文章编号：2095-2163(2023)02-0139-06 中图分类号：TP309.7 文献标志码：A

基于 LSB 和提升小波变换的选择性医疗图像加密

刘 星，陈慧琴，夏万贵
（黑龙江科技大学 计算机与信息工程学院，哈尔滨 150022）

摘 要：数字图像作为重要的信息载体，其安全性受到越来越多的重视，图像加密算法也因此成为研究的热点。医疗图像作为一种特殊的数字图像，其中包含了病人的隐私信息，对其进行安全加密显得尤为重要。本文重点关注医疗加密图像的真实性和完整性，提出了一种基于最低有效位算法的视觉无损信息隐藏算法。首先，通过阈值分割算法，将医疗图像分为感兴趣区域和非感兴趣区域，再将感兴趣区域像素的高四位通过最低有效位隐写术嵌入到非感兴趣区域中；之后对感兴趣区域进行提升小波变换生成低频分量，将生成的低频分量通过混沌系统置乱后小波重构；最后将小波重构后的感兴趣区域进行一轮扩散加密后放回原图。实验仿真和实验分析表明，该算法具有更好的信息解密优势，在保证安全性的同时，解密后图像的峰值信噪比和结构相似性都有明显提升。

关键词：图像加密；提升小波变换；无损加密

Selective medical image encryption based on LSB and lifting wavelet transform

LIU Xing, CHEN Huiqin, XIA Wangui
(School of Computer and Information Engineering, Heilongjiang University of Science and Technology, Harbin 150022, China)

【Abstract】As an important information carrier, the security of digital images has received more and more attention, and the image encryption algorithm has therefore become a research hotspot. As a special digital image, medical image contains the patient´s private information, and it is particularly important to encrypt it securely. This paper focuses on the authenticity and integrity of medical encrypted images, and proposes a visual lossless information hiding algorithm based on the least significant bit algorithm. First, the medical image is divided into regions of interest and regions of non-interest through a threshold segmentation algorithm, and then the upper four bits of the pixels of the region of interest are embedded into the region of interest through the least significant bit steganography. The lifting wavelet transform is performed to generate low-frequency components, and the generated low-frequency components are scrambled by the chaotic system and then reconstructed by wavelet. Experimental simulation and analysis show that the algorithm has better information decryption advantages. While ensuring security, the peak signal-to-noise ratio and structural similarity of the decrypted images are significantly improved.

【Key words】image encryption; lifting wavelet transform; lossless encryption

0 引 言

随着信息和互联网技术的飞速发展，大量的信息通过互联网进行传输，因此信息安全受到人们广泛的关注[1-3]。数字图像具有直观、生动的特点，成为多媒体信息的重要形式之一，并在网络上得到广泛传播[4]。网上图像传输给人们提供了很大的便利，但在网络应急通信情况下，海量图像数据的安全存储和传输问题日显突出。在军事、医疗、商业等特殊领域，数字图像通常需要具有更高的保密程度。数字医疗图像嵌入了许多患者隐私信息，其中包含的医学信息对于诊断至关重要，泄漏和因保护不当而破坏医疗信息会给医疗机构和患者造成巨大的损失和伤害，甚至会对生命健康造成威胁[5]。随着远程医疗技术的发展以及区域医疗卫生服务信息化发展，医学影像在医疗机构之间的共享将会成为未来的发展趋势，医学图像需要在公共渠道进行传输和存储，非常容易受到安全威胁。因此，医疗机构为了保证医学影像的私密性和保密性，使用了各种安全服务，其中图像加密技术已成为保护医疗信息免受各种攻击的重要技术手段之一。

一般来说，数字医疗图像最重要的应该是其嵌入的患者隐私和医疗信息，即一张图像只有一部分是有意义的，也就是说只有一部分图像信息需要进

作者简介：刘 星(1993-)，男，硕士研究生，主要研究方向：图像加密、人工智能、NLP；陈慧琴(1996-)，女，硕士研究生，主要研究方向：图像处理、SAR 图像变化检测；夏万贵(1993-)，男，硕士研究生，主要研究方向：人工智能与机器学习。

收稿日期：2022-04-15

行加密保护。因此图像是分为两部分的即隐私区，也称作为感兴趣区域(Region of Interest，ROI)和无隐私区域，也称为非感兴趣区域(Region of Background，ROB)[5]。近年来，选择性图像加密作为一种趋势，在保持足够安全级别的同时，最大限度地减少图像加密和解密的处理时间，引起众多科学家和工程师的关注，为此提出了许多的加密方案。与作用于整个图像的传统加密方案不同，选择性加密方案仅作用于图像的选定部分。因此可用于许多实时医疗应用，以保护医疗记录，包括无线医疗网络和移动医疗服务。现已有边缘图[6]、感兴趣区域(ROI)[7]和基于熵[8]等选择技术。

受上述分析及研究成果的启发，本文提出了一种基于 ROI 的选择性图像无损加密方案。根据仿真结果验证，此方案可以加密图像中含有重要信息的部分。此外，为了保证足够的安全级别，本文引入了提升小波变换和混沌系统对图像进行加密。

1 选择性加密/解密方案

1.1 Tent 混沌映射

混沌系统是非线性确定系统，由于内容随机性而产生的外在复杂表现，是一种貌似随机的非随机现象[9]。混沌系统对于初始值和系统参数的敏感性，使其初始条件的微小差异会导致结果产生巨大差异。由于混沌序列具有优良的密码学特性，基于混沌的保密技术已经被应用到数据安全和通信保密等众多领域。其中 Tent 混沌映射是一种具有逐段线性的混沌映射。Tent 混沌映射可以定义为

$$x_{n+1} = g(x_n) = \begin{cases} \dfrac{x_n}{\alpha}, 0 \leqslant x_n \leqslant \alpha \\ \dfrac{1 - x_n}{1 - \alpha}, \alpha \leqslant x_n \leqslant 1 \end{cases} \quad (1)$$

其中，$\alpha \in (0,1)$。

该映射是具有均匀分布特性的函数，其产生的混沌序列具有良好的统计性质。在本文方案中设定 $\alpha = 1.999\ 999$，并用其生成置乱序列 J 和扩散序列 U。

1.2 提升小波变换

为了解决小波变换在对图像进行分解并重构的过程中会使图像的小部分信息丢失的问题，Sweldens 等[9]于 1994 年研究出了一种新的双正交小波构造方法，即提升小波变换。其使得小波构造摆脱了傅里叶变换的依赖，只在时域或空域内进行操作，简单且清晰，便于直接应用。提升方案用于构造第二代小波，第二代小波不必是一个函数的伸缩和平移[10]。实际上，提升小波变换的重构就是分解的逆过程。提升小波变换主要通过分裂/合并、预测和更新 3 个阶段完成。其中：分裂/合并是将输入的原始信号 X 分裂成两个互不相交的子集合，每个子集的长度是原来的一半。通常是将一个数列分裂成一个奇数序列 X_{odd} 和一个偶数序列 X_{even}；预测是利用偶数序列和奇数序列之间的相关性，由其中一个序列来预测另一个序列，通常用偶数序列 X_{even} 和预测算子 P 来预测奇数序列 X_{odd}；经过分裂步骤产生的子集中某些整体特征可能与原始数据并不一致，为了保持原始数据的整体特征，需要一个更新过程。更新过程用算子 U 来代替，利用更新算子 U 更新偶数序列 X_{even}，使其保持原始信号 X 的一些特性。提升小波变换过程如图 1 所示。

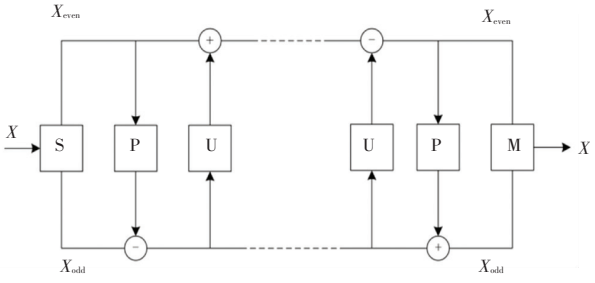


图 1 小波提升过程

Fig. 1 Wavelet lifting process

原始医学图像经过提升小波变换，可以分解成一个低频分量和 3 个高频分量。低频分量主要是对整幅图像强度的综合度量；高频分量主要是对图像边缘和轮廓的度量。由于原始图像的绝大部分能量都集中在小波变换后的低频分量上，因此只需要低频成分就可以重构与原始图像近似的图像。然而对经过频域加密后的图像进行解密时，并不是无损解密。因此，改进的算法就是在保存感兴趣区域像素高 4 位的基础上，对 ROI 的低频部分进行加密。该算法可在一定程度上降低频域加密后解密图像的失真程度。

1.3 加密方案

为了实现无损的选择性医学图像加密，整个实验方案包含图像分割、数据嵌入、图像加密 3 个主要阶段。本文在 2.1 节中已设定了 Tent 混沌映射的 α 参数，接下来将先对实验选定的医学图像进行分割，分割出 ROI 区域和 ROB 区域，在将 ROI 信息嵌入到 ROB 的 LSBs 中以后，最后使用 Tent 混沌序列产生的密钥对图像进行加密。加密方案的整体流程如图 2 所示。

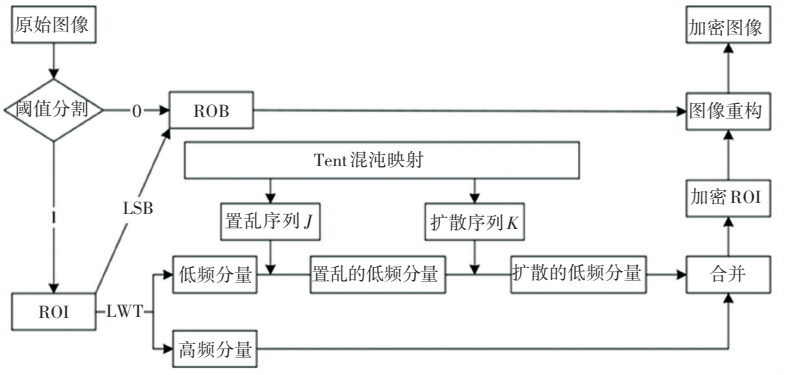


图 2　图像加密方案

Fig. 2　Image encryption scheme

1.3.1　图像分割

为了构建加密医学图像，首先要对图像进行分区：实验用的原始图像是 RGB 彩色图像，为了方便分区要先将图像转换为 8 位的灰度医学图像，尺寸是 $M \times N$ 并且像素值 $p(j,j) \in [0,256]$，$1 \leqslant i \leqslant M$，$1 \leqslant j \leqslant N$。为了重新构造加密图像，将原始图像 I 分割成 3 部分：感兴趣区域 ROI、非感兴趣区域 ROB 和边界区域(Border)。由于在大多数案例中医学图片的感兴趣区域一般是不规则图形，因此将图像的底部边框划为 Border 区域以记录 ROI 的位置信息。实验中，参数 u 设为 0，a 设定为 8。图像分割过程如下所述：

步骤 1　设定阈值分割参数。假定两个参数 u 和 a。u 是阈值分割算法的阈值参数，u 设为 0；a 是子矩阵的尺寸。子矩阵的个数可以通过 a 计算。

步骤 2　标记感兴趣区域。阈值 u 为人工设定。假定根据步骤 1 将图像 I 分解为 k 个子矩阵，$I[k]$ 表示第 k 个子矩阵，每个子矩阵的大小为 $a \times a$，$mc\_mean[k]$ 表示第 k 个子矩阵的像素均值。则 $t = \sum l_k^{ij} - mc\_mean_k$，$1 \leqslant i \leqslant a$，、$1 \leqslant j \leqslant a$，若 t 大于 u，则将此子矩阵标记为 1，反之标记为 0。

步骤 3　图像重新排列。将所有标记为 1 的元胞数组提取出来，重新排列构成新的感兴趣区域图像。

1.3.2　数据嵌入

在数据隐藏技术中，一个重要的子学科技术就是数字隐写术。隐写术是一种在封面图像中隐藏数据的方法，带有嵌入数据的图像称为隐写图像，隐写术可以在空间域或变换域中执行。隐写术为通过公共渠道进行私密和安全的通信提供了巨大的保障[11]。目标接收者可以从隐写图像中提取数据，但其他人(例如攻击者)并不知道隐写图像中存在嵌入数据[12]。

最低有效位(Least-significant-bit，LSB)数据隐藏是一种普遍的数据隐藏方法，可以将数据嵌入到图像的 LSB 中。

$$P_i = (b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0) \tag{2}$$

其中，b_0 是 LSB。数据嵌入可以通过简单地用秘密位替换 K-LSB 的 P_i 来实现，其中 $1 \leqslant k \leqslant 8$。

如果 $k = 1$，则只有 LSB 被替换为秘密位，当 $k = 8$ 时，所有位都被替换。换句话说，如果想要嵌入更多的数据，k 值应该设置的更大。

在本文的加密方案中采用最低有效位隐写术，将 ROI 的高位真实信息嵌入到 ROB 区域的 LSBs 中。

第一步：提取上一阶段分割出的 ROI 的真实信息。

第二步：将 ROI 的真实信息通过最低有效位隐写术嵌入到 ROB 的 LSBs 中。

第三步：将 ROI 的位置信息嵌入到边界区域。

1.3.3　图像加密

首先，将 ROI 区域定义为图像 I(尺寸为 $M \times N$)，并利用 Tent 混沌映射生成置乱序列 J 和扩散序列 U；之后将对图像 I 进行置乱扩散加密。ROI 区域加密过程如下：

步骤 1　对图像 I 进行提升小波变换，选取图像变换后的低频成分。

步骤 2　置乱扩散。先将图像 I 转换成一维向量，接着利用置乱序列 U 将 ROI 进行置乱。置乱后的图像 I 定义为 J，最后利用扩散序列 U 对图像 J 进行异或逻辑运算扩散，掩盖明文信息。扩散后的图像 J 定义为 E。扩散公式定义为：

$$\begin{cases} E(i+1) = (E(i) \oplus J(i)) \oplus K(i) \\ E(1) = K(1) \oplus J(1) \end{cases}$$

$$1 \leqslant i \leqslant M \times N \tag{3}$$

步骤 3 对图像 E 进行提升小波逆变换得到加密后的 ROI。此时已初步达到掩盖明文信息的要求。

步骤 4 将加密后的 ROI 和 ROB 重新构造,得到加密图像。

1.4 图像解密

由于加密/解密方案是对称的,因此图像解密实际就是加密过程的逆过程。解密流程如图 3 所示。

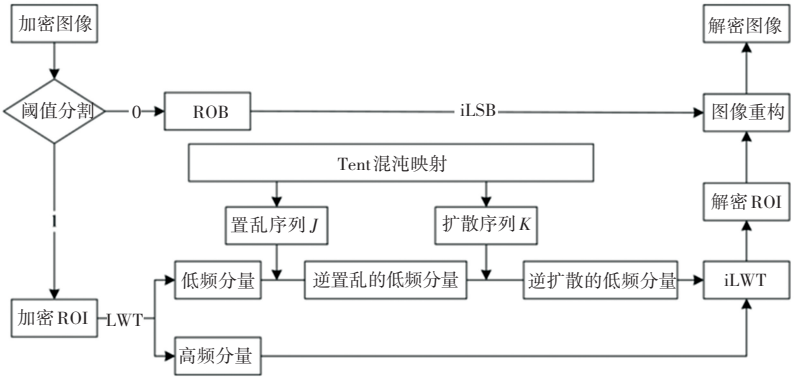


图 3 图像解密方案

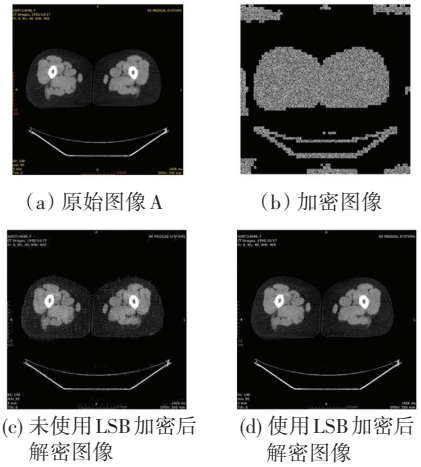
Fig. 3 Image decryption scheme

解密时,要将 Tent 的混沌序列初始值和置乱序列作为密钥传给接收方,接收方进行混沌解密反置乱和小波逆变换,就可以还原得到原始感兴趣区域图像;然后将非感兴趣区域像素的低四位数值提取出来,通过最低有效位算法,将原始图像像素的高四位数值重新嵌入到感兴趣区域,最后将感兴趣区域重新嵌入到原始图像中,就可以还原得到原始图像。

2 实验结果与分析

2.1 实验结果

为了验证和比较本文提出的加密算法性能,选择将图像分割为 8×8 大小的单元结构,分割阈值设为 0 进行仿真实验。图像 A 的灰度医学图像加解密结果如图 4 所示。



(a) 原始图像 A (b) 加密图像

(c) 未使用 LSB 加密后解密图像 (d) 使用 LSB 加密后解密图像

图 4 加密实验结果对比

Fig. 4 Comparison of encryption experiment results

2.2 ROI 统计分析

2.2.1 直方图分析

直方图分析是用于评估图像加密方案稳健性的重要指标[13],是一种视觉测试,显示了可用强度级别上的像素分布。本文计算和分析了医学图像 ROI 的直方图(如图 5 所示)。实验结果显示,加密图像 ROI 的直方图相当均匀,并且与原始图像 ROI 各个直方图明显不同,可以有效抵御任何统计攻击。且解密后图像 ROI 的直方图分布与原始图像 ROI 的分布基本相似。

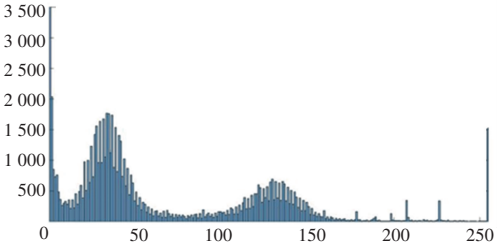
2.2.2 信息熵

信息熵是衡量图像混肴程度的重要工具。图像加密的过程其实就是一个信息熵增加的过程,信息熵越大,图像信息越混乱,图像信息不确定性越大,从而可视信息也就越少。所以,对于图像加密系统来说,需要对其密文图像的信息熵进行分析。信息熵的计算公式为

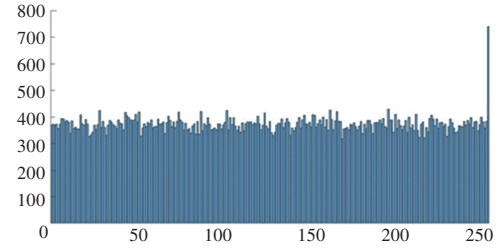
$$H = \sum_{i=0}^{255} p_{ij} \log p_{ij} \tag{4}$$

式中:i 表示像素的灰度值($0 \leqslant i \leqslant 255$),$j$ 表示邻域灰度值($0 \leqslant j \leqslant 255$)。

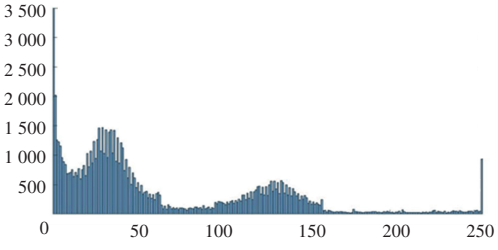
经过计算,8 位加密图像的理想信息熵为 8。当 ROI 阈值为 0 时,信息熵的计算结果,见表 1。从表 1 可见,8 位的加密图像信息熵都超过了7.997,并且非常接近 8 位图像信息熵的理想值,证明本文算法具有良好的保密效果及良好的保密等级,可以有效抵御熵的攻击。



（a）原始图像 ROI 直方图



（b）加密图像 ROI 直方图



（c）解密图像 ROI 直方图

图 5　图像 A 及加解密后的 ROI 直方图

Fig. 5　Image A and ROI histogram after encryption and decryption

表 1　信息熵对比

Tab. 1　Information entropy comparison

图像	原始图像	加密图像
a	6.154 3	7.997 7
b	7.060 0	7.999 0

2.2.3　相关性分析

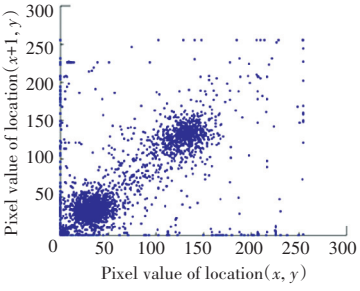
相邻像素的相关性反映了图像相邻位置像素的相关程度。在未加密的医学图像上，相邻像素的相关系数总是很高，而在加密的医学图像上，其应该显著降低。一个好的图像加密算法应该减少相邻相关系数，并尽量实现零相关[6]。通过从明文图像或加密图像中随机抽取 N 对随机相邻像素来测试像素相关性。

在相邻像素相关性方面，本文对原始图像 A 进行了相关性分析。在其明文图像和加密图像中，沿水平、垂直和对角线方向随机选取了 4 000 对相邻像素进行了相关性分析。测试结果如图 6 所示，加密图像的相关性分析结果详见表 2。

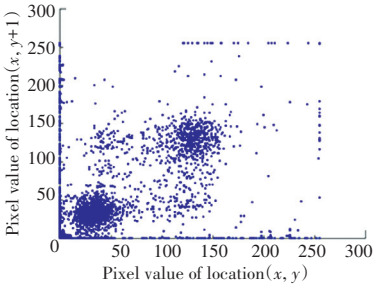
表 2　加密图像的相关性分析

Tab. 2　Correlation analysis of encrypted images

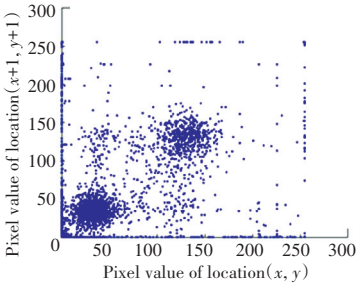
图像	水平	垂直	对角
a	−0.003 7	−0.001 4	0.012 9
b	0.011 2	0.015 8	0.023 8



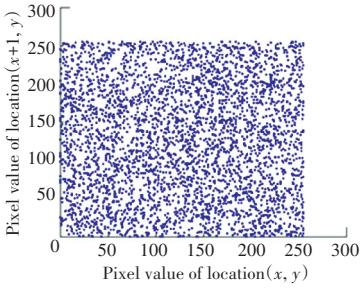
（a）明文图像水平方向相关性



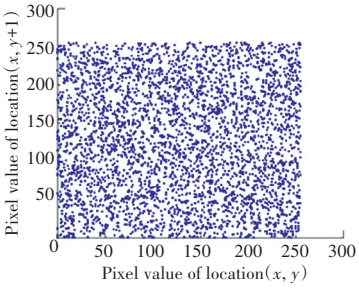
（b）明文图像垂直方向相关性



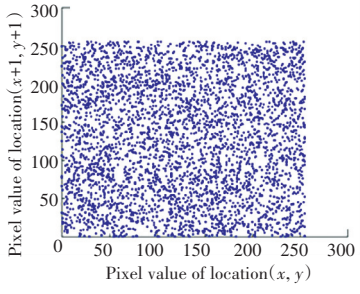
（c）明文图像对角线方向相关性



（d）加密后图像水平方向相关性



（e）加密后图像垂直方向相关性



（f）加密后图像对角线方向相关性

图 6　图像 A 的相关性分析

Fig. 6　Correlation analysis of image A

从表 2 中可以看出,加密后的图像相关系数近似为 0,表明密码图像中相邻像素在水平、垂直和对角线方向的相关系数极低,呈现低相关。因此,加密方案可以抵御基于像素相关性的统计攻击。

2.3 峰值信噪比和结构相似性

医学图像包含患者的个人信息,如果解密后的医学图像丢失过多的图像信息,就会影响医生的诊断,可能会导致误诊,甚至造成医学事故,因此医学图像应该实现无损解密。在本文的加密方案中,通过最低有效位数据隐藏方案实现医学图像主要信息的保存和还原,以此实现无损解密。

本文以峰值信噪比(*PSNR*)和结构相似性(*SSIM*)作为评价指标,来评价算法是否达到无损加密。*PSNR* 与 *SSIM* 均是最常应用的图像质量客观评价指标,*PSNR* 是基于对应像素点之间的误差,即基于误差敏感性的图像质量评价;*SSIM* 主要用来衡量图像在亮度、对比度和结构方面的相似性。如果图像是无损解密的,则原始图像和解密图像的 *PSNR* 和 *SSIM* 的理论值应为 ∞ 和 1。从表 3 中可以看出,本文的加密算法在两个指标上都有明显的提升,*SSIM* 的指标都趋近于理论值 1,*PSNR* 提升了 7 个点以上。

表 3 峰值信噪比和结构相似性对比

Tab. 3 Comparison of peak signal-to-noise ratio and structural similarity

图像	ROI	加密图像	ROI 占比	*PSNR*		*SSIM*	
				本文算法		本文算法	
a	95 232	262 144	0.363	21.780 4	29.651 4	0.844 9	0.953 4
b	188 608	262 144	0.719	26.328 0	31.475 9	0.870 5	0.931 1

3 结束语

本文提出了基于 LSB 的频域加密算法,在保证了图像安全级别的同时,也极大改善了频域加密而导致的图像信息丢失问题。同时不需要对整个图像进行加密,加密解密的速度更快,相比全图像加密,更加适合远程医疗图像的传输加密。整个方案只是使用了简单的 Tent 映射加密,未来可以选择更换混沌系统进行加密。

参考文献

[1] CHEN G, MAO Y, CHUI C K. A symmetric image encry ption based on 3D chaotic cat maps[J]. Chaos, Solitons Fractals. v21, 749-761.

[2] ENAYATIFAR R, ABDULLAH A H, ISNIN I F. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence[J]. Optics and Lasers in Engineering, 2014, 56: 83-93.

[3] ÇAVUŞOLU Ü, KAÇAR S, ZENGIN A, et al. A novel hybrid encryption algorithm based on chaos and S-AES algorithm[J]. Nonlinear Dynamics, 2018, 92(4): 1745-1759.

[4] WU J, LIAO X, YANG B. Color image encryption based on chaotic systems and elliptic curve ElGamal scheme[J]. Signal Processing, 2017, 141: 109-124.

[5] ZHOU J, LI J, DI X. A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position[J]. IEEE Access, 2020, 8: 122210-122228.

[6] ZHOU Y, PANETTA K, AGAIAN S. A lossless encryption method for medical images using edge maps[C]//2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE, 2009: 3707-3710.

[7] MAHMOOD A B, DONY R D. Segmentation based encryption method for medical images[C]//2011 International Conference for Internet Technology and Secured Transactions. IEEE, 2011: 596-601.

[8] CHEDDAD A, CONDELL J, CURRAN K, et al. Digital image steganography: Survey and analysis of current methods[J]. Signal processing, 2010, 90(3): 727-752.

[9] DAUBECHIES I, SWELDENS W. Factoring wavelet transforms into lifting steps[J]. Journal of Fourier analysis and applications, 1998, 4(3): 247-269.

[10] ZHANG Y Q, WANG X Y. A new image encryption algorithm based on non-adjacent coupled map lattices[J]. Applied Soft Computing, 2015, 26: 10-20.

[11] SUBHEDAR M S, MANKAR V H. Current status and key issues in image steganography: A survey[J]. Computer science review, 2014, 13: 95-113.

[12] SUN J, LIAO X, CHEN X, et al. Privacy-aware image encryption based on logistic map and data hiding[J]. International Journal of Bifurcation and Chaos, 2017, 27(5): 1750073.

[13] ZHANG Y Q, WANG X Y. A new image encryption algorithm based on non-adjacent coupled map lattices[J]. Applied Soft Computing, 2015, 26: 10-20.