qu Qiang, Jiang Qingshan. DNA encryption and coding method based on chaotic system and fountain code[J]. Integrated Technology, 2024, 13(3): 4-24.

[6] 刘维宇, 杨景凯, 刘妮, 等. 基于深度学习的图像显著性区域加密[J]. 物联网技术, 2024, 14(3): 78-80, 85.
Liu Weiyu, Yang Jingkai, Liu Ni, et al. Image saliency region encryption based on deep learning[J]. Internet of Things Technology, 2024, 14(3): 78-80, 85.

[7] Feng L Y, Du J Z, Fu C, et al. Image encryption algorithm combining chaotic image encryption and convolutional neural network[J]. Electronics, 2023, 12(16): 34-55.

[8] Wang X Y, Ren Q, Jiang D H. An adjustable visual image cryptosystem based on 6D hyperchaotic system and compressive sensing [J]. Nonlinear Dynamics, 2021, 104(4): 4543-4567.

[9] Benkouider K, Bouden T, Yalcin M, et al. Anew family of 5D, 6D, 7D and 8D hyperchaotic systems from the 4D hyperchaotic vaidyanathan system, the dynamic analysis of the 8D hyperchaotic system with six positively apunov exponents and an application to secure communication design[J]. International Journal of Modelling, Identification and Control, 2021, 35(3): 241-257.

[10] 高若云, 白牡丹, 黄佳鑫, 等. 基于多混沌系统的多图像加密算法[J]. 计算机系统应用, 2024, 33(3): 170-177.
Gao Ruoyun, Bai Mudan, Huang Jiaxin, et al. Multi-image encryption algorithm based on multi-chaotic system[J]. Computer system applications, 2024, 33(3): 170-177.

[11] 赵坤, 何建斌. 新高维超混沌系统的设计及其图像加密应用[J]. 科学技术与工程, 2022, 22(31): 13643-13652.
Zhao Kun, He Jianbin. Design of new higher-dimensional hyperchaotic system and its application in image encryption[J]. Science Technology and Engineering, 2022, 22(31): 13643-13652.

[12] Zhou R G, Li Y B. Quantum image encryption based on Lorenz hyper-chaotic system[J]. International Journal of Quantum Information, 2020, 18(5):1-21.

[13] 牛士铭, 薛茹, 丁聪. 基于改进型 3D_Henon 混沌映射的彩色图像加密方法[J]. 计算机工程与科学, 2024, 46(4): 657-666.
Niu Shiming, Xue Ru, Ding Cong. Color image encryption method based on improved 3D_Henon chaotic map[J]. Computer Engineering and Science, 2024, 46(4): 657-666.

[14] Jain K, Aji A, Krishnan P. Medical image encryption scheme using multiple chaotic maps[J]. Pattern Recognition Letters, 2021, 152: 356-364.

[15] Chen L J, Tang S, Li, Q D, et al. A new 4D hyperchaotic system with high complexity[J]. Mathematics and Computers inSimulation, 2018, 146: 44-56.

[16] Liu Y J, Jiang Z G, Xu X P, et al. Optical image encryption algorithm based on hyper-chaos and public-key cryptography[J]. Optics and Laser Technology, 2020, 127: 106171.

[17] Devipriya M, Brindha M. Reconfigurable architecture for DNA diffusion technique-based medical image encryption[J]. Journal of Circuits, Systems and Computers, 2023, 32(4): 2350065.

[18] 赵雨, 杨真, 雍江萍, 等. 基于混沌映射的图像加密算法研究[J]. 华东交通大学学报, 2022, 39(6): 26-36.
Zhao Yu, Yang Zhen, Yong Jiangping, et al. Research on image encryption algorithm based on chaos mapping[J]. Journal of East China Jiaotong University, 2022, 39(6): 26-36.

[19] Hua Z Y, Zhou Y C. Image encryption using 2D logistic-adjusted-sine map[J]. Information Sciences, 2016, 339: 237-253.

[20] Li S S, Zhao L, Yang N. Medical image encryption based on 2D Zigzag confusion and dynamic diffusion[J]. Security and Communication Networks, 2021, 2021: 1-23.

[21] Gafsi M, Abbassi N, Hajjaji M A, et al. Improved chaos-based cryptosystem for medical image encryption and decryption[J]. Scientific Programming, 2020, 2020: 6612390.

[22] Yasser I, Khalil A T, Mohamed M A, et al. A robust chaos-based technique for medical image encryption[J]. IEEE Access, 2021, 10: 244-257.

[23] Liu J Z, Tang S S, Lian J, et al. A novel fourth order chaotic system and its algorithm for medical image encryption[J]. Multidimensional Systems and Signal Processing, 2019, 30(4): 1637-1657.

[24] Hafsa A, Gafsi M, Malek J, et al. FPGA implementation of improved security approach for medical image encryption and decryption[J]. Scientific Programming, 2021, 2021: 6610655.

[25] Choi U S, Cho S J, Kang S W. Color image encryption algorithm for medical image by mixing chaotic maps[C]//12th International Symposium on Communication Systems, Networks and Digital Signal Processing. Porto: IEEE, 2020: 1-5.

[26] Kamal S T, Hosny K M, Elgindy T M, et al. A new image encryption algorithm for grey and color medical images[J]. IEEE Access, 2021, 9: 37855-37865.

[27] Moafimadani S S, Chen Y C, Tang C M. A new algorithm for medical color images encryption using chaotic systems[J]. Entropy, 2019, 21(6): 577.