基于张量积压缩感知的高效安全的影像传输

王成宇[1],陈自刚[2],李书芳[1],王怡宁[3]

(1.北京邮电大学信息与通信工程学院,先进信息网络北京实验室,网络体系构建与融合北京市重点实验室,北京 100876;
2.重庆邮电大学信息与通信工程学院,重庆 400065;
3.中国医学科学院北京协和医院放射科,疑难重症及罕见病国家重点实验室,北京 100730)

摘要:为解决海量医疗数据存储占用巨大空间以及传输安全,提出了基于压缩感知技术的医疗影像安全传输系统。将医学图像以较低的压缩率压缩可以达到加快数据传输、节省存储空间的效果。通过新的方式生成Chaotic测量矩阵可以降低生成矩阵所需时间、节省矩阵的存储空间并扩大加密系统的密钥空间。使用Logistic-chaotic系统以及Chen-chaotic系统对医学图像进行双重加密,保证其在传输过程中的安全性。实验结果显示提出的系统具备高效性、安全性以及节省空间的性能,同时密钥空间可以达到10^{200}。

关键词:压缩感知;P张量积;医学影像传输;混沌系统

中图分类号:O422 **文献标识码:**A **文章编号:**1673-4793(2021)02-0068-07

Efficient and secure transmission system based on tensor product compressed sensing

WANG Chengyu[1], CHEN Zigang[2], LI Shufang[1], WANG Yining[3]

(1.School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China; 2. School of Information and Communication Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065; 3. Department of Radiology, Peking Union Medical College Hospital, Peking Union Medical College, Chinese Academy of Medical Sciences, Beijing 100730, China)

Abstract: A medical image security transmission system based on compressed sensing (CS) is proposed to reduce storage space and ensure security of medical data. Compress medical images in a small ratio to transmit faster and reduce storage space. Generating the chaotic measurement matrix in a new way takes shorter time, saves the storage space of measurement matrix and expands the key space of the encryption system. Encrypting medical images by Logistic-chaotic system and Chen-chaotic system can prevent privacy leakage when transmitted on internet. The experimental results show that the proposed system has the performance of high efficiency, security and space saving, and the key space can be 10^{200}.

Key words: compressed sensing; P-tensor product; medical image transmission; chaotic systems

---

基金项目:中华国际医学交流基金会2019 SKY影像科研基金项目(编号:Z-2014-07-1912-01)

作者简介:王成宇(1996—),男,北京邮电大学硕士研究生;李书芳(1963-),女,北京邮电大学教授,博士生导师,E-mail:lisf@bupt.edu.cn;王怡宁,女,北京协和医院放射科主任教授、博士研究生导师,E-mail:yiningpumc@163.com;陈自刚,男,重庆邮电大学副教授,E-mail:chenzg@cupt.edu.cn.

1　引言

随着网络带宽的增大，医学影像通过互联网进行传输的需求增大，同时面临保证数据传输的安全性以及完整性的挑战。压缩感知技术是一种兼具压缩与加密特性的技术，与云存储以及大数据计算平台已成为医院网络架构场景中的热点话题[1]。

解决医学图像的存储空间占用问题以及传输安全面对挑战。首先，图像的信息安全应该得到保障。为满足卫星图像传输安全，提出基于替换图像像素并通过密码学改变图像像素分布的方案[2]。通过共享秘密图像以及密钥保护的方案，能够达到隐藏彩色图像信息的效果[3]。基于SSH协议与密钥加密技术开发出医学图像传输的应用软件[4]。

图像的传输速度也是一个值得关注的话题。基于压缩感知技术提出一种端到端的图像压缩系统，融合了图像重建、量化以及熵编码等技术，加快医疗系统中的图像传输速度[5]。通过允许快速访问大量医学图像数据的框架，通过在线网页客户端进行图像展示实现数据的实时交互[6]。

海量的医学图像的存储占用巨大的空间，解决空间占用问题具有一定的挑战。提出区块链的医疗数据管理以及云上存储的模式[7]，为解决海量医学图像的存储提供了新的思路。通过私有云对图像进行加密以及解密，公有云对图像进行存储的模式[8]，不仅可以解决图像的存储问题还可以为图像信息安全提供保障。基于云存储提出一种可扩展传输速度更快的系统，可以实现图像的存储以及检索等操作[9]。

然而，大多数上述的工作仅致力于解决当前面临的三个问题中的一个或者两个。我们提出基于压缩感知技术、混沌系统以及云上存储的方式实现医学影像的传输系统。此系统可以加快云端图像的上传以及下载速度，同时由混沌系统实现的双重加密可以保障云端数据的安全性。基于新型的张量积压缩感知模型，使用张量积的方式生成高维矩阵，同时采用迭代加权最小二乘（Iterative weighted least squares，IRLS）算法对图像进行还原重建能够保证对压缩图像的高精度重建。为确保图像信息的安全性，使用双重 Chen-chaotic 系统分别对压缩图像进行空间置乱以及像素值加密，具备密钥空间大、密钥高敏感度的特点，能够保障信息安全性。

2　相关工作

2.1　传统感知模型

传统压缩感知模型基于欠定性方程的一种特殊情况

$$\boldsymbol{y} = \boldsymbol{\Phi x} \tag{1}$$

等式(1)表示原始信号 $x \in R^n$ 经过非线性采样压缩为 $y \in R^m$ 且 $m < n$。通常情况下，信号 x 需要是一个稀疏信号或者在某个域稀疏

$$\boldsymbol{x} = \boldsymbol{\Psi s} \tag{2}$$

其中 Ψ 为正交稀疏基，$\Psi \in R^{m \times n}$，最常用的正交稀疏基为离散小波变换(Discrete Wavelet Transform, DWT)基与离散余弦变换(Discrete Cosine Transform, DCT)基。由等式(1)与(2)可以得到压缩感知模型的最终模型表达式

$$\boldsymbol{y} = \boldsymbol{\Phi x} = \boldsymbol{\Phi \Psi s} = \boldsymbol{\theta s} \tag{3}$$

有限等距原则(Restricted Isometry Property, RIP)能够保证信号的重建能够保证唯一且准确[10]。Spark 常数可以衡量测量矩阵内的列的线性相关性，保证信号的采样能够准确唯一的还原。Coherence 常数衡量 θ 内向量的最大内积，反映两个列向量的相似性。基于以上三个性质，能够保证信号能够唯一且准确的还原重建。

2.2　分块压缩感知模型

分块压缩感知模型，基于将原始图像分成大小相同的子图像的思想达到降低计算复杂度的效果[11]

$$\boldsymbol{Y}_i = \boldsymbol{\Phi}_B \boldsymbol{X}_i \tag{4}$$

其中 X_i 表示子图像块，设原始图像大小为 $q \times s$，被分为 N 个子图像快，由于每一块子图像使用相同的测量矩阵进行采样，因此可以达到降低测量矩阵存储空间的效果。分块压缩感知模型框架为

$$\boldsymbol{Y} = \boldsymbol{\Phi}_{BCS} \boldsymbol{X} \tag{5}$$

对于原始图像测量矩阵可以表示为

$$\boldsymbol{\Phi}_{BCS} = \begin{pmatrix} \boldsymbol{\Phi}_B & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{\Phi}_B & \cdots & \boldsymbol{0} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{0} & \boldsymbol{0} & \cdots & \boldsymbol{\Phi}_B \end{pmatrix} \tag{6}$$

分块压缩感知模型的提出能够在图像未完全呈现时就可以将图像进行压缩，适用于卫星图像以及遥感图像领域的应用。

3　提出的医学影像传输系统

提出的医学影像传输系统由三部分组成，包括负

责图像压缩的压缩感知模块、图像加密模块以及图像解密重建模块。

3.1 张量积压缩感知模型

传统的压缩感知模型[12,13]中,测量矩阵必须与图像矩阵的维度匹配才可以进行矩阵的乘法运算。张量积压缩感知模型中,设图像矩阵表示为 $X \in R^{q\times q}$,离散小波变换(a discrete wavelet transform,DWT)基是一个正交稀疏基表示为 $\Psi \in R^{q\times q}$,则图像矩阵的稀疏域转换过程表示为

$$\boldsymbol{X} = \boldsymbol{\Psi S} \tag{7}$$

其中,$S \in R^{q\times q}$表示 X的稀疏域。

提出的压缩感知技术的关键不同在于构造测量矩阵的方式。提出的压缩感知的框架可以表示为:

$$Y = \boldsymbol{\Phi} \underset{\ltimes}{^{P}} \boldsymbol{X} \tag{8}$$

其中$\underset{\ltimes}{^{P}}$表示P张量积。于是有

$$Y = \boldsymbol{\Phi} \underset{\ltimes}{^{P}} \boldsymbol{X} = (\boldsymbol{\Phi} \otimes P)\boldsymbol{X} = (\boldsymbol{\Phi} \otimes P)\boldsymbol{\Psi S} \tag{9}$$

其中 $\otimes$ 表示 Kronecker product。设有矩阵 $\Phi \in R^{m\times n}, P \in R^{t\times t}, m < n$且t = q/n。将 $\boldsymbol{\Phi}$写为向量的形式为 $\Phi = \left[\varphi_1,\cdots,\varphi_n\right]$,则矩阵的P张量积可以表示为

$$\boldsymbol{\Phi} \otimes \boldsymbol{P} = (\varphi_1 P,\cdots,\varphi_n \boldsymbol{P}) = \begin{pmatrix} \varphi_{11}P & \cdots & \varphi_{1n}P \\ \vdots & \ddots & \vdots \\ \varphi_{m1}P & \cdots & \varphi_{mn}P \end{pmatrix} \tag{10}$$

于是,$(\boldsymbol{\Phi} \otimes P) \in R^{(m\times t)\times(n\times t)}$并且 $Y \in R^{(\frac{mq}{n})\times q}$,我们称$\frac{m}{n}$为压缩率,将q/$n$称为矩阵的放大系数。

在P张量积压缩感知中,矩阵 $\boldsymbol{\Phi}$是一个随机矩阵,例如Gaussian矩阵、Bernoulli矩阵、Chaotic矩阵。而矩阵P可以是一个单位矩阵也可以是一个随机矩阵。在本实验中矩阵 $\boldsymbol{\Phi}$与矩阵P都使用Chaotic矩阵。

3.2 加密算法

在加密模块中,矩阵 $\boldsymbol{\Phi}$是由第一个Logistic-chaotic系统生成,系统参数为$\left(\boldsymbol{\Phi}_{\mu},\boldsymbol{\Phi}_{x0},\boldsymbol{\Phi}_{d}\right)$,矩阵P由另一个Logistic-chaotic系统生成,系统参数为$\left(P_{\mu},P_{x0},P_{d}\right)$。Logistic-chaotic系统中的控制参数 $\mu\in(3.569\,946,4)$,初始值 $x0\in(0,1)$,采样距离 $d\in(15,+\infty)$。两个系统的系统参数是我们加密系统中的密钥的一部分。基于共享密钥的加密方式与压缩感知的方式结合可以提供具备安全性与鲁棒性的加密算法。

图像矩阵 $X \in R^{q\times q}$经过压缩采样后得到观测矩阵 $Y \in R^{(\frac{mq}{n})\times q}$。将压缩后的图像矩阵进行量化处理,将矩阵Y中的元素的数值值域转换至$\left[0,2^{\alpha}-1\right]$,可以表示为

$$\boldsymbol{N} = \frac{(\boldsymbol{2^{\alpha}-1})(\boldsymbol{Y}-\boldsymbol{Y}_{\min})}{\boldsymbol{Y}_{\max}-\boldsymbol{Y}_{\min}} \tag{11}$$

其中,α为正整数,$Y_{\max}$为矩阵Y中的最大元素的值,$Y_{\min}$为矩阵中的最小值。

对于量化后的图像矩阵使用Chen-chaotic系统进行双重加密,系统中的参数为$\left(C_X^i,C_Y^i,C_Z^i,C_H^i,C_d^i\right)$,$i$ = 1,2。其中 C_d^i为采样距离,其它参数为系统的初始值并且取值范围都为(0,1)。使用 $A_i \in R^{\frac{mq^2}{n}\times 4}$表示Chen-chaotic系统生成的混沌矩阵,

$$\boldsymbol{S}_i = \frac{\boldsymbol{A}_i(:,\boldsymbol{1}) + \boldsymbol{A}_i(:,\boldsymbol{2}) + \boldsymbol{A}_i(:,\boldsymbol{2}) + \boldsymbol{A}_i(:,\boldsymbol{3})}{\boldsymbol{4}} \tag{12}$$

其中 S_i为得到的混沌序列,将第一个Chen-chaotic系统产生的混沌序列使用C表示,对 C_1进行排序后的序列使用$C1_SORT$表示,空间置乱加密算法如下算法1所示:

Algorithm 1 The first step encryption algorithm.

Require:

The normalized matrix $N \in R^{\left(\frac{mq}{n}\right)\times q}$, Chaotic sequences

$C1$ and the sorted sequence $C1\_SORT$;

Initialize N_S=zeros(1,mq^2/n);

Ensure:

The encrypted matrix $N1$;

1: Expand N by line to be a vector represented by N_v

2: for i=1:mq^2/n

3: N_S(i)=N_v($C1$==$C1\_SORT$(i))

4: end for

5: Reshape $N_S$to be a matrix with size of $\frac{mq}{n}\times q$, represent the matrix as $N1$.

6: return $N1$.

算法1 第一步加密算法伪代码描述

将第二个Chen-chaotic系统产生的序列使用 C_2表示,生成过程为

$$\boldsymbol{C}_2 = \boldsymbol{floor}\left[\boldsymbol{S}_2 \times \boldsymbol{10^{15}}\right] \boldsymbol{mod}\ \boldsymbol{2^{\alpha}} \tag{13}$$

将混沌序列C_2转化为维数为$\frac{mq}{n}\times q$的矩阵,表示为$C2_m$。第二次的加密方式为对图像矩阵进行像素值加密,描述为

$$\boldsymbol{N2}_m = \boldsymbol{\beta N}_1 + (\boldsymbol{1}-\boldsymbol{\beta})\,\boldsymbol{C2}_m \tag{14}$$

其中，$\beta \in (0,1), N2_m \in R^{\frac{mq}{n}\times q}$。

描述中，将生成测量矩阵的过程也看作为加密的原因是压缩感知中的图像压缩过程本质上也是改变图像的像素值，而且基于这种方式可以很好的将压缩感知的加密特性进行量化评估。同时基于 Chen-chaotic 混沌系统的加密方式属于无损加密。

3.3　解密与图像的还原重建

图像的解密过程就是加密过程的逆过程，根据得到的正确的密钥构造 Chen-chaotic 序列 C_1 与 C_2，接收到的图像矩阵设为 $N2m\_r \in R^{\frac{mq}{n}\times q}$，则解密过程为

$$N1_d = \frac{N2m\_r - (1-\beta)C2_m}{\beta} \tag{15}$$

则 $N1_d$ 为第二次加密的解密结果。

第一步加密的解密过程实质上为将图像矩阵中的像素值的位置进行还原，即为空间置乱的逆过程，解密算法如算法 2。

加密图片完成解密之后，进行量化过程的逆过程观测矩阵即压缩后的图像矩阵使用 Yr 表示，描述为

$$Yr = \frac{N_d \times (Y_{\max} - Y_{\min})}{2^{\alpha} - 1} + Y_{\min} \tag{16}$$

Algorithm 2 The decryption algorithm of the first encryption.

Require:

The matrix $N1\_d \in R^{\left(\frac{mq}{n}\right)\times q}$, Chaotic sequences $C1$ and

the sorted sequence $C1\_SORT$;

Initialize N_S=zeros(1,mq^2/n);

Ensure:

The encrypted matrix N_S_d;

1：Expand $N1\_d$ by line to be a vector represented by $N1\_dv$.

2：for i=1：mq^2/n

3：　　N_S_d(i)=$N1\_dv$($C1\_SOPT$==$C1(i)$)

4：end for

5：Reshape N_S_d to be a matrix with size of $\frac{mq}{n}\times q$, represent the matrix as N_d.

6：return N_d.

算法 2　第一步加密的解密算法伪代码描述

最后，对观测矩阵进行还原重建得到相对精确的图像矩阵。还原算法为 IRLS 算法，由于矩阵的还原算法为逐列进行还原，因此 IRLS 对每一列的还原过程使用伪代码的形式进行描述，如算法 3

因为原始图像在进行压缩之前进行了稀疏域转换，因此观测矩阵的每一列符合 $x \in \sum_k$ 的稀疏原则，因此图像能够被成功且精确的还原重建。

关于 IRLS 算法中的迭代权重 $\omega_i^{(n)}$ 其中 n 表示迭代的次数，i 表示观测矩阵的第 i 列在进行迭代还原时的权重。IRLS 算法中的迭代权重最初的表达式为 $\omega_i^{(n)} = \left[\left|x_i^{(n)}\right|^2 + \varepsilon_n^2\right]^{-1}$，Daubechies[14] 提出使用 $\omega_i^{(n)} = \left[\left|x_i^{(n)}\right|^2 + \varepsilon_n^2\right]^{-1+\frac{\rho}{2}}$，$0 < \rho < 1$，重建结果更加准确。彭海朋提出使用 l_ρ 范数的迭代权重可以得到比 l_0 范数与 l_1 范数更加准确的重建结果，并且使用 l_ρ 范数可以降低对采样信号数量的要求，$\omega_i^{(n)} = \left[\left|x_i^{(n)}\right|^2 + \varepsilon_n^{1+\rho}\right]^{-1+\frac{\rho}{2}}$，$0 < \rho < 1$，特别地当 $\rho = 0.8$ 时重建效果最好。实验过程中的 IRLS 算法中的迭代权重为 $\omega_i^{(n)} = \left[\left|x_i^{(n)}\right|^2 + \varepsilon_n^{1+\rho}\right]^{-1+\frac{\rho}{2}}$，$\rho = 0.8$。

Algorithm 3 The IRLS in P-tensor product CS signal reconstruction

Require:

The signal x which has been transformed to sparse domain $x \in \sum_k$;

Initialize ε_0=1,$\omega^{(0)}$=(1,⋯,1),$x^{(0)}$=(1,⋯,1);

Ensure:

The reconstruted signal x';

1：Set x as a k-sparse vector, $x \in R^{q\times 1}$ and $y \in R^{\left[\frac{mq}{n}\right]\times 1}$ as the obvervation vector.

2：for every column vector y_i *in* the obvervation matrix y .

3：while $\varepsilon > 10^{-9}$,then we do as following：

4：update $\omega_i^{(n)} \leftarrow \left[(x_i^{(n)})^2 + \varepsilon_n^{1+\rho}\right]^{-1+\frac{\rho}{2}}$.

5：let $Q_n \leftarrow \frac{1}{\omega^{(n)}}$.

6：update $\varepsilon_{n+1} \leftarrow (\Phi \otimes P \cdot Q^T)^T \cdot \left[\Phi \otimes P \cdot (\Phi \otimes P \cdot Q^T)T\right]^{-1} \cdot y$.

7：update $\varepsilon \leftarrow \min(\varepsilon_n, \left[r(x^{(n+1)})_{k+1}\right]/q$

8：end while

9：return $x'=x^{(n+1)}$

10：end for

算法 3　IRLS 算法伪代码描述

4　实验及结果分析

在本章节中，我们对提出的压缩感知模型以及加密

算法进行实验检测。详细对比与其它压缩感知模型下在测量矩阵方面的优势,并且找到与提出的压缩感知模型相匹配的还原重建算法,最后检验加密算法的性能。

4.1 生成测量矩阵的效率以及空间占用对比

由于测量矩阵需要与图像的维数相匹配,当面临压缩感知的图像维数较大时,会造成测量矩阵的空间占用过大的问题。而我们提出的P张量积压缩感知模型与传统的压缩感知模型以及分块压缩感知模型(Block Compressing Sensing,BCS)构造测量矩阵的方式不同。由于P张量积压缩感知模型与半张量积压缩感知模型构造测量矩阵的方式相同,因此在测量矩阵生成时间以及空间占用方面的表现相同。

采用不同的压缩感知模型对尺寸为1000 × 1000的图像进行压缩,图像压缩率ratio。传统压缩感知模式下测量矩阵内的元素个数为1000 × 1000 × *ratio*;分块压缩感知模型下,设将图像分为N_b块,则测量矩阵内的元素个数为$\frac{1000\times1000}{N_b}\times ratio$;在P张量积压缩感知模型下,设测量矩阵的维度放大系数为N_p,则测量矩阵内的元素个数为$\frac{1000}{N_b}\times\frac{1000}{N_b}\times ratio$。在不同的压缩率下各个压缩感知模型构造测量矩阵时矩阵内的元素的个数如表1,表格中元素数值的量级为10^5。

表1 不同压缩感知模型下的测量矩阵所需元素个数

Ratio	0.25	0.375	0.50	0.625	0.75
T-CS	2.500	3.750	5.000	6.250	7.500
BCS-32	2.621	3.932	5.243	6.554	7.864
BCS-16	38.147	57.220	76.294	95.367	114.44
BCS-8	610.35	915.53	1220.7	1525.9	1831.1
P-CS-8	0.039	0.059	0.078	0.098	0.117
P-CS-4	0.156	0.234	0.313	0.391	0.467

从表1可以看出分块压缩感知模型与P张量压缩感知模型都比传统的压缩感知模型需要更少的矩阵元素,同时由于在分块压缩感知模式下如果图像分块数量较大,造成每一块图像维数过小,使得图像还原重建效果不理想。因此,P张量积压缩感知模型构造的测量矩阵能够在保证图像还原重建效果的前提下降低测量矩阵的空间占用。

P张量积压缩感知模型下,不同压缩率下图像还原重建效果,如图1,其中第一行为原始高分辨率图像,从第二列至最后一列分别为0.75、0.50、0.25的压缩率下的还原重建图像及其对应的峰值信噪比(Peak Signal to Noise Ratio,PSNR)

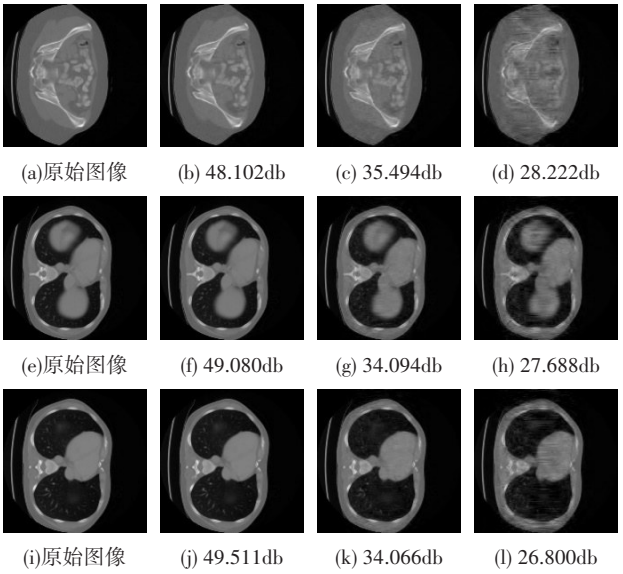


图1 P张量压缩感知对三张医学图像进行压缩的还原重建效果

由于Chaotic测量矩阵是通过在混沌序列中进行等间距采样的方式构造的,同时采样间距d必须满足$d \geq 15$的条件才能够保证矩阵内的元素相关性足够低,通常d的设置为1000,从而造成生成测量矩阵的过程中需要生成长度很大的混沌序列,造成Chaotic测量矩阵的生成速度较慢且占用空间较大,应用的广泛性受到限制。表2中为对尺寸为512 × 512的图片进行采样压缩,构造测量Chaotic矩阵所需要的时间,随着矩阵的放大系数的增大所需时间大幅下降(单位:毫秒)。

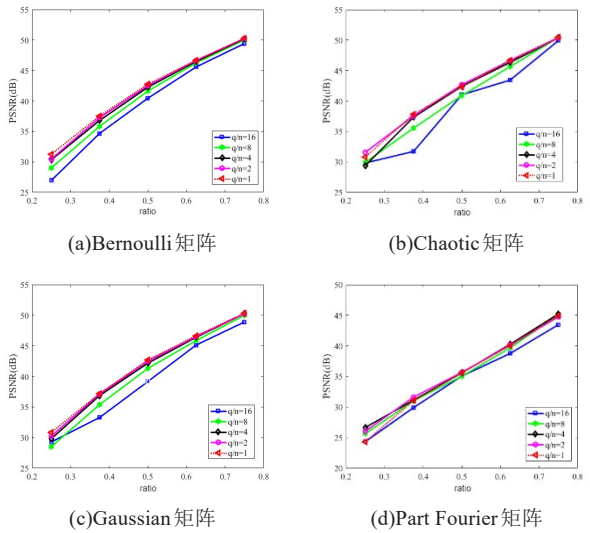
表2 不同压缩感知模型下的测量矩阵所需元素个数

q/n	16	8	4	2	1
0.25	1.400	5.000	19.80	72.30	286.1
0.50	2.200	9.200	36.30	143.5	577.1
0.75	3.400	15.40	55.10	215.4	875.1

P张量积压缩感知模型下,不仅能够降低生成测量矩阵的空间占用同时能够降低测量矩阵的生成时间。

4.2 测量矩阵性能对比

在P张量积压缩感知模型下,通过设置不同的矩阵放大系数分别为1、2、4、8、16,对尺寸为512×512的图像进行采样压缩,以及还原重建,如图2所示。不同的测量矩阵在P张量积压缩感知模型下的表现,特别地,当$q/n = 1$时,为传统压缩感知模型下的测量矩阵表现,P张量积压缩感知模型下能够保证测量矩阵



(a)Bernoulli 矩阵　(b)Chaotic 矩阵

(c)Gaussian 矩阵　(d)Part Fourier 矩阵

图 2　P 张量积压缩感知模型下测量矩阵性能对比

的性能的前提下降低存储空间占用。

4.3　重建算法对比

使用 IRLS 算法以及正交匹配追踪(Orthogonal Matching Pursuit,OMP)算法，测量矩阵为 chaotic 矩阵，进行 10 次重复实验。可以看出在传统压缩感知模型下 IRLS 算法与 OMP 算法的表现几乎相同，但是在 P 张量积压缩感知模型下，IRLS 算法的优势逐渐明显。同时随着矩阵的放大系数还原重建的稳定性降低，这是由于测量矩阵的维数降低，测量矩阵性能受到影响。IRLS 算法与 P 张量积压缩感知模型更为契合。如表 4 中图像还原重建的 PSNR 值。

表 3 不同压缩感知模型下的测量矩阵所需元素个数

q/n	S	IRLS&ratio		OMP&ratio	
		0.25	0.75	0.25	0.75
1	mean	29.598	49.219	29.283	49.502
	std	0.206	0.0492	0.236	0.0468
4	mean	27.402	48.987	11.607	28.645
	std	3.195	0.169	1.623	9.301
16	mean	27.011	48.017	10.714	22.270
	std	2.6789	0.699	3.219	7.458
32	mean	27.213	46.112	10.060	25.400
	std	3.301	0.920	2.236	4.888

4.4　加密算法性能

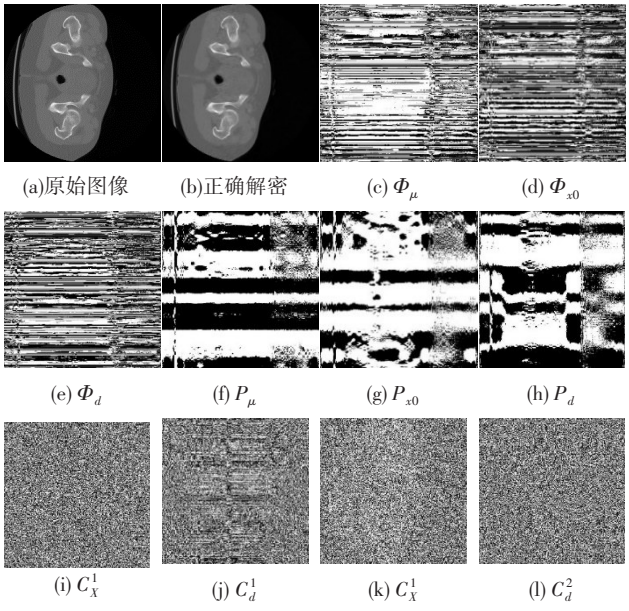
加密算法由两部分组成，包括 Chen-chaotic 系统和生成 chaotic 测量矩阵的 Logistic-chaotic 系统，$\left(\Phi_\mu,\Phi_{x0},\Phi_d,P_\mu,P_{x0},P_d,C_X^i,C_Y^i,C_Z^i,C_H^i,C_d^i\right)i = 1,2$，为加密系统密钥的组成。$\left(C_Y^i,C_Z^i,C_H^i,C_d^i\right)$的密钥空间以及密钥敏感性相同，设密钥空间为 S_1，$\left(\Phi_\mu,\Phi_{x0},P_\mu,P_{x0}\right)$的密钥空间为 S_2，Φ_d与P_d的取值空间为$\left[15,S_3\right]$，P_d的取值范围为$\left[1,S_4\right]$，经过混沌序列误差实验

$$MAE(s,\bar{s}) = \frac{1}{N}\sum_{i=1}^{N}\left|s_{i-\bar{S}_i}\right| \tag{17}$$

得到加密算法的密钥空间为

$$S = 10^{S_1\times 8}\times 10^{S_2\times 4}\times S_3^2\times S_4^2 \tag{18}$$

其中 S_1 为 16，密钥敏感性为 10^{-16}，同理 S_2 为 15，取 S_3 为 1000，S_4 为 100，故加密算法的密钥空间为 10^{200}。足够抵抗暴力破解的攻击，保证信息安全性。图 3 为分别对每一个密钥进行敏感度实验，测试每一个密钥在错误为 1 个敏感度时的解密效果。



(a)原始图像　(b)正确解密　(c) Φ_μ　(d) Φ_{x0}

(e) Φ_d　(f) P_μ　(g) P_{x0}　(h) P_d

(i) C_X^1　(j) C_d^1　(k) C_X^1　(l) C_d^2

图 3　每个密钥错误为 1 个敏感度时的解密效果

表 4 图 2 中图像的数据结果(单位：dB)

–	PSNR db	MSE	UACI %
(c)	6.391	1.131E+4	16.739
(d)	6.718	1.385E+4	18.2173
(e)	7.597	1.492E+4	19.336
(f)	−10.173	6.767E+5	29.525
(g)	1.312	4.803E+5	23.710
(h)	−11.464	9.110E+5	31.132
(i)	−8.693	4.813E+5	43.719
(j)	−26.626	9.901E+6	48.872
(k)	−5.464	2.288E+5	41.612
(l)	−50.751	7.730E+9	50.012

从实验结果中可以看出加密算法能够抵抗暴力破解,同时具备密钥高敏感性、密钥空间大的特点。初次之外,我们还进行了关于图像的信息熵的实验,加密图像的信息熵可以达到7左右,同时分析加密图像的像素相关性发现加密算法性表现良好,原始图像各个像素相关性为1左右,加密后的图像的像素相关性为0左右。同时由于加密系统中考虑到了图像像素值篡改的问题,将密钥的组成部分与图像的像素值相关联,达到了防止篡改的目的。

5 结论与展望

本文提出的基于P张量积的压缩感知的医学影像传输系统,能够降低存储空间占用保护图像信息内容的安全,缩短测量矩阵生成时间加快压缩过程。实验结果表明,提出的压缩感知模型具备高效性以及稳定性。提出的加密算法在密钥空间上表现突出,密钥具备高灵敏度。

参考文献(References):

[1] Duk-Woo Ro. PACS and imaging informatics:basic principles and applications(book review)[J]. Ridiology, 2005, 235(3).

[2] Ahmad M., Farooq O. Secure satellite images transmission scheme based on Chaos and discrete wavelet transform [C]. HPAGC 2011: High Performance Architecture and Grid Computing, 2011:257-264.

[3] Kumar H, Srivastava A. A secret sharing scheme for secure transmission of color images[C]. 2014 International Conference on Issues & Challenges in Intelligent Computing Techniques (ICICT 2014), 2014:857-860.

[4] Felipe Rodrigues Martinêz Basile,Flávio Cezar Amate. Secure transmission of medical images by SSH tunneling[C]. HCI International 2011 – Posters' Extended Abstracts, 2011:486-490.

[5] Yuan X, Haimi-Cohen R. Image compression based on compressive sensing: end-to-end comparison with JPEG [J]. IEEE Transactions on Multimedia, 2020,22(11): 2889 - 2904.

[6] Wei Li, Chaolu Feng , Kun Yu, Dazhe Zhao. MISS-D: a fast and scalable framework of medical image storage service based on distributed file system[J]. Computer Methods and Programs in Biomedicine,2020, 186.

[7] Chen Y, Ding S, Xu Z, et al. Blockchain-Based Medical Records Secure Storage and Medical Service Framework[J]. Journal of Medical Systems ,2019, 43(1):5.

[8] Mouhib Ibtihal, DM El Ouadghiri , Naanani Hassan. Homomorphic encryption as a service for outsourced images in mobile cloud computing environment[J]. International Journal of Cloud Applications and Computing. 2017,7(2): 27-40.

[9] Meena M, Bharadi V A, Krunali vartak. Hybrid wavelet based cbir system using software as a service (saas) model on public cloud[J].Procedia Computer Science, 2016, 79: 278-286.

[10] Candes E J, Romberg J, Tao T. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information[J]. IEEE Transactions on Information Theory,2006,52(2):489-509.

[11] Wang J, Ye S, Ruan Y. et al. Low storage space for compressive sensing: semi-tensor product approach[J]. EURASIP Journal on Image and Video Processing,2017:51.

[12] Sun Z , Liu J , Li Z , et al. CSR-IM: Compressed Sensing Routing-Control- Method With Intelligent Migration-Mechanism Based on Sensing Cloud-Computing[J]. IEEE Access, 2020, 8: 28437 - 28449.

[13] Zheng S , Zhang X P , Chen J , et al. A high-efficiency compressed sensing-based terminal-to-cloud video transmission system [J]. IEEE Transactions on Multimedia, 2019,21(8): 1905 - 1920

[14] Chartrand R , Yin W . Iteratively reweighted algorithms for compressive sensing [C]. IEEE International Conference on Acoustics, Speech and Signal Processing ,2008.

[15] Peng H , Mi Y , Li L , et al. P-tensor product in compressed sensing[J]. IEEE Internet of Things Journal, 2019, 6(2): 3492 – 3511.

责任编辑:王谦,王雨田