计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2023,32(1):187−196 [doi: 10.15888/j.cnki.csa.008918]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

结合 *P* 张量积压缩感知的混沌图像加密算法①

周　洋[1], 于海洋[1], 蒋东华[2], 陈颖频[3]

[1](黑龙江大学 计算机科学技术学院, 哈尔滨 150080)
[2](长安大学 信息工程学院, 西安 710064)
[3](闽南师范大学 物理与信息工程学院, 漳州 363000)
通信作者: 于海洋, E-mail: 1995011@hlju.edu.cn

摘　要: 针对目前数据加密算法缺乏隐蔽性的缺点, 提出了一种结合 *P* 张量积压缩感知 (*P*-tensor product compressive sensing, PTP-CS) 模型和新分段混沌映射 (segmented chaotic map, SCM) 的视觉安全图像加密算法. 首先, 根据“拉伸和挤压”机制设计出一新的具有分式结构的分段混沌映射, 用以构建受控测量矩阵. 其次, 在测量矩阵和密码流的共同控制下, 明文的小波包系数矩阵经过二维阿诺德置乱、线性测量以及双向异或扩散生成视觉上无语义的中间秘密图像. 然后, 再采用数字隐写编码方法将其随机地嵌入到某一非涉密传输介质中以同步实现对敏感明文数据的内容和视觉的双重保护. 最后, 一系列的仿真实验和安全性分析表明所提加密算法能够抵御多种常见的攻击, 且具有很好的视觉安全性和压缩性能.

关键词: 图像加密; *P* 张量积; 压缩感知; 分段混沌映射; 安全性分析

引用格式: 周洋,于海洋,蒋东华,陈颖频.结合 *P* 张量积压缩感知的混沌图像加密算法.计算机系统应用,2023,32(1):187–196. http://www.c-s-a.org.cn/1003-3254/8918.html

Chaotic Image Encryption Algorithm Combining *P*-tensor Product Compressive Sensing

ZHOU Yang[1], YU Hai-Yang[1], JIANG Dong-Hua[2], CHEN Ying-Pin[3]

[1](School of Computer Science and Technology, Heilongjiang University, Harbin 150080, China)
[2](School of Information Engineering, Chang'an University, Xi'an 710064, China)
[3](School of Physics and Information Engineering, Minnan Normal University, Zhangzhou 363000, China)

Abstract: As the current data encryption algorithms lack covertness, a visually secure image encryption algorithm is proposed, which combines the *P*-tensor product compressive sensing (PTP-CS) model and the new segmented chaotic map (SCM). First, the new SCM with fractional structure is designed according to the “stretching and squeezing” mechanism to construct the key-controlled measurement matrix. Secondly, under the joint control of the measurement matrix and cipher code streams, the intermediate secret image without visual semantics is generated after the two-dimensional (2D) Arnold scrambling, linear measurement, and bidirectional XOR diffusion of the plaintext wavelet-packet coefficient matrix. Then, the digital steganographic coding approach is employed to embed it stochastically into the non-secret-involved transmission medium to synchronously protect the content and appearance of the sensitive plaintext data. Simulation experiments and security analysis indicate that the proposed encryption algorithm is capable of defending against various common attacks, and it has good visual security and compression performance.

Key words: image encryption; *P*-tensor product; compressive sensing; segmented chaotic map; security analysis

① 基金项目: 福建省自然科学基金 (2020J05169, 2020J01816)
收稿时间: 2022-05-26; 修改时间: 2022-06-27, 2022-07-06, 2022-07-20; 采用时间: 2022-07-22; csa 在线出版时间: 2022-11-14
CNKI 网络首发时间: 2022-11-15

随着多媒体技术的发展和移动互联网技术的普及, 作为重要的数字化信息载体, 数字图像被广泛地应用于各个领域中. 然而, 在当前开放的网络环境中, 数字图像所面临潜在的诸如监听、篡改、盗用及伪造等安全风险也不容小觑. 为有效保护敏感图像数据的安全, 数字图像加密技术孕育而生, 并已然成为信息安全领域的研究重点之一.

混沌信号所具有的长期不可预测性和其对初始状态的极度敏感性使得混沌系统在安全通信领域得到迅速的发展[1]. 迄今为止, 通过将混沌理论与神经网络[2]、量子计算[3]、压缩感知[4,5] 和元胞自动机[6] 等技术相结合, 提出了许多高安全性且视觉上无语义特征的图像加密算法. 此外, 随着研究的深入, 一些科研人员有针对性地对遥感、光学以及医学领域中数字图像的特征进行分析, 进而提出相应的隐私数据保密技术[7–9]. 例如在文献 [9] 中, Jeevitha 等结合二维多层离散小波分解和边缘图设计出适用于 MRI (magnetic resonance imaging) 图像的加密算法. 然而, 前面所提及到的数据加密方案均存在一个共同的缺陷, 即最终生成的密文图像具有统计类噪声特性. 特别是近年来随着深度学习技术的不断创新和突破, 基于数据驱动的深度人工神经网络模型可以智能化地对公用信道中传输的无视觉意义的密文数据进行解密分析、恶意攻击以及非法拦截等.

为了对密文图像的外观进行保护, Bao 等在文献 [10] 中介绍了一种先加密后嵌入的算法框架. 在该方案中, 首先通过现有的加密技术手段完成对明文图像的内容保护. 其次, 再通过提升离散小波变换嵌入方法将具有统计伪随机特性的秘密图像嵌入到可公开获取的载体图像中. 随后, Wang 等[11] 和 Chai 等[12] 分别将并行压缩感知模型和二维压缩感知模型引入到 Bao 的加密框架中, 以降低不必要的存储资源和传输花销. 然而, 正如在文献 [13] 中所指出的, 压缩感知模型的本质是线性投影 (或线性测量), 因此其不能有效地抵御一系列基于明文分析的安全攻击模型. 不过通过采用明文数据的特征值、哈希值[14] 或者分块计数器模式[15] 来更新测量矩阵的策略恰好可以弥补这一点缺陷. 其他方面, 对于现有的基于变换域嵌入的视觉安全加密算法, 如多分辨率奇异值分解嵌入[16]、舒尔分解嵌入[17] 和斜变换嵌入[18], 由于在嵌入阶段中存在截断误差和误差扩散效应, 因此很难得到较好的视觉安全性和重建质量.

针对上述问题, 本文首先提出一新颖的分段混沌映射, 并对其混沌性能进行分析和对比. 其次, 将该分段混沌映射与 P 张量积压缩感知模型、数字隐写编码方法相结合, 设计出一种新颖的具有视觉安全性的图像加密算法. 该加密算法主要由压缩加密和随机嵌入这两个阶段组成. 首先在第 1 阶段中, 通过 Arnold 置乱策略、线性测量和双向扩散对明文图像进行压缩加密, 获得无语义特征的中间秘密图像. 在第 2 阶段中, 在不扩大载体图像分辨率的情况下, 利用隐写编码嵌入生成最终视觉安全的密文图像.

1 相关知识

1.1 超混沌 Qi 系统

考虑到 Qi 等[19] 所提出的四维超混沌系统具有复杂的非线性动力学行为, 且在相空间中, 其运动轨迹的遍历范围广, 因此适用于图像加密领域. 该四维超混沌系统的数学定义如式 (1) 所示:

$$\begin{cases} \dot{x} = a(y-x)+yz \\ \dot{y} = b(x+y)-xz \\ \dot{z} = -cz-ew+xy \\ \dot{w} = -dw+fz+xy \end{cases} \tag{1}$$

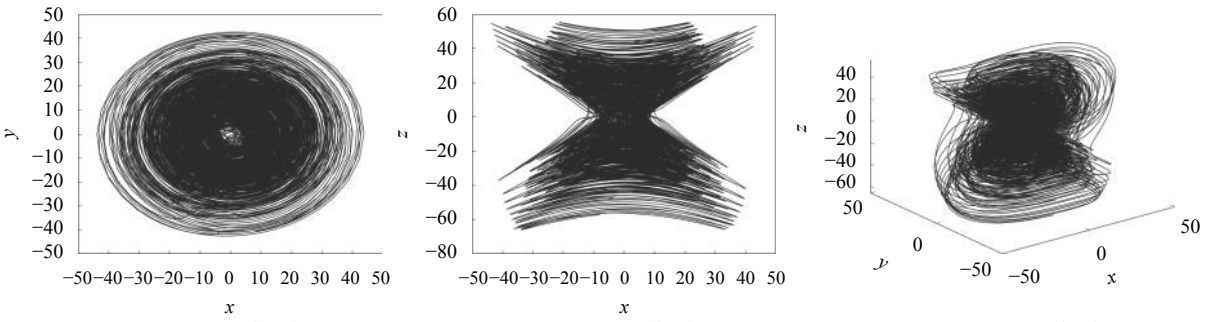
其中, 符号 a, b, c, d, e 和 f 为可调的系统控制参数, 而 $[x, y, z, w]$则为该混沌系统的 4 个输出状态变量, $\dot{x}$表示对x执行微分运算. 当$a = 50$, $b = 24$, $c = 13$, $d = 8$, $e = 33$, $f = 30$时, 式 (1) 中存在两个大于 0 的李雅普诺夫指数, 表明该非线性动力系统进入超混沌状态. 再将该系统的初始参数分别设为 5, 7, 9 和 11, 步长设为 0.000 1, 则通过四五阶龙格库塔法所得到的混沌吸引子如图 1 所示.

1.2 P 张量积压缩感知模型

相比于传统的一维压缩感知模型, P 张量积压缩感知模型可以在测量矩阵与像素值矩阵的维度不匹配的情况下完成对明文数据的线性压缩[20]. 将明文图像和正交小波包稀疏基分别记为$X \in \mathbb{R}^{q\times q}$和$\Psi \in \mathbb{R}^{q\times q}$, 其中上标$q\times q$为矩阵维度. 则明文图像的稀疏分解过程可表示为:

$$X = \Psi \times S \tag{2}$$

其中, 矩阵$S \in \mathbb{R}^{q\times q}$表示为明文图像在$\Psi$域中的稀疏系数矩阵. 则在 PTP-CS 模型中, 对明文图像 X 进行压缩的过程可表示为:



(a) x-y 平面相图 (b) x-z 平面相图 (c) x-y-z 平面相图

图 1 超混沌 Qi 系统的吸引子图

$$Y=\Phi_{\triangleright}^{P}\times X=(\Phi\otimes P)\times X=(\Phi\otimes P)\times\Psi\times S \tag{3}$$

其中, 符号$\triangleright^{P}$和$\otimes$分别表示为 P 张量积和克罗内克积. 假设, $\Phi\in\mathbb{R}^{m\times n}$, $P\in\mathbb{R}^{t\times t}$, $m<n$, $t=\left\lfloor q\times n^{-1}\right\rfloor$, 并将测量矩阵$\Phi$重写为向量的形式, 即为$\Phi=[\varphi_1,\varphi_2,\cdots,\varphi_n]$, 则矩阵的 P 张量积可以写为:

$$\Phi\otimes P=(\varphi_1 P,\cdots,\varphi_n P)=\begin{pmatrix}\varphi_{11}P & \cdots & \varphi_{1n}P\\ \vdots & \ddots & \vdots\\ \varphi_{m1}P & \cdots & \varphi_{mn}P\end{pmatrix} \tag{4}$$

于是有$\Phi\otimes P\in\mathbb{R}^{(m\times t)\times(n\times t)}$, 且$Y\in\mathbb{R}^{\left(mq\times n^{-1}\right)\times q}$. 其中, 系数$mn^{-1}$和$qn^{-1}$分别叫做矩阵的压缩率和放大系数. 在本文所提算法中, 矩阵 P 设置成维度为 2 的单位阵, 而矩阵Φ则由所提出的一维分段混沌映射所构建.

2 所提出的分段混沌映射

2.1 分段混沌映射的定义

本文所提出的具有分式结构的一维分段混沌映射的数学迭代式如式 (5) 所示. 其中, 符号$\beta\in[-0.25,\ 0.25]$和 x 分别为该映射的可调参数和输出变量.

$$x_{i+1}=\begin{cases}\dfrac{2\cos(\beta\pi x_i)}{2x_i^4+1}-x_i,\ 0\leqslant x_i\leqslant 2\\ -\dfrac{2\cos(\beta\pi x_i)}{2x_i^4+1}-x_i,\ -2\leqslant x_i<0\end{cases} \tag{5}$$

其中, 分式结构$\pm2\cos(\beta\pi x_i)\Big/(2x_i^4+1)$用于分离相空间中相邻演化轨道的两个点, 且常数“1”用于防止分式无意义. 另外, 相减部分则是将该非线性映射的输出范围限制在区间 [−2, 2] 内.

2.2 性能分析与对比

分岔图反映非线性动力系统在确定的初始条件下所产生的时间序列的长期演化状态, 其中包括稳定状态、非稳定状态、周期状态和混沌状态[21]. 接着, 将所提出的分段混沌映射的初始状态x_0随机设置成 1.2, 绘制出该一维混沌映射的分岔图, 如图 2 所示. 可以看出, 与经典一维 Logistic 混沌映射不同, 即其所生成的时间序列经历稳定态→非稳定态→周期态→混沌态等 4 个不同演化阶段, 本文所设计的非线性映射始终处于混沌状态, 且具有更宽的遍历范围.

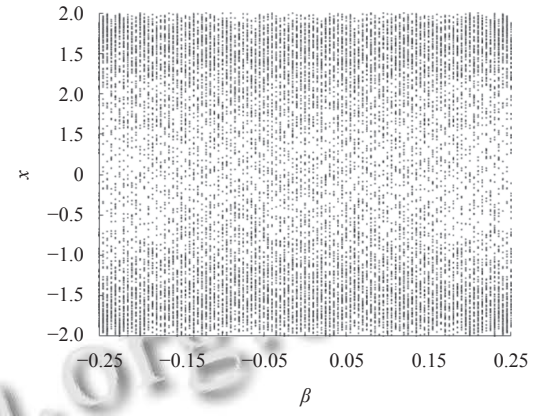


图 2 所提混沌映射的分岔图

0-1 测试是一种用于衡量非线性系统是否存在混沌现象的测试方法[22]. 与其他评估方法相比, 此方法最大的优点是在测试过程中不需要对时间序列进行相空间重构. 对于混沌序列 Q 而言, 其 0-1 测试的数值结果可由式 (6) 计算得到:

$$\begin{cases}K=\lim\limits_{n\to\infty}\ln\left(\dfrac{1}{N}\sum\limits_{i=1}^{n}\left([p(i+n)-p(i)]^2+[s(i+n)-s(i)]^2\right)\right)\\ \qquad\times\ln(n)^{-1}\\ p(n)=\sum\limits_{i=1}^{n}Q(i)\cos(ir)\\ s(n)=\sum\limits_{i=1}^{n}Q(i)\sin(ir)\end{cases} \tag{6}$$

其中, 变量 r 和 N 分别被设置为[0.25π,0.8π]和 1 000. 接下来, 图 3 给出了若干个一维混沌映射在控制参数不同取值下所产生的混沌序列的 0-1 测试结果. 可以清楚地看出, 与文献 [23–25] 中所介绍的一维非线性映射相比, 本文所提出的映射的 K 值更大且更宽, 说明所设计的分式结构映射具有良好的混沌性能.

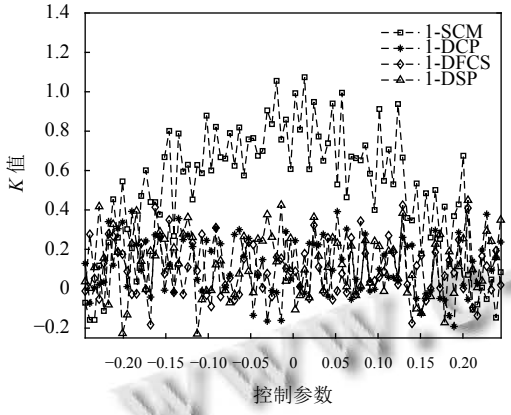


图 3　若干个混沌映射的 0-1 测试图

3　视觉安全图像加解密算法

本文所提出的视觉安全图像加密算法主要由基于 PTP-CS 模型的压缩加密阶段和基于矩阵编码的信息嵌入阶段两部分组成, 其加密流程如图 4 的上半部分所示. 从图中可以看出, 在密码流的控制下, 明文图像首先经过稀疏化分解、Arnold 置乱、压缩和双向异或扩散以生成没有视觉语义特征的秘密图像. 其次, 再在空域-中通过矩阵编码嵌入将秘密图像随机地隐藏到载体图像中, 得到具有视觉安全性的密文图像. 所提加密算法的技术细节如下.

3.1　压缩加密阶段

步骤 1. 首先, 对明文图像$P_1 \in \mathbb{N}^{N\times N}$执行二维离散小波包变换以得到明文稀疏系数矩阵$P_2 \in \mathbb{R}^{N\times N}$, 其次, 为了进一步提升矩阵$P_2$的稀疏度和重建图像的视觉质量, 对其进行阈值处理和二维 Arnold 置乱操作, 并将该过程所生成的系数矩阵记作$P_3 \in \mathbb{R}^{N\times N}$. 另外, Arnold 置乱可以通过式 (7) 表示, 其中, 坐标$[i_{n-1},\ j_{n-1}]$和$[i_n,\ j_n]$分别为置乱前后系数矩阵中元素的位置, 序列X_a和X_b是在密钥的控制下由超混沌 Qi 系统所产生的伪随机序列, 而符号 mod 则表示取模操作.

$$\begin{bmatrix} i_n \\ j_n \end{bmatrix} = \begin{bmatrix} 1 & X_a \\ X_b & X_a \cdot X_b + 1 \end{bmatrix} \times \begin{bmatrix} i_{n-1} \\ j_{n-1} \end{bmatrix} \bmod \begin{bmatrix} N \\ N \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \end{bmatrix} \tag{7}$$

步骤 2. 通过加模操作对给定的初始状态和明文图像的平均像素值进行处理. 在运算得到的新初始状态下, 迭代新分段混沌映射若干次以获得混沌序列X_c. 然后, 再根据式 (8) 对该序列进行进一步处理. 其中, 常量 d 为抽样距离.

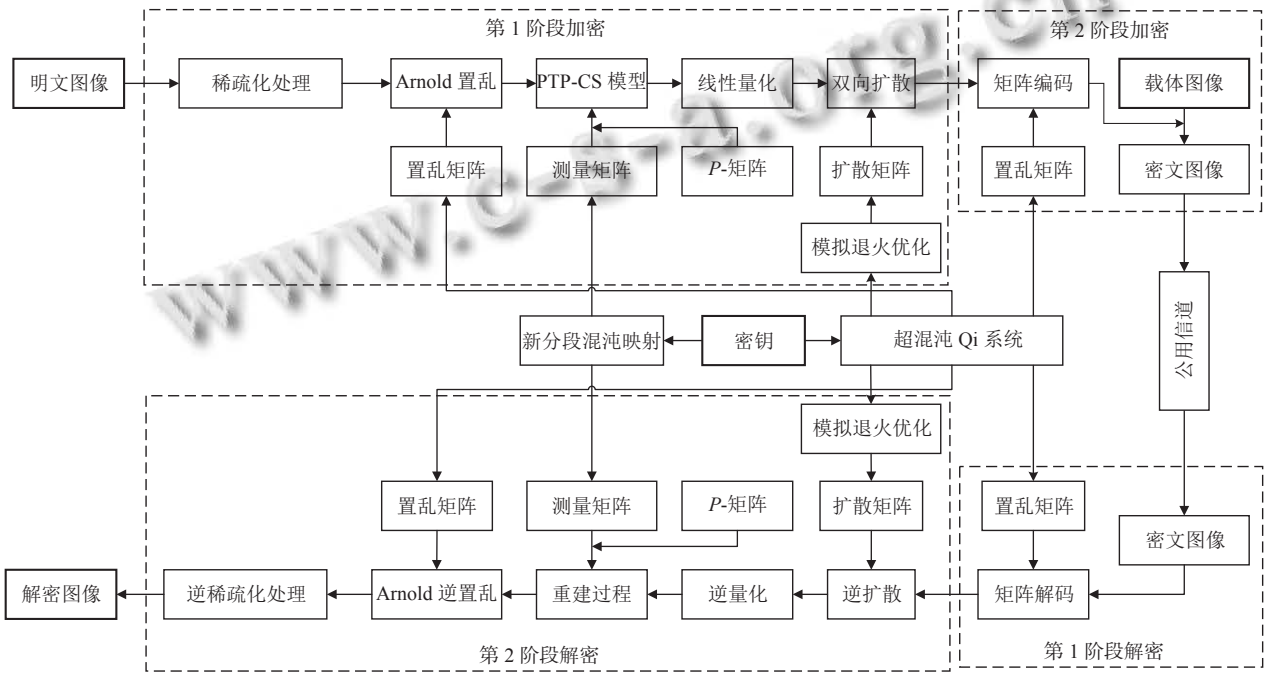


图 4　所提视觉安全图像加密/解密算法的流程图

$$W(i)=1-2X_c(di),\ i=1,\ 2,\ 3,\ \cdots \tag{8}$$

接着对混沌抽样序列 W 以按列的方式重塑为二维矩阵并执行归一化处理, 得到测量矩阵Φ, 如式 (9) 所示:

$$\Phi=\sqrt{\frac{4}{N}}\begin{bmatrix} W_1 & W_{N/8+1} & \cdots & W_{N(N-2)/16+1} \\ W_2 & W_{N/8+2} & \cdots & W_{N(N-2)/16+2} \\ \vdots & \vdots & \ddots & \vdots \\ W_{N/8} & W_{N/4} & \cdots & W_{N^2/16} \end{bmatrix} \tag{9}$$

将矩阵 P 设置为$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, 并对矩阵$P_3$执行如式 (10) 和式 (11) 所示的操作, 即可得到压缩图像P_5. 其中, 变量$P_{\max}$和$P_{\min}$分别记为矩阵P_4中的极值.

$$P_4=\Phi_{\triangleright}^{P}\times P_3=(\Phi\otimes P)\times P_3 \tag{10}$$

$$P_5=\left\lfloor\left(2^8-1\right)\times(P_4-P_{\min})\times(P_{\max}-P_{\min})^{-1}\right\rfloor \tag{11}$$

步骤 3. 由于文献 [13] 中指出压缩感知模型的本质是线性映射, 因此不能有效抵抗选择明文攻击, 有必要对压缩图像执行扩散操作以使得明文图像发生细微的差别都将产出存在具有巨大差异且无语义的秘密图像. 首先, 在给定初始状态的情况下, 量化超混沌 Qi 系统迭代若干次生成的两条混沌序列, 获得整数序列X_d和X_e. 然后通过模拟退火算法对这两条序列进行优化[26], 具体步骤如下.

(1) 对两条整数序列做差 (X_d-X_e) 以得到目标序列 L.

(2) 如果$L_i\geqslant 0$, 则最优解为$D_i=L_i$. 否则, 计算出阈值$P_c=\exp\left(-|L|\cdot i^{-1}\right)$和概率$P_t=\exp\left(-i^{-1}\right)$.

(3) 如果$P_c\geqslant P_t$, 则最优解为$D_i=L_i$. 否则, 最优解为$D_i=X_d\oplus X_e\mod 256+1$.

接下来对压缩图像执行双向异或扩散操作, 如式 (12) 所示. 其中, 变量$m_0\in[0,255]$和$m_1\in[0,255]$为外部密钥, $D^{(1)}$表示序列D中的第 1 个元素值.

$$\begin{cases} P_6^{(1)}=m_0\oplus P_5^{(1)}\oplus D^{(1)} \\ P_6^{(n)}=P_6^{(n-1)}\oplus P_5^{(n)}\oplus D^{(n)} \\ P_7^{(\mathrm{end})}=m_1\oplus P_6^{(\mathrm{end})}\oplus D^{(\mathrm{end})} \\ P_7^{(\mathrm{end}-i)}=P_7^{(\mathrm{end}-i+1)}\oplus P_6^{(\mathrm{end}-i)}\oplus D^{(\mathrm{end}-i)} \end{cases} \tag{12}$$

3.2 嵌入阶段

就现有的图像加密算法而言, 其所产生的密文图像具有明显的伪随机特性. 因该类密文图像在公用网络中传输时, 极易遭到人工神经网络模型的拦截、窃听、伪造以及恶意攻击等. 基于此, 本文将采用基于矩阵编码的嵌入方法为加密数据提供视觉上的保护.

步骤 1. 在初始状态情况下, 对迭代超混沌 Qi 系统若干次生成的序列X_f进行排序, 并用得到的索引值序列对加密图像P_7执行索引置乱, 得到矩阵P_8.

步骤 2. 在算法 1 的控制下, 在空域中将加密数据通过隐写编码的方式嵌入到非涉密传输介质-载体图像中. 至此, 加密过程完成.

算法1. 基于隐写编码的空域嵌入算法

输入: 秘密图像P_8, 载体图像$H\in\mathbb{N}^{N\times N}$

输出: 具有视觉安全性的密文图像$V\in\mathbb{N}^{N\times N}$

```
(1) [m, n] = size(P8)
(2) for i = 1:mn end
(3)     T1 = bitand(P8(i), 192, "int16");
(4)     T2 = bitand(P8(i), 48, "int16");
(5)     T3 = bitand(P8(i), 12, "int16");
(6)     T4 = bitand(P8(i), 3, "int16");
(7)     Z(1) = bitshift(T1, –6); Z(2) = bitshift(T2, –4);
(8)     Z(3) = bitshift(T3, –2); Z(4) = T4;
(9)     for j = 1:4 do
(10)      a = bitget(H(i), 1);
(11)      b = bitget(H(i), 2);
(12)      c = bitget(H(i), 3);
(13)      su= c×1⊕b×2⊕a×3
(14)      if su != Z(i) do
(15)          s= su⊕Z(i)
(16)        if bitget(H(i), 4–s) == 0 do
(17)            v = 1;
(18)        else
(19)            v = 0;
(20)        end do
(21)        I(i) = bitset(H(i), 4–s, v)
(22)      end do
(23)    end do
(24)    V(4i–3) = I(1); V(4i–2) = I(2);
(25)    V(4i–1) = I(3); V(4i) = I(4);
(26) end do
```

3.3 解密过程

本文提出的加密算法所对应的解密流程如图 4 下半部分所示. 当解密方通过安全通道获得解密密钥以后, 可以对视觉有意义的密文图像进行以下操作来恢复出其所携带的明文敏感数据.

步骤 1. 首先, 利用接收到的解密密钥迭代超混沌 Qi 系统和新提出的分段混沌映射以生成若干条混沌序列, 进而构建出解密过程中所需的密码流.

步骤 2. 通过矩阵解码算法和索引逆置乱操作从隐写的密文图像中提取出加密图像P_7.

步骤 3. 在密码流的控制下, 对加密图像执行双向的逆异或扩散, 并再利用量化参数P_{max}和P_{min}进行逆量化操作, 得到压缩后的明文稀疏系数矩阵.

步骤 4. 根据优化算法, 使用矩阵Φ和P从P_4中恢复出明文系数矩阵P_3.

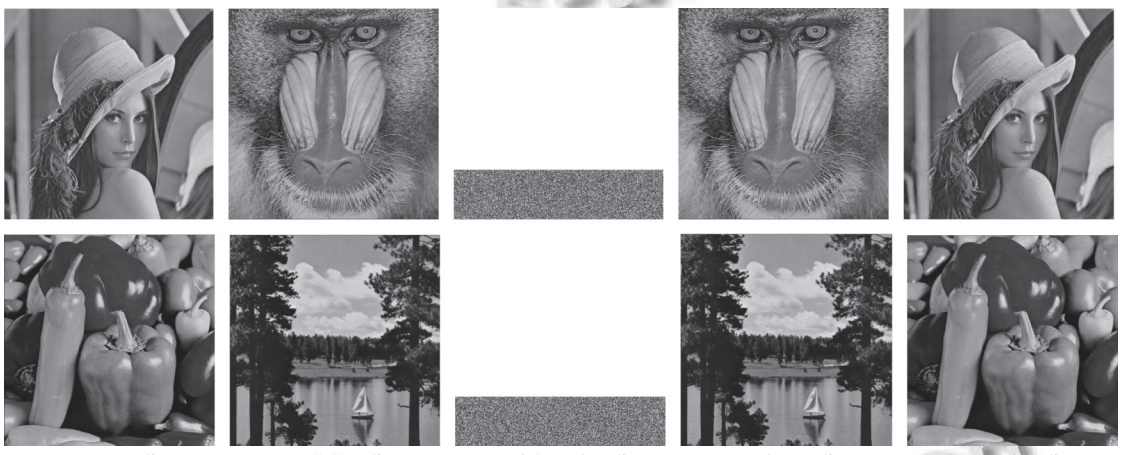
步骤 5. 再通过对系数矩阵P_3执行二维 Arnold 置乱和逆离散小波包变换, 得到最终的解密图像.

4 实验结果与分析

4.1 仿真实验结果

实验平台为搭载在 I7-8550U CPU 和 16 GB 内存笔记本电脑上的 Matlab 2020B. 仿真实验中, 新分段混沌映射的初始状态和控制参数分别设为 0.678 和 0.2, 而超混沌 Qi 系统的 3 个初始状态分别为 0.238, 0.471, −1.2 和 0.39. 另外, 参数$d = 15$, $m_0 = m_1 = 127$, 压缩率为 0.25, 稀疏基选为多贝西小波.

随机选择分辨率为512×512的两幅明文图像和两幅可公开获取的载体图像进行仿真实验, 且所得到的实验结果如图 5 所示. 可以看出, 明文图像被有效地压缩并加密成类噪声的中间秘密图像, 实现了对明文图像数据的内容保护. 除此之外, 生成的密文图像具有视觉上的语义, 与相应的载体图像高度相似. 其他方面, 从密文图像中恢复出的解密图像与对应的明文图像在视觉上并无差别.



(a) 明文图像 (b) 载体图像 (c) 中间秘密图像 (d) 密文图像 (e) 解密图像

图 5 所提视觉安全图像加密/解密算法的仿真结果

接下来, 采用定量的评估方法, 即峰值信噪比 (peak signal-to-noise ratio, PSNR) 和平均结构相似度 (mean structural similarity, MSSIM)[18], 来对所提加密方案的重构效果和视觉安全性进行评价. 测得两组实验中明文图像与解密图像, 载体图像与密文图像之间平均 PSNR 和 MSSIM 值分别为 36.680 4 dB, 0.947 7 和 43.949 0 dB, 0.995 0. 从得到的实验数值结果可以看出, 在不受到噪声等因素的干扰情况下, 所提出的算法具有不错的视觉安全性和解密质量.

4.2 安全性分析

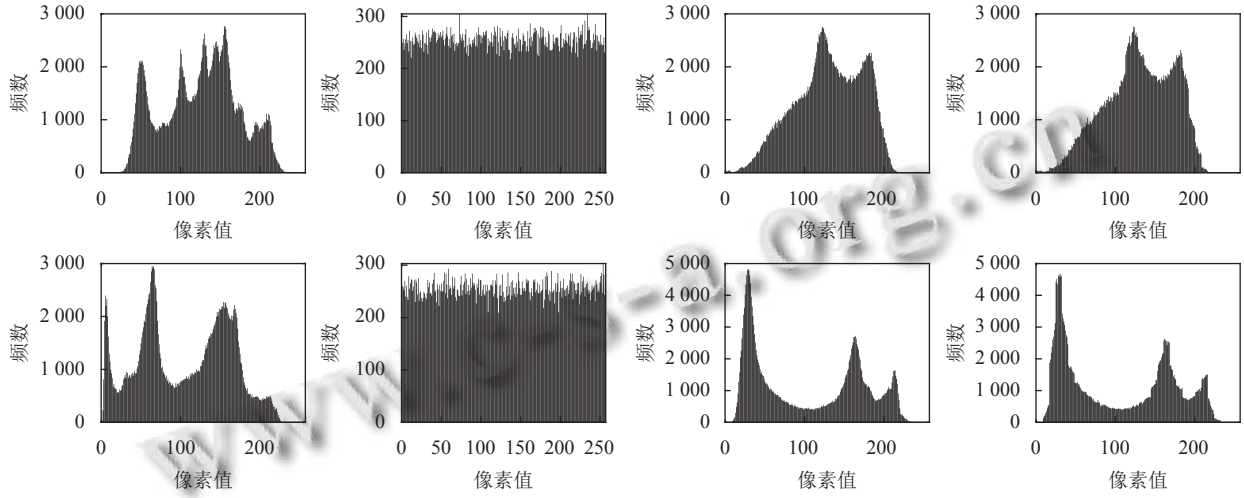
4.2.1 穷举攻击分析

密钥空间和密钥敏感性是抵御穷举攻击的两个重要评估指标. 在本文所提出的视觉安全加密算法中, 混沌系统被应用于加密过程的各个阶段, 包括并行压缩、双向扩散加密以及随机嵌入. 由于混沌序列对初始状态极度敏感, 因此所提加密算法具有相当高的密钥敏感性. 其他方面, 将所采用的两个混沌系统的初始状态作为外部密钥, 则在双精度数据类型的条件下, 本算法总的密钥空间约为10^{120}, 远远大于标准理论值[1], 即2^{100}. 值得一提的是, 其他的一些参数, 如m_0, m_1, d以及量化参数P_{max}和P_{min}, 均可以作为密钥以提升算法在抵抗穷举攻击方面的能力.

4.2.2 统计攻击分析

直方图反映在自然图像中像素值的分布比例. 接下来, 将分辨率均为512×512的两张明文图像 (Lena 和 Peppers) 和两张载体图像 (Baboon 和 Sailboat) 分别单独地传入所提加密算法进行统计分析实验, 其实验结果绘制在图 6 中. 首先, 从图中可以看出, 生成的中间秘密图像的像素值分布近似均匀, 表明明文图像的统计特征信息得到有效的隐藏, 同时也防止在加密的

第 2 阶段中嵌入信息不对称的漏洞. 其次, 明文图像的直方图与对应的载体图像的直方图极为相似, 同时在第 4.1 节中也给出了这两者之间的定量数值结果, 即 43.949 0 dB 和 0.995 0. 另外, 相比于现有的非视觉安全的图像加密而言, 本文所提加密算法从两个方面来抵抗统计分析攻击. 其一是通过压缩加密和双向扩散操作来消除明文特有的统计信息, 其次是采用隐写编码方法来隐藏加密的统计信息. 通过上述分析可知, 所本文介绍的图像加密算法具有不错的抗统计分析的性能.



(a) 明文图像的直方图 (b) 中间秘密图像的直方图 (c) 载体图像的直方图 (d) 密文图像的直方图

图 6 统计攻击分析的实验结果

4.2.3 差分攻击分析

差分分析是一种常用且可行的攻击方法. 密码分析者首先构造出多个特殊的明文图像并单独地对它们进行加密, 然后通过分析多个明文-密文对之间的关系, 以推导出加密方案所采用的密码流. 接下来, 采用像素变化率 (number of pixels change rate, NPCR) 和归一化平均变化强度 (unified average changing intensity, UACI)[27] 等评估指标来定量衡量本文提出的加密算法在抵抗差分攻击方面的能力. 本实验的数值结果如表 1 所示. 值得一提的是, 由于本算法所产生的密文图像具有视觉安全性. 因此, 在实验前须将嵌入阶段移除. 从实验结果数据来看, NPCR 和 UACI 值接近文献 [15] 给出的理论值, 即 99.59% 和 33.55%, 且相比于文献 [1,11] 具有更大的指标值, 表明本文介绍的加密算法具有不错的抵御差分攻击的能力.

4.3 健壮性分析

视觉安全的密文图像在传输信道中传输时, 不可避免地会遭到噪声的污染或数据丢包. 接下来, 为模拟出这两种攻击的效果, 人为地在密文图像中分别单独地添加30×30的掩模块, 不同强度的盐椒噪声和斑点噪声. 实验结果如图 7 所示. 可以清楚地看到, 在不同强度的噪声和剪切攻击干扰下, 解密图像在视觉上仍具有一定的语义和可读性, 并且所提算法在抗椒盐噪声攻击方面具有很好的抵御能力. 此外, 由于本文介绍的加密算法具有强大的雪崩效应, 即当密文图像中的某一像素值发生细微变化时, 所产生的误差会逐步扩散到整个解密图像中, 这可以看作是对追求极高安全性的一种让步.

表 1 抗差分攻击分析的实验结果 (%)

加密方案	Lena			Pepper			Woman		Girlface	
	本文	文献[1]	文献[11]	本文	文献[1]	文献[11]	本文	文献[11]	本文	文献[11]
NPCR	99.61	99.43	99.51	99.64	99.37	99.42	99.61	99.60	99.60	99.62
UACI	33.14	33.09	33.12	33.10	33.02	33.10	33.70	33.69	33.72	33.53

4.4 时间复杂度分析

加密算法的时间复杂度在很大程度上决定了其本身的执行效率[27]. 针对分辨率均为$N\times N$的明文图像和载体图像. 首先, 在密码流的构造阶段, 利用$\Theta\left((d\cdot C_R+1)N^2\right)$

的时间复杂度来对新设计的分段混沌映射和四维超混沌 Qi 系统进行迭代, 生成混沌序列 (符号 C_R 为预设的压缩率). 在 PTP-CS 阶段, 二维 Arnold 置乱操作所消耗的时间复杂度为$\Theta\left(N^2\right)$. 其次, 在加密阶段中, 压缩图像进行双向的扩散操作共占用时间复杂度$\Theta\left(2N^2\right)$. 最后, 将秘密图像随机地嵌入非涉密传输介质中, 而这部分操作所占用的时间复杂度为$\Theta\left(4C_R \cdot N^2\right)$. 因此, 本文所提加密算法总的时间复杂度为$\Theta(((d+4)\cdot C_R+4)N^2)$.

(a) 原始解密图像 (b) 30×30 剪切块 (c) 0.1%椒盐噪声强度 (d) 0.000 23%斑点噪声强度

图 7 健壮性分析的实验结果

就分辨率为512×512的明文图像“Lena”而言, 其加密过程中, 各个部分所消耗的时间占总加密时间的百分比如图 8 所示. 可以看出, 密码流生成阶段与嵌入阶段占据约 90% 的总时间. 因此, 本文建议以分块的形式对明文图像进行加密处理以提高运行速度. 首先, 分块操作可以大大减少混沌映射的迭代次数, 便于在加密过程中同步处理图像的各个子块. 其次, 这种处理手段有助于提高凸优化重建算法的收敛速度.

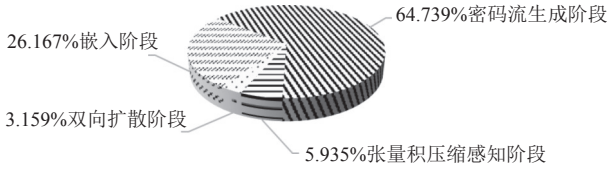


图 8 每部分所消耗的时间占总加密时间的百分比

4.5 算法对比

为了突出本文所介绍的隐私图像加密算法的优越性, 本小节将从视觉安全性、重建质量等两个方面把本文所提算法与其他先进的加密算法进行对比实验, 所得到的数值结果如表 2 和表 3 所示.

对于视觉安全的加密算法而言, 载体图像与密文图像之间的 PSNR 和 MSSIM 值越大, 表明其视觉安全性越好. 表 2 列出了几种视觉有意义图像加密算法的视觉安全性对比实验的数值结果. 从得到的数据来看, 本文提出的加密算法所生成的密文图像具有最好的视觉质量. 相比文献 [11] 中所介绍的加密算法, 视觉安全性提高近 8.5 dB. 同时, 也说明基于矩阵编码的信息嵌入技术对载体图像原始特征信息的损害较小.

表 2 不同加密算法中的视觉安全性对比实验的结果

明文图像	宿主图像	文献[28]		文献[11]		文献[29]		本文	
		PSNR (dB)	MSSIM	PSNR (dB)	MSSIM	PSNR (dB)	MSSIM	PSNR (dB)	MSSIM
Lena	Peppers	35.1347	—	32.3513	0.9257	40.9115	0.9917	**43.8992**	**0.9918**
Jet	Baboon	36.4906	—	37.8967	0.9833	40.9286	0.9967	**43.9296**	**0.9967**

表 3 不同解密算法中的重建质量对比实验的结果 (dB)

明文图像	文献[30]	文献[31]	文献[29]	文献[15]	文献[32]	本文
Lena	28.5000	31.4240	35.3992	31.7986	33.2086	**37.1110**
Pepper	28.0000	30.6809	34.7013	30.6483	32.7140	**36.1479**

在本文所提出的方案中, 将从以下两个方面来提高解密图像的重构质量. 首先, 在 PTP-CS 模型中, 通过对明文系数矩阵进行阿诺德置乱, 可以有效缓解测量矩阵的有限等距性质的限制, 从而提高重构图像的质量[13]. 其次, 采用完全可逆的编码嵌入方法来消除截断损失. 在不同解密算法中, 从密文图像中恢复出的解密图像的重构质量如表 3 所示. 可以看出, 与其他压缩加密算法相比, 本文提出的算法具有更好的压缩性能.

5 结论与展望

针对公用信道中的敏感明文数据, 本文基于张量积压缩感知模型、混沌理论和数字隐写编码嵌入提出了一种具有视觉安全性的加密算法以实现对明文图像的同步加密和隐写. 在本项工作中, 在新提出的分段混沌映射和超混沌 Qi 系统的共同控制下, PTP-CS 模型和二维阿诺德置乱策略可以有效地提升所提算法的压缩性能. 同时, 所采用的编码嵌入方法保证了类噪声秘密数据的高度不可感知性. 最后, 仿真实验的数值结果和综合分析表明所提出的加密算法具有足够的安全性以够抵御常见的多种攻击. 下一步工作, 将对循环生成对抗网络模型 (cycle generative adversarial network model, cycle GAN) 进行研究并将其引入到图像加密领域.

参考文献

1 蒋东华, 刘立东, 王兴元, 等. 基于细胞神经网络和并行压缩感知的图像加密算法. 图学学报, 2021, 42(6): 891–898.

2 陈森, 薛伟. 基于混沌系统和人工神经网络的图像加密算法. 计算机系统应用, 2020, 29(8): 236–241. [doi: 10.15888/j.cnki.csa.007578]

3 Abd-El-Atty B, Iliyasu AM, Alanezi A, *et al*. Optical image encryption based on quantum walks. Optics and Lasers in Engineering, 2021, 138: 106403. [doi: 10.1016/j.optlaseng.2020.106403]

4 Khan JS, Kayhan SK. Chaos and compressive sensing based novel image encryption scheme. Journal of Information Security and Applications, 2021, 58: 102711. [doi: 10.1016/j.jisa.2020.102711]

5 蒋东华, 朱礼亚, 沈子懿, 等. 结合二维压缩感知和混沌映射的双图像视觉安全加密算法. 西安交通大学学报, 2022, 56(2): 139–148. [doi: 10.7652/xjtuxb202202015]

6 梁晏慧, 李国东. 基于分数阶超混沌的混沌细胞自动机图像加密算法. 计算机科学, 2019, 46(S2): 502–506.

7 徐锡统, 陈圣波, 于岩. 结合小波包变换与混沌神经元的遥感图像加密. 遥感信息, 2021, 36(4): 76–83. [doi: 10.3969/j.issn.1000-3177.2021.04.011]

8 Wang Y, Li XW, Wang QH. Integral imaging based optical image encryption using CA-DNA algorithm. IEEE Photonics Journal, 2021, 13(2): 7900812.

9 Jeevitha S, Prabha NA. Novel medical image encryption using DWT block-based scrambling and edge maps. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(3): 3373–3388. [doi: 10.1007/s12652-020-02399-9]

10 Bao L, Zhou YC. Image encryption: Generating visually meaningful encrypted images. Information Sciences, 2015, 324: 197–207. [doi: 10.1016/j.ins.2015.06.049]

11 Wang H, Xiao D, Li M, *et al*. A visually secure image encryption scheme based on parallel compressive sensing. Signal Processing, 2019, 155: 218–232. [doi: 10.1016/j.sigpro.2018.10.001]

12 Chai XL, Wu HY, Gan ZH, *et al*. An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing. Information Sciences, 2021, 556: 305–340. [doi: 10.1016/j.ins.2020.10.007]

13 朱礼亚, 张曦, 张亮. 基于并行压缩感知与混沌映射的图像加密方案设计. 微电子学与计算机, 2019, 36(10): 96–102. [doi: 10.19304/j.cnki.issn1000-7180.2019.10.019]

14 Dou YQ, Li M. An image encryption algorithm based on a novel 1D chaotic map and compressive sensing. Multimedia Tools and Applications, 2021, 80(16): 24437–24454. [doi: 10.1007/s11042-021-10850-y]

15 Zhu LY, Song HS, Zhang X, *et al*. A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding. Signal Processing, 2020, 175: 107629. [doi: 10.1016/j.sigpro.2020.107629]

16 Musanna F, Dangwal D, Kumar S. A novel chaos-based approach in conjunction with MR-SVD and pairing function for generating visually meaningful cipher images. Multimedia Tools and Applications, 2020, 79(33): 25115–25142.

17 Tan ZY, Dong YX, Huang XL, *et al*. Visually meaningful image encryption scheme based on DWT and Schur decomposition. Security and Communication Networks, 2021, 2021: 6677325.

18 Jiang DH, Liu LD, Zhu LY, *et al*. Adaptive embedding: A novel meaningful image encryption scheme based on parallel compressive sensing and slant transform. Signal Processing, 2021, 188: 108220. [doi: 10.1016/j.sigpro.2021.108220]

19 Qi GY, van Wyk MA, van Wyk BJ, *et al*. A new hyperchaotic system and its circuit implementation. Chaos, Solitons & Fractals, 2009, 40(5): 2544–2549.

20 Peng HP, Mi YQ, Li LX, *et al*. *P*-tensor product in compressed sensing. IEEE Internet of Things Journal, 2019, 6(2): 3492–3511. [doi: 10.1109/JIOT.2018.2886841]

21 Hua ZY, Zhou YC, Huang HJ. Cosine-transform-based chaotic system for image encryption. Information Sciences, 2019, 480: 403–419. [doi: 10.1016/j.ins.2018.12.048]

22 Mansouri A, Wang XY. A novel one-dimensional chaotic map generator and its application in a new index

representation-based image encryption scheme. Information Sciences, 2021, 563: 91–110. [doi: 10.1016/j.ins.2021.02.022]

23 Mansouri A, Wang XY. A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme. Information Sciences, 2020, 520: 46–62. [doi: 10.1016/j.ins.2020.02.008]

24 Midoun MA, Wang XY, Talhaoui MZ. A sensitive dynamic mutual encryption system based on a new 1D chaotic map. Optics and Lasers in Engineering, 2021, 139: 106485. [doi: 10.1016/j.optlaseng.2020.106485]

25 Talhaoui MZ, Wang XY, Midoun MA. A new one-dimensional cosine polynomial chaotic map and its use in image encryption. The Visual Computer, 2021, 37(3): 541–551. [doi: 10.1007/s00371-020-01822-8]

26 罗玉玲, 欧阳雪, 曹绿晨, 等. 遗传模拟退火算法和混沌系统的图像加密方法. 西安电子科技大学学报, 2019, 46(5): 171–179. [doi: 10.19665/j.issn1001-2400.2019.05.024]

27 芮杰, 杭后俊. 基于超混沌系统的明文关联图像加密算法. 图学学报, 2020, 41(6): 917–921.

28 Ping P, Fu J, Mao YC, *et al*. Meaningful encryption: Generating visually meaningful encrypted images by compressive sensing and reversible color transformation. IEEE Access, 2019, 7: 170168–170184. [doi: 10.1109/ACCESS.2019.2955570]

29 Hua ZY, Zhang KY, Li YM, *et al*. Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing. Signal Processing, 2021, 183: 107998. [doi: 10.1016/j.sigpro.2021.107998]

30 Chen JX, Zhang Y, Qi L, *et al*. Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression. Optics & Laser Technology, 2018, 99: 238–248.

31 Gan ZH, Chai XL, Zhang JT, *et al*. An effective image compression-encryption scheme based on compressive sensing (CS) and game of life (GOL). Neural Computing and Applications, 2020, 32(17): 14113–14141. [doi: 10.1007/s00521-020-04808-8]

32 Jiang DH, Liu LD, Wang XY, *et al*. Image encryption algorithm for crowd data based on a new hyperchaotic system and Bernstein polynomial. IET Image Processing, 2021, 15(14): 3698–3717. [doi: 10.1049/ipr2.12237]

(校对责编: 孙君艳)