文章编号:1007－6735(2022)03－0262－07　DOI: 10.13255/j.cnki.jusst.20211007001

一种密文域医学图像可逆信息隐藏算法

付　笛[1]，　孔　平[2]，　周　亮[2]，　张建青[3]，
周艳丽[4]，　王宏杰[4]，　陈立范[4]

（1. 上海理工大学 健康科学与工程学院，上海 200093；2. 上海健康医学院附属嘉定区中心医院，上海 201899；3. 上海健康医学院 医学影像学院，上海 201318；4. 上海健康医学院 文理教学部，上海 201318）

摘要： 鉴于图像的密文域可逆信息隐藏在安全云计算和隐私保护方面的重要作用，为了提高信息嵌入率，结合医学 DICOM 图像像素深度高、像素分布连续性高的特点，提出了一种结合两种压缩算法的密文域医学图像可逆信息隐藏算法。首先发送方对图像进行预处理，根据像素中高位比特连续为 0 的数量嵌入标记信息，腾出高位的冗余空间；然后用一种特殊设计的块加密算法进行加密，在保证明文信息不被泄露的同时保留了部分图像相关性；接着嵌入方根据标记信息，在对应位置嵌入额外信息；此外，为了进一步提高嵌入率，嵌入方还可以利用图像像素的相关性，在块内进行做差，并压缩实施信息嵌入。实验结果表明，该算法不仅具有较高的信息嵌入率，同时还有较好的安全性表现。

关键词： 医学图像；可逆信息隐藏；图像压缩；图像加密
中图分类号： TP 309.7　　**文献标志码：** A

A reversible data hiding method for encrypted medical image

FU Di[1], KONG Ping[2], ZHOU Liang[2], ZHANG Jianqing[3], ZHOU Yanli[4], WANG Hongjie[4], CHEN Lifan[4]

(1. *School of Health Science and Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China*; 2. *Jiading District Central Hospital Affiliated Shanghai University of Medicine and Health Sciences, Shanghai 201899 , China*; 3. *College of Medical Imaging, Shanghai University of Medicine and Health Sciences, Shanghai 201318, China*; 4. *College of Arts and Science, Shanghai University of Medicine and Health Sciences, Shanghai 201318, China*)

Abstract: Reversible data hiding in encrypted images (RDH-EI) is important in secure cloud computing and privacy protection. In order to improve the embedding rate, the characteristics of high pixel depth and high pixel distribution continuity of medical DICOM image was considered, and a reversible data hiding method in encrypted images combining two compression strategies was proposed in this paper. Firstly, the sender preprocessed the image and embedded the mark according to the number of consecutive high-order bits in the pixel. Then a unique block encryption algorithm was used for encryption, which ensured the plaintext information was not leaked while some image correlations were retained. The data-hider embedded additional information in the corresponding position according to the

收稿日期: 2021−10−07
基金项目: 国家自然科学基金资助项目（61672354）
第一作者: 付　笛(1997−)，男，硕士研究生．研究方向：医学图像的可逆信息隐藏．E-mail：193832382@st.usst.edu.com
通信作者: 孔　平 (1979−)，女，副教授．研究方向：智能信息处理．E-mail：kongp@sumhs.edu.cn

mark. In addition, in order to further improve the embedding rate, the data-hider can also make difference in the block and compress the space for information embedding. Experiments show that the method not only has high information embedding rate, but also has good security performance.

Keywords: *medical image*; *reversible data hiding*; *image compression*; *image encryption*

信息隐藏作为一种隐私保护技术，它能够向载体图像嵌入一段额外信息并且保证图像只有很小的改变。但是，这些改变在对图像质量要求特别高的领域比如军事图像、医学图像、法律取证等方面是无法接受的。Barton[1] 首次提出了可逆信息隐藏，可以在提取嵌入的信息后可逆恢复载体图像。

根据信息嵌入的机制，经典的可逆信息隐藏算法可以划分为 3 个主要类别：无损压缩[2]、差值扩展[3] 和直方图平移[4]。基于无损压缩的可逆信息隐藏算法通过压缩原始图像腾出空间；基于差值扩展的可逆信息隐藏通过扩大相邻像素值的差进行信息嵌入。经过广泛研究后，差值扩展发展出了整型变换[5-7] 和预测误差扩展[8-10]。在直方图平移算法中，信息隐藏通过平移直方图的峰值点实现。近年来，伴随着云计算和云存储的飞速发展，发送方(图像拥有者)希望将信息嵌入的操作委托给嵌入方(云服务器)。但是直接向嵌入方发送明文图像存在风险，为了避免信息泄漏，有人提出了密文域的可逆信息隐藏算法。在这种机制中，发送方先用加密密钥对图像进行加密，再发送给嵌入方；嵌入方通过嵌入密钥将额外信息嵌入到加密图像中；接收方提取额外信息并解密恢复原始图像。

Zhang[11] 首次提出了密文域的可逆信息隐藏算法。在该算法中，首先发送方加密图像；然后嵌入方通过翻转密文块的 3 个 LSB(最低有效位)进行信息嵌入；最后接收方解密图像并提取嵌入的信息。算法整体嵌入容量较小，并且存在一定的信息提取和图像恢复错误率。针对 Zhang 所提出的算法缺陷，Hong 等[12] 提出的改进算法充分利用像素间的相关性，利用 Side-match 技术计算图像块的平滑度并按顺序进行信息提取和图像恢复，提高了信息提取和图像恢复的正确率。Zhang[13] 提出了一种信息提取和图像恢复操作可以分离的密文域可逆信息隐藏算法，通过压缩图像部分信息以腾出空间。Liu 等[14] 提出了一种基于冗余转换的密文域可逆信息隐藏算法，将冗余空间从原始图像传输到加密图像。文献 [15]在文献 [14] 的基础上，提升了嵌入率和安全性。文献 [16] 基于傅里叶变换和 Gyrator 变换对图像进行加密，获得了较好的解密图像质量和系统安全性。文献 [17] 采用块置乱和流密码加密技术对图像进行加密，并通过分析 MSB(最高有效位)的分布对其进行自适应压缩嵌入信息。文献 [18] 用一种特殊的加密方式加密图像，并根据阈值将加密后的图像块分为平滑区和复杂区，通过替换平滑区部分像素的最高有效位进行信息嵌入，并利用 LDPC 矩阵压缩的方式对剩余像素的最低有效位再次进行信息嵌入。文献 [19] 将可逆信息隐藏算法与不可逆信息隐藏算法相结合，在失真较小的情况下实现隐藏更多的秘密信息。但是，这些算法并没有考虑医学图像的特点。

DICOM(digital imaging and communications in medical) 是医学数字成像和通信标准[20]，为数字医学影像在电脑和网络上的传输、存储提供了规范。随着云计算、计算机网络和远程医疗的飞速发展，医学图像的安全性越来越受到重视。为了保护医学图像的隐私安全，本文提出了一种适用于医学 DICOM 图像的密文域可逆信息隐藏算法，考虑医学 DICOM 图像更大像素深度和像素分布连续的特点，以期在保证图像格式以及安全性的同时，提升算法的嵌入率。

1　算法描述

密文域医学图像可逆信息隐藏算法包含发送方、嵌入方以及接收方 3 个部分。首先，发送方采用一种特殊设计的块加密算法，能够在保留部分图像相关性的同时获得较好的安全性；然后，嵌入方采用多高位比特压缩和块编码技术向加密图像进行信息嵌入；最后，接收方可以通过拥有的密钥种类对图像进行信息提取、图像解密和图像恢复 3 种操作。算法流程如图 1 所示。

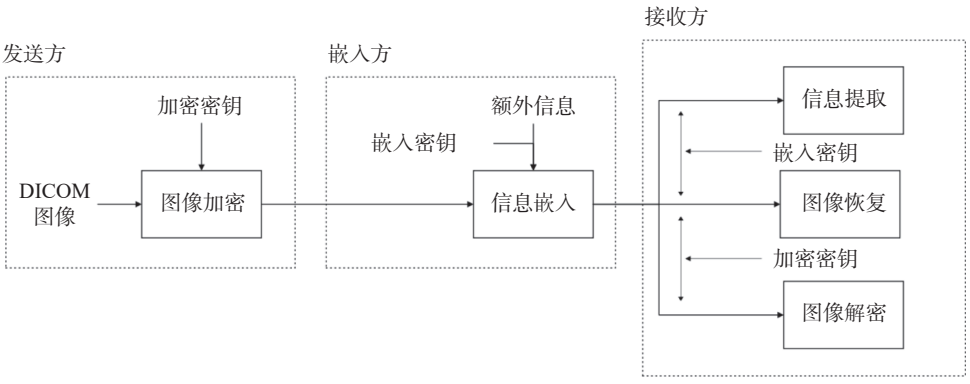


图 1 算法流程图

Fig.1 Flowchart of proposed scheme

1.1 图像加密

发送方首先将图像划分为若干个不重叠的块，为每个块生成标记信息；然后根据加密密钥 $K_e=\{K_e^{(1)},K_e^{(2)},K_e^{(3)}\}$对图像进行加密。用$K_e^{(1)}$对每个块的部分位平面进行异或加密；用$K_e^{(2)}$对块进行置乱；用$K_e^{(3)}$对像素进行置乱，得到最终的加密图像。图像加密过程如图 2 所示。

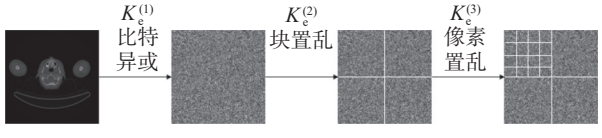


图 2 图像加密流程图

Fig.2 Flowchart of image encryption

定义大小为 $M\times N$ 且像素深度为 16 的原始 DICOM 图像为 I。将像素值分为 12 个区间 T_1，T_2，…，T_{12}(除了 4 个 MSB 的其他位平面)，统计各个区间的像素数并找到最多的 4 个区间 T_a，T_b，T_c，T_d。将处于 4 个区间以外的其他区间合并到这 4 个区间中，合并方法如图 3 所示。其中：T_a 表示像素值占据了 1 个 LSB；T_b 表示像素值占据了 4 个 LSB；T_c 表示像素值占据了 8 个 LSB；T_d 表示像素值占据了 12 个 LSB。

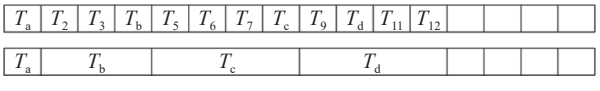


图 3 区间合并示例

Fig.3 Example of intervals merging

根据哈夫曼编码思想，分别用 0，10，110，111 标记属于这 4 个区间的像素。将图像分为若干个大小为 $S\times S$ 的不重叠块，然后统计块内所有像素表示的标记，记录其中最大的标记，并用该标记替换块中第一个像素的 MSB。根据加密密钥 $K_e^{(1)}$，对每个块的像素中除了标记信息以外的所有比特进行异或，定义 $b_{i,j}$ 为位置 (i,j) 的像素，$b_{i,j,1}$，$b_{i,j,2}$，…，$b_{i,j,u}$ 表示像素 $b_{i,j}$ 中的 16 个比特。

$$b'_{i,j,u}=b_{i,j,u}\oplus r_{i,j,u},\ k_{i,j}<u\leqslant 16 \tag{1}$$

式中：$r_{i,j,u}$ 为由加密密钥生成的伪随机比特流；$k_{i,j}$ 为 $b_{i,j}$ 中标记长度。

在嵌入标记后，根据加密密钥$K_e^{(2)}$，将所有图像块置乱。最后，根据加密密钥$K_e^{(3)}$，对每个块内的像素进行置乱，并得到最终的加密图像 I_e。

1.2 信息嵌入

嵌入方收到加密图像后，首先识别标记，并将标记的长度定义为$l_m^{i,j}$，然后将图像分割为若干个大小为 $S\times S$ 的不重叠块，根据发送方额外发送的信息解析块中第一个像素的标记，计算出像素中加密数据的长度$l_p^{i,j}$。每个块中可以嵌入的比特数为 $S^2\times(16-l_p^{i,j})-l_m^{i,j}$。嵌入方可以通过嵌入密钥$K_h^{(1)}$将额外信息进行加密，并将加密后的额外信息嵌入腾出的空间中，得到嵌入信息后的加密图像。

此外，为了提高嵌入率，嵌入方还可以对加密图像进行块编码，并利用嵌入密钥$K_h^{(2)}$向腾出的空间嵌入信息。定义 $B_{u,v}$ 为坐标 (u,v) 的图像块。对于每个块，找到其中加密数据值最大的像素 P_m，并用其减去块内剩余像素的加密数据值，获得差值 $d_1,d_2,\cdots,d_n$，其中 $n=S^2-1$。按下列方式对块进行重新编码：用 b_2 表示最大的加密数据值，b_2 的长度 l_2 是该块中所有标记可表示的最大长度；用 b_3 表示最大像素的索引，b_3 的长度是 l_3；用 b_5 表示差值的长度，b_5 的长度为 l_5；l_5 的长度用 b_4 表示，b_4 的长度是 l_4。

$$l_3=\lceil\log_2 S^2\rceil \tag{2}$$

$$l_4 = \begin{cases} 0, & P_m \leqslant \lambda \\ 3, & P_m > \lambda \end{cases} \tag{3}$$

$$l_5 = \begin{cases} 0, & P_m \leqslant \lambda \\ \sum_{k=1}^{l_4} b_4^k, & P_m > \lambda \end{cases} \tag{4}$$

式中，λ表示阈值。

如果 $P_m \leqslant \lambda$，则不需要 b_4，且 b_5 的长度为 3，否则需要一个长度为 3 的 l_4 记录 b_5 的长度。使用b_6^1，b_6^2，…，b_6^n表示差值，最后计算 b_2，b_3，b_4，b_5，b_6^1，b_6^2，…，b_6^n长度的和。如果该和大于原加密数据长度的和 l_m，表示该块无法进行信息嵌入，则 b_1 的值为 0，否则值为 1。被 b_1 替换的 LSB 与额外信息一起嵌入压缩后腾出的空间内。用于嵌入额外信息的 b_s 的长度 l_s 可以用式(5)计算。

$$l_s = l_m - \sum_{k=1}^{6} b_i \tag{5}$$

图 4 给出了块编码的示例，在该示例中，区间 $T_a = [2, 5]$，$T_b = [1, 1]$，$T_c = [11,12]$，$T_d = [6, 10]$，并且标记分别为 0，10，110，111。$S=2$，因此每个块由 4 个像素组成。第一行表示已加密的 4 个像素，其中灰色表示加密后的像素值，蓝色表示标记，白色表示已经嵌入的额外信息。第二行表示加密数据、差值、最大像素值，第三行表示重编码后的像素。

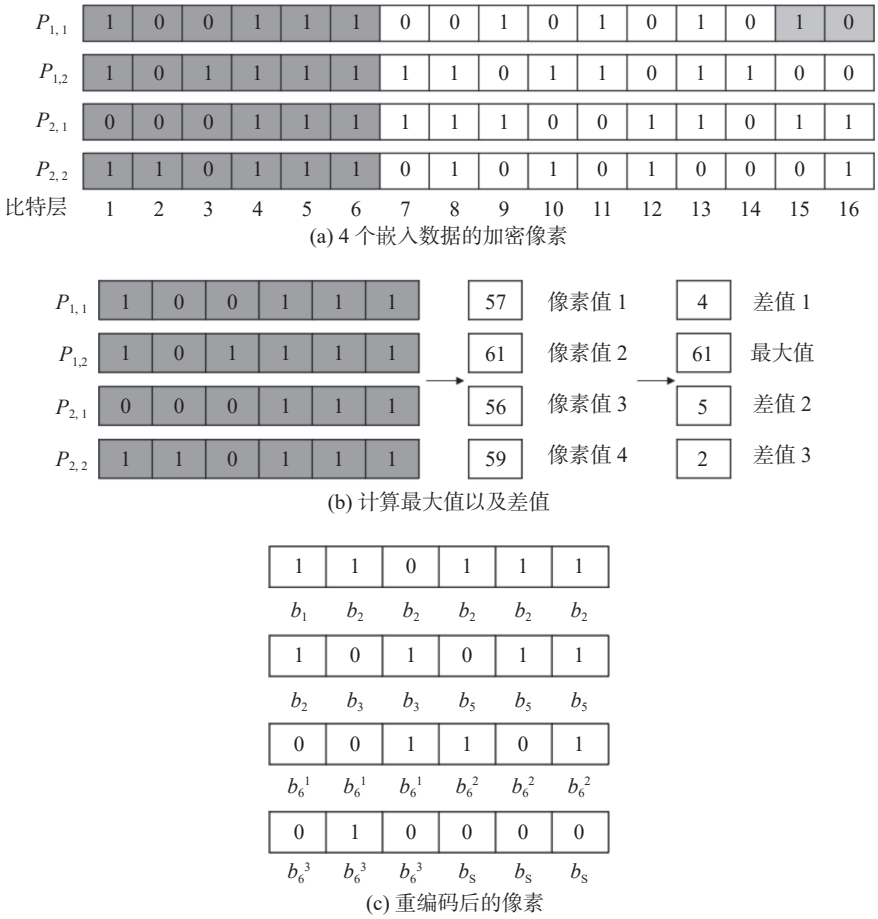


图 4　块编码示例

Fig.4　Example of block encoding

该示例中，块中第一个加密像素的标记为 10，根据发送方额外发送的信息可以得知，10 标记位表示加密像素数据占有 6 个比特，因此可以获取加密像素数据的位平面是 1 至 6 位。找出该块中 4 个加密像素数据的最大值，并对其他 3 个加密像素数据作差，经过计算后得到 $l_1 = 1$，$l_2 = 6$，$l_3=2$，$l_4=0$，$l_5=3$，$l_6^1 = l_6^2 = l_6^3 = 3$，$l_m=24$，$l_s=l_m-(l_1 + l_2 + l_3 + l_4 + l_5 + l_6^1 + l_6^2 + l_6^3) = 3$，即可以嵌入 3 个比特，$b_1 = 1$。用重编码后的块替换原始块，每个块中可以嵌入的比特数为 l_s。嵌入方可以通过嵌入

密钥$K_h^{(2)}$将额外信息进行加密，并将加密后的额外信息嵌入腾出的空间中，得到嵌入信息后的加密图像$I_{ew}^{(2)}$。

1.3 信息提取和图像恢复

获取嵌入信息的加密医学图像$I_{ew}^{(2)}$后，接收方可以根据拥有的密钥种类进行不同的操作。

a. 拥有加密密钥$K_e=\{K_e^{(1)},K_e^{(2)},K_e^{(3)}\}$。接收方首先识别标记并根据标记获取原有像素数据所在的位平面，反编码经过压缩的块；然后用加密密钥$K_e^{(3)}$对块内像素进行置乱；接着用加密密钥$K_e^{(2)}$对块进行置乱；再使用加密密钥$K_e^{(1)}$对像素内比特进行异或解密；最后将除像素数据以外的比特位值置为 0。此时获得一张几乎与原始图像一模一样的恢复图像。如果接收到的图像只经过一次嵌入而没有通过块编码进行二次嵌入，那么经过解密可以获得与原始图像相同的恢复图像。

b. 拥有嵌入密钥$K_h^{(1)}$和$K_h^{(2)}$。接收方首先识别标记并根据标记获取原有像素数据所在的位平面，剩下的位置存储的是嵌入的额外信息，接收方通过嵌入密钥$K_h^{(1)}$生成的伪随机比特流对其进行异或解密即可提取嵌入的信息。

读取加密像素数据，根据 b_1 的值判断块内是否被二次嵌入额外信息，如果 b_1 的值为 1，则块内存在额外信息。根据上文的块编码方式，解析块并获取额外信息 b_s；最后接收方通过嵌入密钥$K_h^{(2)}$生成的伪随机比特流对其进行异或解密，即可提取嵌入的信息。

c. 拥有加密密钥$K_e=\{K_e^{(1)},K_e^{(2)},K_e^{(3)}\}$和嵌入密钥$K_h^{(1)}$和$K_h^{(2)}$。接收方首先按照 b 中的方法进行信息提取，然后用 a 中的方法对图像进行解密，最后根据提取的信息恢复每个块中第一个像素被替换的 LSB，此时得到与原始图像完全相同的恢复图像。

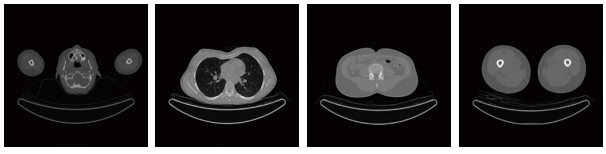
2 实验结果分析

实验所用硬件系统为 4.2 GHz Intel i7 处理器、16.00 GB 内存、Windows 10 操作系统的台式电脑，算法软件应用 Matlab R2018b。实验针对一个 DICOM 图像库进行，图 5 为其中的 4 张 CT 图像。以下从各个方面对实验结果进行分析。

2.1 加密图像直方图分析

图 6 给出了图 5(a) 的原始图像以及 3 次加密后的图像，根据图 7 的直方图分析可以看出，无法从直方图分布中获取明文图像的信息。

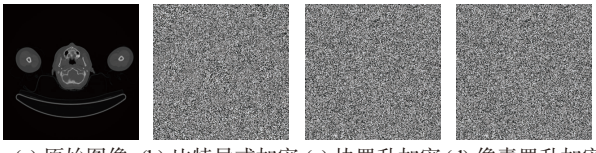
由图 7 可以看出，原始 CT 图像中，像素主要分布于 0 附近，而加密后的密文图像直方图分布



(a) CT1 (b) CT2 (c) CT3 (d) CT4

图 5 DICOM 图像库中的 4 张 CT 图像

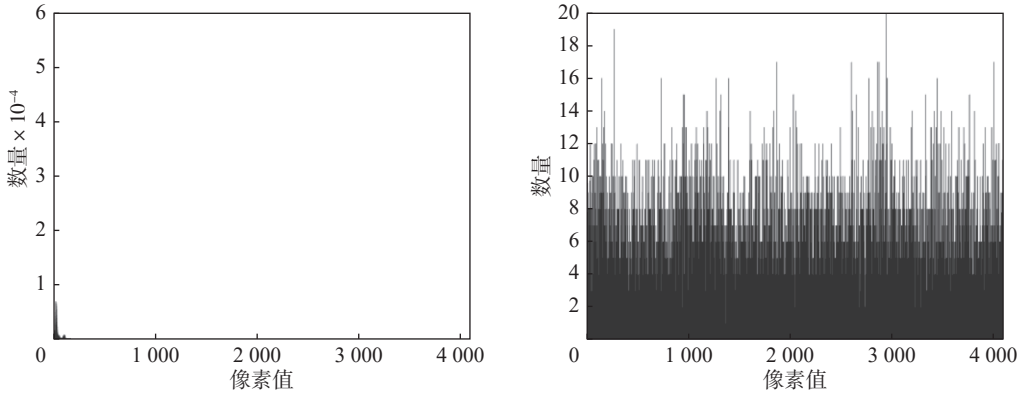
Fig. 5 Four CT images in DICOM image library



(a) 原始图像 (b) 比特异或加密 (c) 块置乱加密 (d) 像素置乱加密

图 6 原始 CT 图像与经过异或、块置乱和像素置乱加密后的图像

Fig. 6 Original CT image and images encrypted by bit xor, block scrambling and pixel scrambling



(a) 原始图像直方图 (b) 加密图像直方图

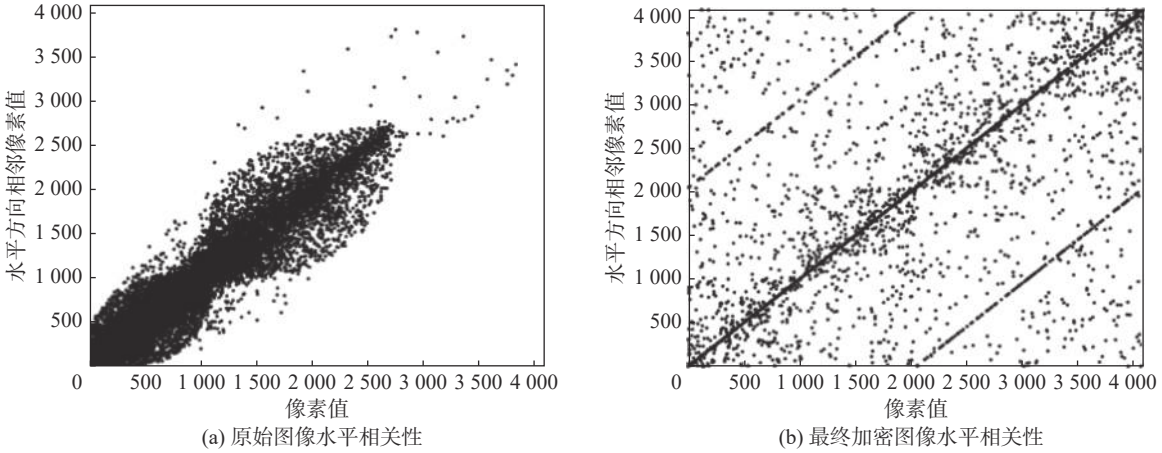
图 7 原始 CT 图像和最终加密图像的直方图

Fig.7 Histograms of original CT image and encrypted image

均匀，保护了明文信息的安全，从视觉和像素分布上都不能得到原图像的信息。

2.2　加密图像相关性和熵值分析

图 8 给出了图 5(a) 的水平相关性以及 3 次加密后的水平相关性。从图 8 可以看出，原始图像具有很强的水平相关性，加密后图像虽然仍有一定的水平相关性，但是相较原始图像，降低了很多。表 1 中给出了图 5 中 4 张 CT 图像加密前后图像的一维熵，原始图像和加密图像的像素深度都是 16，从表中可以看出，原始图像的熵值较低，经过加密后图像的熵值接近 16，证明了算法是安全的。



(a) 原始图像水平相关性　　(b) 最终加密图像水平相关性

图 8　原始 CT 图像和最终加密图像的水平相关性

Fig.8　Horizontal correlation of original CT image and encrypted image

表 1　加密前后图像的一维熵

Tab.1　Order-1 entropies before and after encryption for images

图像	加密前	加密后($S=2$)
CT1	6.7207	15.2917
CT2	6.8655	15.5486
CT3	6.4133	15.2545
CT4	6.5308	15.5329

一维熵的计算公式为

$$H^{(1)}(\beta)=-\sum_{i=1}^{h}P(\beta_i)\log_2 P(\beta_i) \qquad (6)$$

2.3　算法嵌入率和直接解密图像峰值信噪比分析

嵌入率(BPP)表示平均每个像素可以嵌入比特数量，其值越大表示可以嵌入的数据越多。峰值信噪比(PSNR)表示解密图像的质量，其值越高表示与原始图像的差异越小。表 2 和表 3 分别表示了本算法对图 5 中 4 张 CT 图像进行实验得到的嵌入率和峰值信噪比。其中：嵌入率 τ_1 表示通过压缩高位 MSB 得到的结果，嵌入率 τ_2 表示通过块编码得到的结果。

从表 2 可以看出，本算法能够获取良好的嵌入率，特别是压缩多高位比特时获得的嵌入率 τ_1 接近 8.5 bpp(bit per pixel)，而块编码获得的嵌入率受到块边长 S 的影响，S 过小或过大时都会降低嵌入率。因为块边长过小时，用于压缩的比特数目较少导致辅助信息所占比例增加，所以会降低嵌入率；块边长 S 过大时，块内像素的差异会变大，计算得到的差也会变大，同样导致辅助信息所占比例增加，降低嵌入率。

从表 3 可以看出，本算法能够获得良好的解密图像质量，此外，如果未采用块编码方式进行二次信息嵌入，解密图像将与原始图像完全相同。

表 2　不同块边长下的嵌入率

Tab.2　Embedding rates with different block sizes

DICOM 图像	嵌入率τ_1	嵌入率τ_2					
		$S=2$	$S=3$	$S=4$	$S=8$	$S=12$	$S=16$
CT1(281)	8.5132	0.9019	1.0912	1.1129	0.8436	0.6887	0.5866
CT2(320)	8.4327	0.7934	0.9154	0.8685	0.5697	0.4089	0.3653
CT3(360)	8.4109	0.8457	1.0260	0.9910	0.6278	0.4594	0.3908
CT4(500)	8.2903	0.9153	1.1191	1.1110	0.8086	0.5704	0.4431

表 3 不同块边长下的峰值信噪比

Tab.3 PSNR with different block sizes

DICOM 图像	峰值信噪比(PSNR)					
	$S=2$	$S=3$	$S=4$	$S=8$	$S=12$	$S=16$
CT1(281)	135.1	142.3	143.0	132.9	128.6	124.3
CT2(320)	150.1	155.4	153.2	138.5	131.2	128.7
CT3(360)	138.7	141.2	140.5	132.5	128.7	127.5
CT4(500)	138.2	142.4	141.7	136.7	129.5	126.5

3 结 论

提出了一种基于多高位比特压缩和块编码的密文域医学图像可逆信息隐藏算法。通过一种独特设计的加密算法，每个图像块中的相关性得到了部分保留。嵌入方可以通过压缩高位比特对加密图像进行信息嵌入。此外，为了进一步提高嵌入率，嵌入方还可以通过块编码的方式对加密图像进行二次嵌入。接收方可以根据自己拥有的密钥种类进行信息提取、图像解密或图像恢复。实验结果表明，该算法获得了良好的嵌入率以及较好的安全性。

参考文献：

[1] BARTON J M. Method and apparatus for embedding authentication information within digital data：U.S.Patent 5646997[P]. 1997-07-08.

[2] FRIDRICH J, GOLJAN M, DU R. Lossless data embedding —new paradigm in digital watermarking[J]. EURASIP Journal on Advances in Signal Processing, 2002, 2002(1): 185-196.

[3] TIAN J. Reversible data embedding using a difference expansion[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 890–896.

[4] NI Z C, SHI Y Q, ANSARI N, et al. Reversible data hiding[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2006, 16(3): 354–362.

[5] COLTUC D, CHASSERY J M. Very fast watermarking by reversible contrast mapping[J]. IEEE Signal Processing Letters, 2007, 14(4): 255–258.

[6] WENG S W, ZHAO Y, PAN J S, et al. Reversible watermarking based on invariability and adjustment on pixel pairs[J]. IEEE Signal Processing Letters, 2008, 15: 721–724.

[7] WANG X, LI X L, YANG B, et al. Efficient generalized integer transform for reversible watermarking[J]. IEEE Signal Processing Letters, 2010, 17(6): 567–570.

[8] HU Y J, LEE H K, LI J W. DE-based reversible data hiding with improved overflow location map[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2009, 19(2): 250–260.

[9] SACHNEV V, KIM H J, NAM J, et al. Reversible watermarking algorithm using sorting and prediction[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2009, 19(7): 989–999.

[10] TAI W L, YEH C M, CHANG C C. Reversible data hiding based on histogram modification of pixel differences[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2009, 19(6): 906–910.

[11] ZHANG X P. Reversible data hiding in encrypted image[J]. IEEE Signal Processing Letters, 2011, 18(4): 255–258.

[12] HONG W, CHEN T S, WU H Y. An improved reversible data hiding in encrypted images using side match[J]. IEEE Signal Processing Letters, 2012, 19(4): 199–202.

[13] ZHANG X P. Separable reversible data hiding in encrypted image[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 826–832.

[14] LIU Z L, PUN C M. Reversible data-hiding in encrypted images by redundant space transfer[J]. Information Sciences, 2018, 433–434: 188–203.

[15] QIN C, QIAN X K, HONG W, et al. An efficient coding scheme for reversible data hiding in encrypted image with redundancy transfer[J]. Information Sciences, 2019, 487: 176–192.

[16] 蔡宁, 沈学举. 基于傅里叶变换和 Gyrator 变换的图像加密 [J]. 光学仪器, 2015, 37(1): 75–78.

[17] FU Y J, KONG P, YAO H, et al. Effective reversible data hiding in encrypted image with adaptive encoding strategy[J]. Information Sciences, 2019, 494: 21–36.

[18] ZHANG W, KONG P, YAO H, et al. Real-time reversible data hiding in encrypted images based on hybrid embedding mechanism[J]. Journal of Real-Time Image Processing, 2019, 16(3): 697–708.

[19] 蒋婵钰, 张紫欣, 秦川. 基于多目标优化的明文域信息隐藏算法 [J]. 光学仪器, 2021, 43(6): 19–25.

[20] PIANYKH O S. Digital imaging and communications in medicine (DICOM): a practical introduction and survival guide[M]. 2nd ed. Heidelberg: Springer, 2012.

（编辑：丁红艺）