文章编号:1007－6735(2024)01－0095－08 DOI: 10.13255/j.cnki.jusst.20221021003

用于实现医学图像对比度增强的密文域可逆信息隐藏算法

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

（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 协同科研中心，上海 201318；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： 针对现有密文域医学图像可逆信息隐藏算法存在解密图像视觉质量较低的问题，提出了一种基于差值直方图平移的密文域可逆信息隐藏算法。首先，发送方采用具有同态密文比较性质的加密算法对原始医学图像进行加密，从而保证医学图像的隐私内容不被泄露。然后，嵌入方利用同态性质对接收到的密文图像计算差值直方图，并通过平移差值直方图在密文图像中嵌入信息。为了获得较大的嵌入率，嵌入方可对密文图像进行多轮次信息嵌入。最后，接收方根据拥有的密钥种类对接收到的含有嵌入信息的密文图像进行信息提取、图像解密和图像恢复。实验结果表明，本文算法提升了解密医学图像的视觉质量，同时具有较高的嵌入率和安全性。

关键词： 可逆信息隐藏；医学图像；直方图平移；同态加密；图像对比度增强
中图分类号： TP 309.7 **文献标志码：** A

Reversible data hiding method in encrypted domain for the contrast enhancement of medical image

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

(1. *School of Health Science and Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China*; 2. *Collaborative Innovation Center, Shanghai University of Medicine and Health Sciences, Shanghai 201318, 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: Aiming at the problem that the visual quality of the decrypted image is low in the existing reversible data hiding methods for the encrypted medical image, a reversible data hiding method in encrypted domain based on the difference histogram shift was proposed. Firstly, to ensure that the private content of the medical image was not leaked, the sender using an encryption algorithm with the property of homomorphic ciphertext comparison encrypted the original medical image. Then, on the data-hider side, the difference histogram of the received encrypted image was calculated using the homomorphic property, and the secret data was embedded in the encrypted image by shifting the

收稿日期: 2022−10−21
基金项目: 国家重点研发计划（2022YFC3103-003002）；上海市浦江人才计划（22PJD031）
第一作者: 李 安（1998−），男，硕士研究生．研究方向：医学图像的可逆信息隐藏．E-mail：202562440@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

difference histogram. In order to obtain a high embedding rate, the data-hider could conduct multiple rounds of data embedding in the encrypted image. Finally, according to the type of the keys possessed, the receiver could perform data extraction, image decryption and image recovery for the received encrypted image containing embedded data. The experimental results show that the proposed method improves the visual quality of the decrypted medical image, and has high embedding rate and security.

Keywords: *reversible data hiding*; *medical image*; *histogram shift*; *homomorphic encryption*; *image contrast enhancement*

随着远程医疗、智慧医疗和云医疗的飞速发展，医学图像的隐私保护与内容认证越来越重要。密文域可逆信息隐藏作为一种隐私保护技术受到了广泛的关注。该技术能够向加密的载体图像嵌入一段额外信息，在解密图像中难以察觉嵌入信息的存在，在提取嵌入信息后可逆恢复载体图像。

Zhang[1] 提出了一种经典的密文域可逆信息隐藏算法，它通过翻转密文块中部分像素的最低3位有效位来嵌入信息。该算法的嵌入率低，在信息提取和图像恢复过程中存在一定的错误率。近几年，学者们提出了很多先进的密文域可逆信息隐藏算法。如 Fu 等[2] 提出了一种基于自适应编码策略的密文域可逆信息隐藏算法，它根据最高有效位出现的频率，自适应地压缩可嵌入块的最高有效位比特层来腾出空间容纳嵌入信息。该算法有较好的率失真性能和较高的嵌入率。Qiu 等[3] 提出了一种基于自适应整数变换的密文域可逆信息隐藏算法，它通过可逆的整数变换去除像素的最低有效位，并将信息嵌入在像素的最低有效位，该算法有较高的嵌入容量。Yu 等[4] 提出了一种新颖的密文域可逆信息隐藏算法，可以在无需知道加密方法或原始图像先验知识的前提下，通过简单的最高有效位替换将额外信息嵌入到加密图像中。但是这些算法均是针对自然图像设计的，不适用于医学图像。因此，医学图像的隐私安全问题亟需设计专门的算法。

Bhardwaj 等[5] 提出一种密文域医学对偶图像可逆信息隐藏算法。该算法为了提高医学图像的嵌入率，将嵌入的信息转换为 base-3 数字框架来解决零值不嵌入问题。Kong 等[6] 提出了一种具有篡改定位功能的密文域医学图像可逆信息隐藏算法。为了提高医学图像恢复的准确率，该算法只在加密图像的部分区域嵌入信息。由于其嵌入信息的方式与 Zhang[1] 的算法类似，在信息提取和图像恢复过程中会存在一定的错误率。由于大多数医学图像是 16 位的灰度图像，Dzwonkowski 等[7] 提出了一种基于循环二进制 Golay(23,12) 码的密文域医学图像可逆信息隐藏算法。该算法在加密图像的最低有效位中嵌入额外信息，而最高有效位被用于确保嵌入过程的可逆性。付笛等[8] 利用医学图像像素深度高、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可逆信息隐藏算法。该算法通过两种压缩算法分别对加密图像的高位比特层和低位比特层进行压缩，从而腾出空间容纳嵌入信息。但是这些算法都存在解密医学图像视觉质量下降的问题。

为了提升解密后医学图像的视觉质量，本文提出了一种基于差值直方图平移的密文域医学图像可逆信息隐藏算法。在该算法中，信息的嵌入不仅使解密医学图像具有对比度增强的效果，且该算法是完全可逆的，即信息提取和图像恢复的错误率为 0，同时算法嵌入的信息量越大，医学图像的对比度增强效果越显著。实验结果表明，本文算法具有较高的嵌入率、解密图像质量和安全性。

1 本文算法

算法流程如图 1 所示。下文将详细阐述算法的图像加密、信息嵌入、信息提取和图像恢复等内容。

1.1 图像加密

为了保护医学图像的隐私，本文采用一种具有同态密文比较性质的同态加密算法[9] 对医学图像进行加密。该同态加密算法基于共轭搜索问题来实现单向安全，支持矩阵环上的实数加密。

假设$\mathbb{R}$是一个实数域，$\boldsymbol{\Psi}$是$\mathbb{R}$上一个2×2的矩阵环。发送方利用加密密钥$\boldsymbol{K}_{\mathrm{e}}=\{K_{\mathrm{e}}^{(1)},K_{\mathrm{e}}^{(2)}\}$分别生成

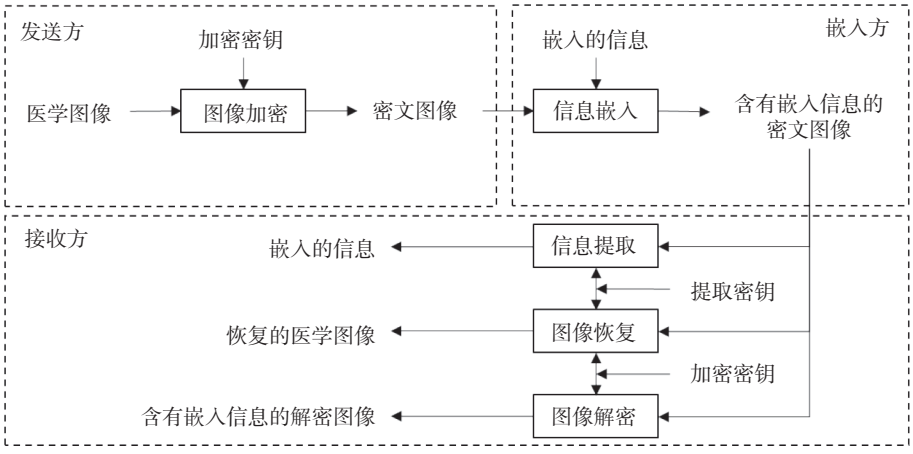


图 1　算法流程图

Fig.1　Flowchart of the proposed scheme

一个随机的可逆矩阵$\boldsymbol{H}$和一个扰动矩阵$\boldsymbol{R}$：

$$\begin{cases} \boldsymbol{H}=\begin{bmatrix} \boldsymbol{h}_1 & \boldsymbol{h}_2 & \boldsymbol{h}_3 \\ \boldsymbol{h}_4 & \boldsymbol{h}_5 & \boldsymbol{h}_6 \\ \boldsymbol{h}_7 & \boldsymbol{h}_8 & \boldsymbol{h}_9 \end{bmatrix} \\ \boldsymbol{R}=\begin{bmatrix} \boldsymbol{r}_1 & \boldsymbol{r}_2 & \boldsymbol{r}_3 \\ \boldsymbol{r}_4 & \boldsymbol{r}_5 & \boldsymbol{r}_6 \\ \boldsymbol{r}_7 & \boldsymbol{r}_8 & \boldsymbol{r}_9 \end{bmatrix} \end{cases} \tag{1}$$

式中，$\boldsymbol{h}_1,\boldsymbol{h}_2,\cdots,\boldsymbol{h}_9\in\boldsymbol{\Psi}$，且$\boldsymbol{r}_1,\boldsymbol{r}_2,\cdots,\boldsymbol{r}_9\in\boldsymbol{\Psi}$。$\boldsymbol{h}_1,\boldsymbol{h}_2,\cdots,\boldsymbol{h}_9$和$\boldsymbol{r}_1,\boldsymbol{r}_2,\cdots,\boldsymbol{r}_9$都是2×2的矩阵。由此可见，$\boldsymbol{H}$和$\boldsymbol{R}$都是6×6的矩阵。

定义大小为$U\times V$的医学图像为$\boldsymbol{I}$。假设$\boldsymbol{I}$中(i,j)位置上像素的灰度值为$\boldsymbol{I}_{i,j}$。发送方对$\boldsymbol{I}$进行加密就是利用矩阵$\boldsymbol{H}$和$\boldsymbol{R}$将$\boldsymbol{I}$中每个像素的灰度值都加密成一个密文。发送方首先将$\boldsymbol{I}$中每个像素的灰度值$\boldsymbol{I}_{i,j}$随机拆分成 6 个不为 0 的值m_1，m_2，m_3，m_4，m_5，m_6，其中，$m_1>m_2$，$m_3>m_4$，$m_5>m_6$，且$\boldsymbol{I}_{i,j}=m_1+m_2=m_3+m_4=m_5+m_6$。然后，用这 6 个值生成 3 个2×2的矩阵$\boldsymbol{M}_1,\boldsymbol{M}_2,\boldsymbol{M}_3$：

$$\begin{cases} \boldsymbol{M}_1=\begin{bmatrix} m_1 & m_2 \\ m_2 & m_1 \end{bmatrix} \\ \boldsymbol{M}_2=\begin{bmatrix} m_3 & m_4 \\ m_4 & m_3 \end{bmatrix} \\ \boldsymbol{M}_3=\begin{bmatrix} m_5 & m_6 \\ m_6 & m_5 \end{bmatrix} \end{cases} \tag{2}$$

最后，用矩阵$\boldsymbol{H}$和$\boldsymbol{R}$将这 3 个矩阵$\boldsymbol{M}_1,\boldsymbol{M}_2,\boldsymbol{M}_3$加密成密文$\boldsymbol{E}_{i,j}$：

$$\boldsymbol{E}_{i,j}=\mathfrak{E}\left(\boldsymbol{I}_{i,j}\right)+\boldsymbol{R} \tag{3}$$

$$\mathfrak{E}\left(\boldsymbol{I}_{i,j}\right)=\boldsymbol{H}\cdot\begin{bmatrix} \boldsymbol{M}_1 & \boldsymbol{n}_1 & \boldsymbol{n}_2 \\ \boldsymbol{O} & \boldsymbol{M}_2 & \boldsymbol{n}_3 \\ \boldsymbol{O} & \boldsymbol{O} & \boldsymbol{M}_3 \end{bmatrix}\cdot\boldsymbol{H}^{-1} \tag{4}$$

式中：$\mathfrak{E}(\cdot)$为加密函数；$\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{n}_3$均是从$\boldsymbol{\Psi}$中随机挑选的；$\boldsymbol{O}$为2×2的全零矩阵。

当将$\boldsymbol{I}$中所有像素的灰度值都加密成密文后，收集所有密文，生成密文图像$\boldsymbol{E}$。需要强调的是，$\boldsymbol{E}_{i,j}$是由$\boldsymbol{I}_{i,j}$加密而成的密文，不是单个值，而是6×6的矩阵。因此，$\boldsymbol{E}_{i,j}$也不是对$\boldsymbol{E}$中(i,j)位置上单个值的索引，而是对$\boldsymbol{E}$中(i,j)位置上密文的索引。图 2 为密文图像中密文索引的示例。

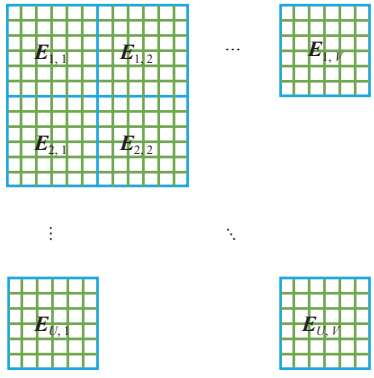


图 2　密文索引示例

Fig.2　Example of the ciphertext indexing

此外，发送方用随机矩阵$\boldsymbol{H}$生成一个用于同态密文比较的公开矩阵$\boldsymbol{T}$：

$$\boldsymbol{T}=\boldsymbol{H}\cdot\begin{bmatrix} \boldsymbol{\delta} & \boldsymbol{n}_4 & \boldsymbol{n}_5 \\ \boldsymbol{O} & \boldsymbol{\delta} & \boldsymbol{n}_6 \\ \boldsymbol{O} & \boldsymbol{O} & \boldsymbol{\delta} \end{bmatrix}\cdot\boldsymbol{H}^{-1} \tag{5}$$

$$\boldsymbol{\delta}=\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{6}$$

式 (5) 中，$\boldsymbol{n}_4,\boldsymbol{n}_5,\boldsymbol{n}_6$也均是从$\boldsymbol{\Psi}$中随机挑选的，并生成一个用于平移差值直方图的偏移子$\boldsymbol{\sigma}=\mathfrak{E}(1)$。需要说明的是，$\boldsymbol{T}$和$\boldsymbol{\sigma}$是公开的，即发送方、嵌入方和接收方都知晓。最后，发送方将密文图像$\boldsymbol{E}$发送给嵌入方。

1.2 信息嵌入

嵌入方接收到密文图像$\boldsymbol{E}$后，将$\boldsymbol{E}$分成$(UV)/9$个不重叠密文块$\boldsymbol{B}^{(1)},\boldsymbol{B}^{(2)},\cdots,\boldsymbol{B}^{((UV)/9)}$。每个密文块$\boldsymbol{B}^{(l)}(l=1,2,\cdots,(UV)/9)$内有 9 个密文，每行每列各 3 个密文，如图 3 所示。

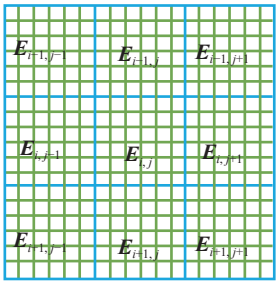


图 3 一个密文块的图解

Fig.3 Illustration of a ciphertext block

由图 3 可知，每个密文块$\boldsymbol{B}^{(l)}$内都有 1 个中心密文$\boldsymbol{E}_{i,j}$和 8 个周边密文。对于每个密文块$\boldsymbol{B}^{(l)}$，嵌入方根据式 (7) 计算 8 个差值：

$$\begin{cases}\boldsymbol{D}_{i,j-1}=\boldsymbol{E}_{i,j-1}-\boldsymbol{E}_{i,j}\\ \boldsymbol{D}_{i-1,j}=\boldsymbol{E}_{i-1,j}-\boldsymbol{E}_{i,j}\\ \boldsymbol{D}_{i,j+1}=\boldsymbol{E}_{i,j+1}-\boldsymbol{E}_{i,j}\\ \boldsymbol{D}_{i+1,j}=\boldsymbol{E}_{i+1,j}-\boldsymbol{E}_{i,j}\\ \boldsymbol{D}_{i-1,j-1}=\boldsymbol{E}_{i-1,j-1}-\boldsymbol{E}_{i,j}\\ \boldsymbol{D}_{i-1,j+1}=\boldsymbol{E}_{i-1,j+1}-\boldsymbol{E}_{i,j}\\ \boldsymbol{D}_{i+1,j-1}=\boldsymbol{E}_{i+1,j-1}-\boldsymbol{E}_{i,j}\\ \boldsymbol{D}_{i+1,j+1}=\boldsymbol{E}_{i+1,j+1}-\boldsymbol{E}_{i,j}\end{cases}\tag{7}$$

其中，$\boldsymbol{E}_{i,j-1}$，$\boldsymbol{E}_{i-1,j}$，$\boldsymbol{E}_{i,j+1}$，$\boldsymbol{E}_{i+1,j}$，$\boldsymbol{E}_{i-1,j-1}$，$\boldsymbol{E}_{i-1,j+1}$，$\boldsymbol{E}_{i+1,j-1}$和$\boldsymbol{E}_{i+1,j+1}$都是$\boldsymbol{B}^{(l)}$内的周边密文，并且计算出来的差值也都是密文，即 6×6 的矩阵。

当计算了所有密文块内的差值后收集所有差值，生成差值序列$(\boldsymbol{D}_{u_1,v_1},\boldsymbol{D}_{u_2,v_2},\cdots,\boldsymbol{D}_{u_s,v_s})$，其中，$s=(8UV)/9$。嵌入方可以用公开矩阵$\boldsymbol{T}$计算任意两差值$\boldsymbol{D}_{u_1,v_1}$与$\boldsymbol{D}_{u_2,v_2}$之间的 t 值：

$$t=\Gamma\left(\boldsymbol{D}_{u_1,v_1},\boldsymbol{D}_{u_2,v_2}\right)=\det\left(\boldsymbol{D}_{u_1,v_1}-\boldsymbol{T}\cdot\boldsymbol{D}_{u_2,v_2}\right)\tag{8}$$

式中：det(·)为计算方阵行列式的函数；$\Gamma(\cdot,\cdot)$是同态密文比较函数。

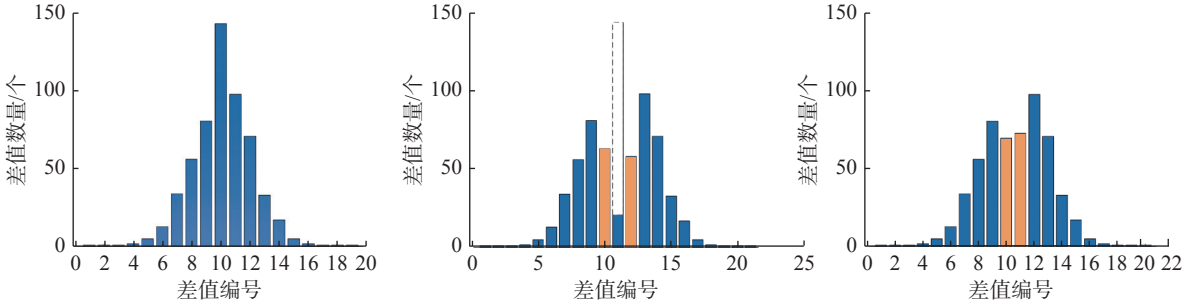
根据同态加密算法[9]的同态密文比较性质，t值的符号与$\mathfrak{D}\left(\boldsymbol{D}_{u_1,v_1}\right)-\mathfrak{D}\left(\boldsymbol{D}_{u_2,v_2}\right)$的符号始终保持一致：

$$\begin{cases}\mathfrak{D}\left(\boldsymbol{D}_{u_1,v_1}\right)>\mathfrak{D}\left(\boldsymbol{D}_{u_2,v_2}\right), & t>0\\ \mathfrak{D}\left(\boldsymbol{D}_{u_1,v_1}\right)=\mathfrak{D}\left(\boldsymbol{D}_{u_2,v_2}\right), & t=0\\ \mathfrak{D}\left(\boldsymbol{D}_{u_1,v_1}\right)<\mathfrak{D}\left(\boldsymbol{D}_{u_2,v_2}\right), & t<0\end{cases}\tag{9}$$

式中，$\mathfrak{D}(\cdot)$为解密函数，将在下文进行介绍。

同态密文比较性质的证明详见文献 [9]。由此可见，嵌入方可以利用同态密文比较性质在未解密任何差值的情况下得知任意两差值之间的大小关系。因此，嵌入方可以对差值序列$(\boldsymbol{D}_{u_1,v_1},\boldsymbol{D}_{u_2,v_2},\cdots,\boldsymbol{D}_{u_s,v_s})$进行由小到大的排序，生成排序后的差值序列$(\widehat{\boldsymbol{D}}_{u_1,v_1},\widehat{\boldsymbol{D}}_{u_2,v_2},\cdots,\widehat{\boldsymbol{D}}_{u_s,v_s})$。

为了生成差值直方图，嵌入方对$(\widehat{\boldsymbol{D}}_{u_1,v_1},\widehat{\boldsymbol{D}}_{u_2,v_2},\cdots,\widehat{\boldsymbol{D}}_{u_s,v_s})$中的每个差值进行编号。第一个差值的编号$f(\widehat{\boldsymbol{D}}_{u_1,v_1})=1$，而后续的每个差值$\widehat{\boldsymbol{D}}_{u_z,v_z}$$(2\leqslant z\leqslant s)$都需要与前一个差值$\widehat{\boldsymbol{D}}_{u_{z-1},v_{z-1}}$进行同态密文比较。若$\Gamma(\widehat{\boldsymbol{D}}_{u_z,v_z},\widehat{\boldsymbol{D}}_{u_{z-1},v_{z-1}})=0$，该差值的编号$f(\widehat{\boldsymbol{D}}_{u_z,v_z})=f(\widehat{\boldsymbol{D}}_{u_{z-1},v_{z-1}})$，否则$f(\widehat{\boldsymbol{D}}_{u_z,v_z})=f(\widehat{\boldsymbol{D}}_{u_{z-1},v_{z-1}})+1$。此时，嵌入方对所有差值的编号进行统计，生成差值直方图，如图 4(a) 所示。从图 4(a) 中可知，生成的差值直方图会在某一差值编号出现峰值，而下文将利用此峰值向密文图像中嵌入信息。



(a) 信息嵌入前的差值直方图 (b) 信息嵌入后差值直方图 ($N_b<N_d$) (c) 信息嵌入后差值直方图 ($N_b=N_d$)

图 4 一轮信息嵌入前后的差值直方图

Fig.4 Difference histograms before and after a round of data embedding

假设所有差值的编号中数量最多的编号为$f\left(\widehat{\boldsymbol{D}}_{u_{\tilde{z}},v_{\tilde{z}}}\right)$，$\tilde{z}\in[1,s]$。嵌入方以光栅的顺序扫描密文图像$\boldsymbol{E}$中每个密文块$\boldsymbol{B}^{(l)}$内的每个差值$\boldsymbol{D}_{u,v}$，并执行以下操作来平移差值直方图，从而嵌入信息：

$$\widehat{\boldsymbol{E}}_{u,v}=\begin{cases}\boldsymbol{E}_{u,v}-\boldsymbol{\sigma}, & f(\boldsymbol{D}_{u,v})<f(\widehat{\boldsymbol{D}}_{u_{\tilde{z}},v_{\tilde{z}}})\\ \boldsymbol{E}_{u,v}+\xi(b)\cdot\boldsymbol{\sigma}, & f(\boldsymbol{D}_{u,v})=f(\widehat{\boldsymbol{D}}_{u_{\tilde{z}},v_{\tilde{z}}})\\ \boldsymbol{E}_{u,v}+\boldsymbol{\sigma}, & f(\boldsymbol{D}_{u,v})>f(\widehat{\boldsymbol{D}}_{u_{\tilde{z}},v_{z}})\end{cases}\tag{10}$$

$$\xi(b)=\begin{cases}-1, & b=0\\ 1, & b=1\end{cases}\tag{11}$$

式 (10) 中：$f(\cdot)$为差值到编号的映射函数；$\xi(\cdot)$为符号函数；b为嵌入的二进制信息；$\widehat{\boldsymbol{E}}_{u,v}$为由$\boldsymbol{E}_{u,v}$更新后的密文，用来替换$\boldsymbol{E}_{u,v}$。

最后，用更新后的密文替换密文图像 $\boldsymbol{E}$ 中相应的密文，生成含有嵌入信息的密文图像 $\boldsymbol{E}^{(1)}$，而信息提取密钥$\boldsymbol{K}_{\mathrm{a}}^{(1)}=\widehat{\boldsymbol{D}}_{u_{\tilde{z}},v_{\tilde{z}}}$。若编号为$f\left(\widehat{\boldsymbol{D}}_{u_{\tilde{z}},v_{\tilde{z}}}\right)$的差值数量为$N_{\mathrm{d}}$，上述一轮的信息嵌入最多能向密文图像 $\boldsymbol{E}$ 中嵌入N_{d}个比特的信息。

假设需要嵌入信息的 bit 数为N_{b}。若$N_{\mathrm{b}}\leqslant N_{\mathrm{d}}$，嵌入方只需要执行一轮信息嵌入就能将所有信息嵌入在密文图像 $\boldsymbol{E}$ 中。图 4 显示了一轮信息嵌入前后差值直方图的变化。从图 4(a)到(b)的变化可知，当$N_{\mathrm{b}}<N_{\mathrm{d}}$时，信息嵌入后的差值直方图中新生成了两个柱体(图 4(b)中橙色柱体)，差值编号的总数量增加了 2 个。图 4(a)中为峰值的差值编号在图 4(b)中增大了 1 个单位且仍有剩余差值数量。从图 4(a)到(c)的变化可知，当$N_{\mathrm{b}}=N_{\mathrm{d}}$时，信息嵌入后的差值直方图中同样新生成了两个柱体(图 4(c)中橙色柱体)，但差值编号的总数量只增加了 1 个。因为图 4(a)中为峰值的差值编号全部被用于信息的嵌入，剩余的差值数量为 0。若$N_{\mathrm{b}}>N_{\mathrm{d}}$，嵌入方先执行一轮信息嵌入，向 $\boldsymbol{E}$ 中嵌入N_{d}个 bit 的信息，再对 $\boldsymbol{E}^{(1)}$ 执行新一轮的信息嵌入。对 $\boldsymbol{E}^{(1)}$ 执行一轮信息嵌入同样包括上述的 5 个步骤，即分割密文块、计算差值、排序和编号差值、生成差值直方图、平移差值直方图。对 $\boldsymbol{E}^{(1)}$ 执行完一轮信息嵌入后，若仍有剩余的信息未被嵌入，嵌入方继续对新生成的含有嵌入信息的密文图像 $\boldsymbol{E}^{(2)}$ 进行新一轮的信息嵌入。如此反复，直到完成所有信息的嵌入，生成最终的含有嵌入信息的密文图像$\boldsymbol{E}^{(\tau)}$，并收集每一轮信息嵌入生成的信息提取密钥$\boldsymbol{K}_{\mathrm{a}}=\{\boldsymbol{K}_{\mathrm{a}}^{(1)},\boldsymbol{K}_{\mathrm{a}}^{(2)},\cdots,\boldsymbol{K}_{\mathrm{a}}^{(\tau)}\}$，其中，$\tau$是信息嵌入的轮数。最后，嵌入方将含有嵌入信息的密文图像$\boldsymbol{E}^{(\tau)}$发送给接收方。

1.3　信息提取和图像恢复

仅拥有加密密钥$\boldsymbol{K}_{\mathrm{e}}=\{K_{\mathrm{e}}^{(1)},K_{\mathrm{e}}^{(2)}\}$的接收方在接收到含嵌入信息的密文图像$\boldsymbol{E}^{(\tau)}$后，可通过对$\boldsymbol{E}^{(\tau)}$解密来获知图像的内容。首先，用$K_{\mathrm{e}}^{(1)}$和$K_{\mathrm{e}}^{(2)}$分别生成矩阵$\boldsymbol{H}$和$\boldsymbol{R}$；然后，用$\boldsymbol{H}$和$\boldsymbol{R}$对$\boldsymbol{E}^{(\tau)}$中每个密文$\boldsymbol{E}_{i,j}^{(\tau)}$进行解密，如式 (12) 所示；最后，收集所有密文的解密结果，生成含有嵌入信息的解密图像$\boldsymbol{I}^{(\tau)}$。

$$\boldsymbol{I}_{i,j}^{(\tau)}=\mathfrak{D}\left(\boldsymbol{E}_{i,j}^{(\tau)}-\boldsymbol{R}\right)=\left[\boldsymbol{H}^{-1}\cdot\left(\boldsymbol{E}_{i,j}^{(\tau)}-\boldsymbol{R}\right)\cdot\boldsymbol{H}\right]_{1,1}+\left[\boldsymbol{H}^{-1}\cdot\left(\boldsymbol{E}_{i,j}^{(\tau)}-\boldsymbol{R}\right)\cdot\boldsymbol{H}\right]_{1,2}\tag{12}$$

式中：$\mathfrak{D}(\cdot)$是解密函数；$[\cdot]_{1,1}$和$[\cdot]_{1,2}$分别表示矩阵中(1,1)和(1,2)位置上的元素；$\boldsymbol{I}_{i,j}^{(\tau)}$是$\boldsymbol{E}_{i,j}^{(\tau)}$解密后的像素值。由于信息的嵌入，相比于原始医学图像$\boldsymbol{I}$，含有嵌入信息的解密图像$\boldsymbol{I}^{(\tau)}$中相邻像素之间灰度差异更大，视觉上$\boldsymbol{I}^{(\tau)}$的对比度更强。

仅拥有信息提取密钥$\boldsymbol{K}_{\mathrm{a}}=\{\boldsymbol{K}_{\mathrm{a}}^{(1)},\boldsymbol{K}_{\mathrm{a}}^{(2)},\cdots,\boldsymbol{K}_{\mathrm{a}}^{(\tau)}\}$的接收方接收到含嵌入信息的密文图像$\boldsymbol{E}^{(\tau)}$后，可以从$\boldsymbol{E}^{(\tau)}$中提取出所有嵌入的信息。接收方从提取密钥中元素的个数可以得知信息嵌入的轮数为τ。为了提取所有嵌入的信息，接收方同样需要τ轮信息提取。每轮信息提取都包括分割密文块、计算差值、提取信息、恢复差值直方图等 4 个步骤。分割密文块和计算差值的两个步骤与前文一致。在执行第 1 轮信息提取的过程中，接收方以光栅顺序扫描$\boldsymbol{E}^{(\tau)}$中每个密文块内的每个差值$\boldsymbol{D}_{u,v}$，并用信息提取密钥$\boldsymbol{K}_{\mathrm{a}}^{(\tau)}$执行以下操作来提取信息：

$$b'=\begin{cases}0, & t_1=0\\ 1, & t_2=0\\ \mathrm{null}, & \text{其他}\end{cases}\tag{13}$$

同时，执行以下操作来恢复差值直方图：

$$\widehat{\boldsymbol{E}}_{u,v}^{(\tau)}=\begin{cases}\boldsymbol{E}_{u,v}^{(\tau)}+\boldsymbol{\sigma}, & t_1\leqslant 0\\ \boldsymbol{E}_{u,v}^{(\tau)}-\boldsymbol{\sigma}, & t_2\geqslant 0\\ \boldsymbol{E}_{u,v}^{(\tau)}, & \text{其他}\end{cases}\tag{14}$$

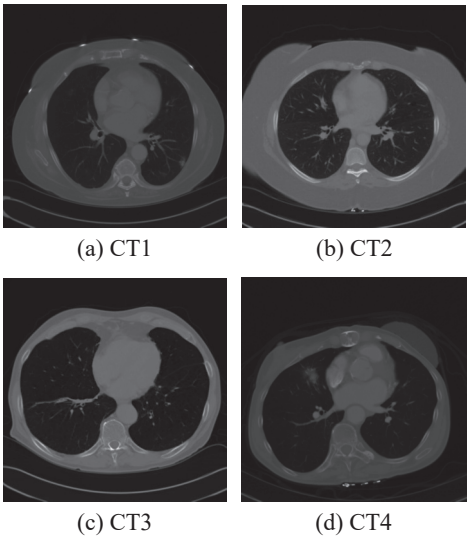
式中：$t_1=\Gamma(\boldsymbol{D}_{u,v},\boldsymbol{K}_{\mathrm{a}}^{(\tau)}-\boldsymbol{\sigma})$；$t_2=\Gamma(\boldsymbol{D}_{u,v},\boldsymbol{K}_{\mathrm{a}}^{(\tau)}+\boldsymbol{\sigma})$；$b'$为提取的二进制信息；$\widehat{\boldsymbol{E}}_{u,v}^{(\tau)}$为由$\boldsymbol{E}_{u,v}^{(\tau)}$更新后的密文，用来替换$\boldsymbol{E}_{u,v}^{(\tau)}$。

最后，用更新后的密文替换密文图像$\boldsymbol{E}^{(\tau)}$中相应的密文，生成信息提取后的密文图像$\boldsymbol{E}^{(\tau-1)}$。若$\tau>1$，接收方用$\boldsymbol{K}_{\mathrm{a}}^{(\tau-1)}$继续对$\boldsymbol{E}^{(\tau-1)}$执行新一轮的信息提取，直到用完所有信息提取密钥。在执行完τ轮信息提取后，接收方可以准确地提取出所有嵌入的信息，并得到不含嵌入信息的密文图像$\boldsymbol{E}^{(0)}$。

拥有信息提取密钥$\boldsymbol{K}_{\mathrm{a}}$和加密密钥$\boldsymbol{K}_{\mathrm{e}}$的接收方在接收到含嵌入信息的密文图像$\boldsymbol{E}^{(\tau)}$后，先用$\boldsymbol{K}_{\mathrm{a}}$对$\boldsymbol{E}^{(\tau)}$执行$\tau$轮信息提取，得到提取的信息和不含嵌入信息的密文图像$\boldsymbol{E}^{(0)}$；再用$\boldsymbol{K}_{\mathrm{e}}$分别生成矩阵$\boldsymbol{H}$和$\boldsymbol{R}$，并用矩阵$\boldsymbol{H}$和$\boldsymbol{R}$根据式 (12) 对$\boldsymbol{E}^{(0)}$进行解密，得到与原始医学图像$\boldsymbol{I}$完全相同的恢复图像$\boldsymbol{I}^{(0)}$。

2 实验结果与分析

本文实验环境为2.60GHz Intel i7处理器、8.00 GB内存、Windows 10操作系统，算法应用Matlab R2018b进行实现。实验选取DICOM(digital imaging and communications in medicine)图像库[10]中4张典型的512×512 CT(computed tomography)图像，如图5所示。以下从安全性、嵌入率、对比度增强效果3个方面对实验结果进行分析。



(a) CT1 (b) CT2

(c) CT3 (d) CT4

图5 DICOM图像库[10]中的4张CT图像

Fig.5 Four CT images in DICOM image library[10]

2.1 安全性分析

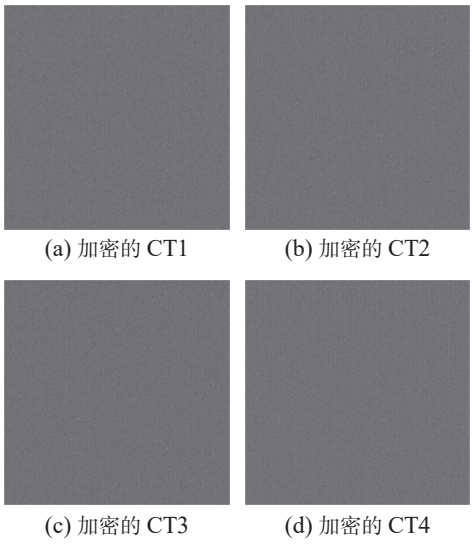
图6给出了图5中4张原始图像加密后的图像。从图6中可以看出，无法从加密后的图像中获取原始图像内容。

2.1.1 密文图像相关性分析

相关性分析是分析图像中相邻像素之间的相关性程度。一个安全性高的图像加密算法应该尽可能地破坏原始图像中相邻像素之间的相关性。表1给出了图5中4张CT图像加密前后图像在水平、垂直、对角线和反对角线4个方向上的平均相关性系数。从表1中可以看出，加密前图像的平均相关性系数都接近于1，表明原始图像中相邻像素之间存在较强的正相关性。加密后图像的平均相关性系数接近于0，表明密文图像中相邻像素之间的相关性弱，证明了本文算法具有较高的安全性。

2.1.2 密文图像差分分析

差分分析是一种密码学领域常用的选择性明文攻击。该攻击将原始图像中的任意一个像素的值改变一个单位，使用相同的加密密钥分别对篡改前后的图像进行加密，通过分析篡改前后密文图像的变化来破译加密密钥。因此，抵抗这种攻击的能力取决于篡改前后密文图像中变化的随机性。像素数变化率NPCR(number of pixels changing rate)[11]和统一平均变化强度UACI(uniform average change intensity)[12]被用来分析篡改前后密文图像的变化。NPCR和UACI分别表示篡改前后密文图像之间的变化像素数和平均变化强度数，它们相应的理论值分别为99.6094%和33.4635%。表2给出了图5中4张CT图像篡改前后密文图像之间的NPCR和UACI。从表2可以看出，4张图像的NPCR和UACI都接近相应的理论值99.6094%和33.4635%，证明本文算法对差分分析具有较强的抵抗能力。



(a) 加密的CT1 (b) 加密的CT2

(c) 加密的CT3 (d) 加密的CT4

图6 4张加密的CT图像

Fig. 6 Four encrypted CT images

表1 加密前后图像的平均相关性系数

Tab.1 Average correlation coefficients of the images before and after the encryption

图像	加密前的平均相关性系数	加密后的平均相关性系数
CT1	0.9869	−0.0373
CT2	0.9894	−0.0260
CT3	0.9860	−0.0351
CT4	0.9905	−0.0299

2.2 嵌入率和解密图像对比度分析

嵌入率是指嵌入信息量与图像像素总数的比值，表示图像中每个像素被嵌入的平均信息量，单位为bpp(bits per pixel)。嵌入率越大，图像可嵌入的比特数量越大。图像对比度IC(image contrast)是指图像中相邻像素灰度差异大小。差异越大，视觉上明暗对比越明显。图像对比度可以通过式(15)来计算。

表 2　加密图像的 NPCR 和 UACI 指标

Tab.2　NPCR and UACI of the encrypted images

图像	NPCR/%	UACI/%
CT1	99.9871	33.5523
CT2	99.9869	33.5106
CT3	99.9867	33.5713
CT4	99.9866	33.5606

$$Q_{\mathrm{IC}}=\frac{1}{\|\boldsymbol{\varepsilon}\|}\sum_{\langle p,q\rangle\in\boldsymbol{\varepsilon}}(w(p)-w(q))^2 \qquad (15)$$

式中：$\boldsymbol{\varepsilon}$为由图像中所有一阶相邻像素对组成的集合；$\langle p,q\rangle$为集合$\boldsymbol{\varepsilon}$中一个相邻像素对；$\|\cdot\|$为集合中元素的总数量；$w(\cdot)$为像素到灰度值的映射函数。由此可见，图像中相邻像素之间的灰度差异越大，计算得到的 IC 越大。

图 7 给出了图 5 中 4 张 CT 图像在不同嵌入轮数n下，嵌入率和含有嵌入信息的解密图像对比度 IC。由图 7 可知，信息嵌入的轮数越多，嵌入率越大，图像可以被嵌入的信息量越多，含有嵌入信息的解密图像的对比度也越大。图 8 显示了图 5 中的 4 张 CT 图像 20 轮信息嵌入后含有嵌入信息的解密图像。从图 8 可以发现，相比于图 5 中的原始图像，含有嵌入信息的解密图像在对比度上有明显的增强效果。因此，本文算法能改善解密医学图像的视觉质量。

2.3　丢包现象对算法有效性的影响

在复杂网络环境下，数据有可能存在丢包现象。因此，含有嵌入信息的密文图像在传输过程中可能丢失部分密文。在实验过程中，利用本文算法仅执行 1 轮信息嵌入，在图 6 的 4 张加密 CT 图像中分别嵌入尽可能多的信息，生成 4 张含有嵌入信息的密文图像。图 9 给出了含有嵌入信息的密文在密文图像中的位置。图 9 中，红色标记出了含有嵌入信息的密文在密文图像中的位置，黄色标记出了含有嵌入信息密文块的中心在密文图像中的位置，绿色标记出了不包含嵌入信息的密文在密文图像中的位置。

若丢失了密文图像中含有嵌入信息的密文，该密文所含的嵌入信息将丢失；若丢失了密文图像中含有嵌入信息的密文块的中心密文，该密文块内所含的所有嵌入信息都将丢失；若丢失了密文图像中不包含嵌入信息的密文，则不会影响本

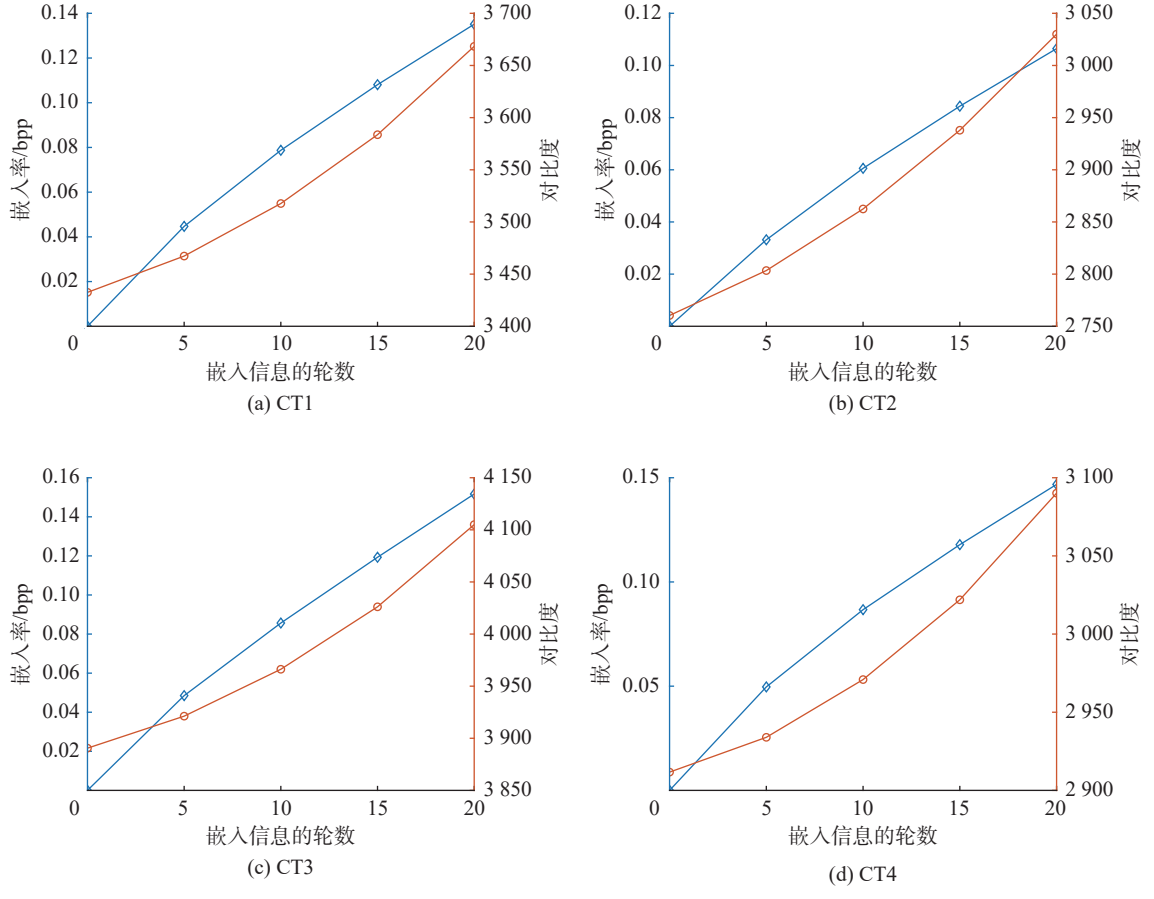
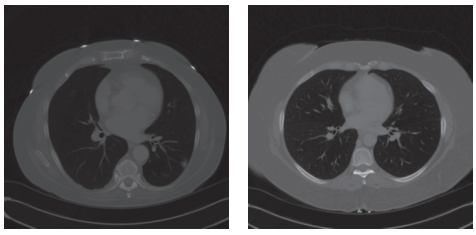


图 7　不同嵌入轮数下各 CT 图像的嵌入率和解密图像对比度

Fig.7　Embedding rate and decrypted image contrast of each CT image under different embedding rounds

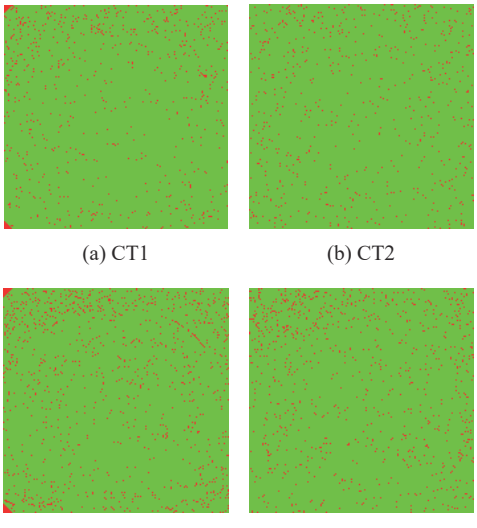


(a) CT1 (b) CT2

(c) CT3 (d) CT4

图 8 各 CT 图像在 20 轮信息嵌入后解密所得的对比度增强图像

Fig. 8 Contra-enhanced image of each CT image after 20 rounds of data embedding and decryption



(a) CT1 (b) CT2

(c) CT3 (d) CT4

图 9 嵌入信息在各 CT 图像密文图像中的位置

Fig. 9 Position of the embedded data in ciphertext image of each CT image

文算法的有效性。图 9 中，4 张图像中绿色像素的占比分别为 95.23%，95.98%，93.10%，94.51%。因此，当丢包率为 0.01% 时，发生嵌入信息丢失的概率分别为 71.97%，65.60%，84.43%，76.95%。综上所述，含有嵌入信息的密文图像在传输过程中丢失部分密文很大概率会导致相应嵌入信息的丢失。

3 结 论

提出了一种基于差值直方图平移的医学图像可逆信息隐藏算法。在该算法中，通过同态加密算法对医学图像的每个像素进行加密来保护医学图像的隐私内容，通过多轮差值直方图平移可以在密文图像中嵌入更多信息。由于信息的嵌入，解密图像中相邻像素之间的灰度差异增大，可有效增强图像的对比度，提升图像视觉质量，并且嵌入的信息越多，解密图像的对比度增强效果越显著。此外，根据信息提取密钥和加密密钥，本算法可以完全恢复原始图像。

参考文献：

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

[2] 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.

[3] QIU Y Q, QIAN Z X, ZENG H Q, et al. Reversible data hiding in encrypted images using adaptive reversible integer transformation[J]. Signal Processing, 2020, 167: 107288.

[4] YU M J, YAO H, QIN C. Reversible data hiding in encrypted images without additional information transmission[J]. Signal Processing：Image Communication, 2022, 105: 116696.

[5] BHARDWAJ R, AGGARWAL A. Hiding clinical information in medical images: an encrypted dual-image reversible data hiding algorithm with base-3 numeral framework[J]. Optik, 2019, 181: 1099–1112.

[6] KONG P, FU D, LI X R, et al. Reversible data hiding in encrypted medical DICOM image[J]. Multimedia Systems, 2021, 27(3): 303–315.

[7] DZWONKOWSKI M, RYKACZEWSKI R. Reversible data hiding in encrypted DICOM images using cyclic binary golay (23, 12) Code[J]. IEEE Access, 2021, 9: 60503–60515.

[8] 付笛, 孔平, 周亮, 等. 一种密文域医学图像可逆信息隐藏算法 [J]. 上海理工大学学报, 2022, 44(3): 262–268.

[9] LI J, KUANG X H, LIN S J, et al. Privacy preservation for machine learning training and classification based on homomorphic encryption schemes[J]. Information Sciences, 2020, 526: 166–179.

[10] GOLDGOF D, HALL L, HAWKINS S, et al. QIN LUNG CT[DB/OL]. [2021-01-15]. https://doi.org/10.7937/K9/TCIA.2015.NPGZYZBZ.

[11] CHEN G R, MAO Y B, CHUI C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons & Fractals, 2004, 21(3): 749–761.

[12] MAO Y B, CHEN G R, LIAN S G. A novel fast image encryption scheme based on 3D chaotic baker maps[J]. International Journal of Bifurcation and Chaos, 2004, 14(10): 3613–3624.

（编辑：丁红艺）