一种基于压缩感知和多维混沌系统的多过程图像加密方案*

石 航 1)6) 王丽丹 1)2)3)4)5)†

1) (非线性电路与智能信息处理重庆市重点实验室, 重庆 400715)

2) (西南大学电子信息工程学院, 重庆 400715)

3) (智能传动和控制技术联合工程实验室, 重庆 400715)

4) (类脑计算与智能控制重庆市重点实验室, 重庆 400715)

5) (重庆市脑科学协同创新中心, 重庆 400715)

6) (西南大学西塔学院, 重庆 400715)

(2019 年 4 月 16 日收到; 2019 年 7 月 15 日收到修改稿)

随着计算机科学的快速发展, 信息的存储和传播常常在各类计算机硬件以及多种网络之间进行, 传统的信息加密方案已逐渐不再适用. 因此, 基于计算机的信息加密算法近年来逐步成为研究热点. 通过结合小波包变换、压缩感知、混沌系统等理论, 一种基于压缩感知和多维混沌系统的多过程图像加密方案被提出. 该加密方案实现了针对灰度图像的压缩和加密及对应的解压、解密过程. 小波包变换理论被应用到图像的预处理阶段对原始图像进行小波包分解, 同时结合阈值处理方法对分解后所得的图像信号分量进行分类, 并在之后的处理过程中根据图像信号分量的特性对其有区分地进行压缩、加密或者保留. 在图像压缩阶段, 引入压缩感知算法克服传统采样定理采样成本高及重构质量偏低等弊端. 在图像加密阶段, 结合多类、多维度混沌系统对相关图像信号分量进行置乱. 最后, 应用压缩、加密以及小波包变换的逆过程实现对原始图像的完整重构. 仿真结果表明, 该图像加密方案在抵抗外界干扰时凭借算法鲁棒性有效地保护了密文图像的基本信息, 且在应对明文攻击等破解手段时不泄露任何有用信息. 此外, 经该加密方案加密后的密文图像的信息熵及相关系数等指标相比于参考文献中加密算法更加接近于理想值, 其加密性能有明显的提升.

关键词: 数字图像, 加密, 小波包变换, 压缩感知

PACS: 05.45.Ac, 05.45.Vx, 05.45.Gg **DOI:** 10.7498/aps.68.20190553

1 引 言

针对数字图像的加密方案往往要求密文图像在视觉效果上不能暴露明文图像的有效信息, 且相邻像素点间要具有极强的随机性, 因此, 数字图像加密方案往往会引入一些伪随机过程处理数字图像或使用一些伪随机序列对图像进行编码以达到加密的目的. 众所周知, 混沌映射与混沌系统具有初值敏感性以及不可预测性等特点, 将混沌理论运用到数字图像加密中能够得到相较于普通伪随机过程更大的密钥空间, 进而提高密文图像的安全

* 国家重点基础研究发展计划 (批准号: 2018YFB1306600)、国家自然科学基金 (批准号: 61571372, 61672436, 61601376)、重庆市基础科学与前沿技术研究专项重点项目 (批准号: cstc2017jcyjBX0050, cstc2016jcyjA0547) 和中央高校基本科研业务费 (批准号: XDJK2016A001, XDJK2017A005) 资助的课题.

† 通信作者. E-mail: ldwang@swu.edu.cn

性. 吴成茂[1]在离散 Arnold 映射的基础上进行改进并应用于图像的置乱加密; Lin 等[2]利用超混沌 Chen 系统提出了一种基于超混沌系统的图像加密算法; Li 等[3]通过结合二维 Logistic 系统与新二维离散系统提出一种能极大扩展密钥空间且增强安全性的图像加密方案. 这些研究成果充分说明了在数字图像加密方案引入混沌系统的可行性以及可靠性.

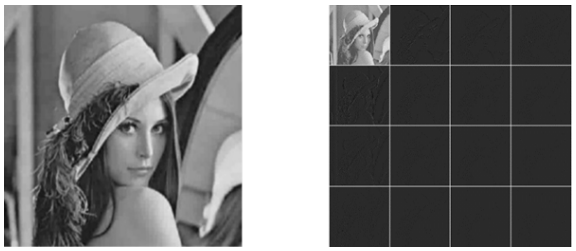
使用数字图像存储信息的缺陷在于其往往包含许多冗余的信息, 因此, 针对数字图像的处理方案一般会引入图像压缩算法以减少处理过程中的数据量以提高算法的执行效率, 但是传统的压缩算法在实际应用中往往存在采样成本高、重构质量低的缺陷, 对后续的图像处理造成了负面影响. 压缩感知 (compress sensing, CS) 作为一种新兴的压缩理论指出在被采样信号为稀疏信号的前提下, 可以通过远低于传统采样定理的采样率对信号进行采样和重构[4], 因此压缩感知理论非常适合运用在较为复杂的图像处理方案中. Chai 等[5]和 Zhu 等[6]在数字图像加密方案中引入了压缩感知理论, 实现了在较少数据量下对明文图像进行加密处理, 在极大地改善加密算法的执行效率的同时, 仍保证了加密方案的安全性.

本文提出了一种基于压缩感知和混沌系统的数字图像加密方案, 通过引入压缩感知理论, 对部分图像信号分量进行压缩处理, 减少了加密过程中需要处理的数据量, 降低了原始图像信息在处理过程中的损耗. 同时, 使用多维混沌系统对待加密的图像信号分量进行像素扩散、置乱, 利用多维混沌系统的随机性保证了密文图像的安全性. 该图像加密方案能够在改善算法执行效率的同时, 保证密文图像的可靠性.

2 一种新的基于压缩感知和混沌系统的图像加密方案

2.1 图像预处理: 基于小波包变换的图像分解法和自适应分类

在数字图像加密方案中, 小波包变换 (wavelet packet transform, WPT) 经常被运用在预处理阶段对明文图像进行分解进而得到不同的图像信号分量以消除一些对于后续处理步骤不利的负面因素及提高图像处理方案整体的运行效率. 本文采用离散二阶小波包变换对明文图像进行分解, 并对分解后的图像信号进行自适应分类处理以减少图像的冗余信息对图像处理效果的影响[7–9]. 以 Lena 图像为例, 其离散二阶小波包变换如图 1 所示.



(a) (b)

图 1 Lena 图像及其二阶小波包变换 (a) 原图; (b) 二阶小波包变换

Fig. 1. Lena and its second-order wavelet packet transformation: (a) Original Lena; (b) second order wavelet packet transformation of Lena.

图 1(b) 中左上角的信号分量包含了原始图像中的大部分能量, 因此, 该信号将作为图像加密处理的主体信号, 记为 S.

对于剩下的 15 个信号分量, 先对其进行阈值处理. 针对于每一个信号分量, 根据下列公式计算其均值 E:

$$E = \frac{1}{n}\sum_{i=1}^{n}|x_i|\,, \tag{1}$$

其中 x_i 为信号分量矩阵的其中一个元素, n 为一个信号分量矩阵所包含的元素个数.

在得到这 15 个信号分量的均值后, 选择最大的一个均值 $E_{\max}$, 再结合下列公式对这 15 个信号分量矩阵中的元素进行阈值处理:

$$x_i = \begin{cases} x_i, & |x_i| \geqslant E_{\max}, \\ 0, & |x_i| < E_{\max}. \end{cases} \tag{2}$$

完成图像信号分量的阈值处理后, 再次计算每一个信号分量的均值 E_i', 除此之外, 针对每个信号分量计算其信息熵 (香农熵, Shannon entropies) SE_i,再结合图 2 所示的算法对剩余的 15 个信号分量进行分类处理 (E表示经阈值处理后除 S 信号以外的所有信号分量像素值的均值).

图 2 中, Z_i 信号表示均值为 0 的图像信号分量, 该类分量没有存储原始图像任何有用的信息, 在后续处理过程中不会涉及, 可直接丢弃; O_i 信号代表均值小于 E'的图像信号分量, 这部分信号存

储了原始图像的部分有效信息量, 为保证对原始图像的完美的重构, 在后续处理过程中需保留该部分信号, 但不做任何处理; C_i 信号作为第四类图像信号分量, 其相比于 O_i 信号包含了原始图像更多的有效信息. 因此, 考虑对 C_i 信号采用压缩感知算法进行压缩处理以减少后续处理过程中的数据量, 进而提高加密方案整体的运行效率.

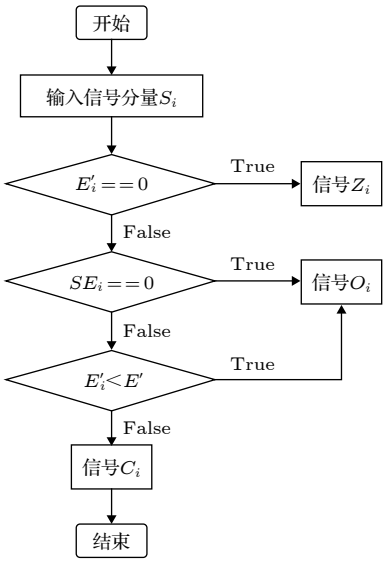


图 2 分类算法流程图

Fig. 2. Flow chart of classification algorithm.

对于 Lena 图像而言, 在对其 16 个图像信号分量进行阈值处理分类后, 得到了 1 个 S 信号, 0 个 Z_i 信号, 7 个 O_i 信号, 8 个 C_i 信号.

2.2 一种新的基于压缩感知和多维混沌系统的图像加密方案

2.2.1 基于压缩感知的图像压缩算法

本节主要针对 2.1 节中得到的 8 个 C_i 图像信号分量进行压缩处理[10–12]. 前文中已经说明压缩感知理论应用的前提在于待压缩信号是稀疏信号, 对于图像信号而言, 其 0 像素点的个数可以简单地反映其稀疏度, 现对 8 个 C_i 信号中的 0 像素点个数及占比进行考察, 结果列于如表 1.

由表 1 中 0 像素点占比一列可知, 8 个 C_i 信号中 0 像素点占比最低为 8.03%, 最高为 22.39%, 因此可以认为这 8 个 C_i 信号是稀疏的, 可以直接进行压缩感知的随机亚采样操作.

本文采用高斯随机矩阵作为对 C_i 信号进行随机亚采样的测量矩阵, 在后续针对压缩信号的重构过程中, 应用正交匹配追踪算法 (orthogonal matching pursuit, OMP) 作为重构算法对已压缩的信号分量进行重构, 最终得到与 C_i 信号等数量、等尺寸的解压信号 DC_i.

表 1 Lena 图像 C_i 信号分量 0 像素点的个数及占比

Table 1. The number and proportion of 0 pixels in C_i signals in Lena.

信号分量	0像素点个数	0像素点占比/%
C_1	329	8.03
C_2	554	13.53
C_3	703	17.16
C_4	682	16.65
C_5	436	10.64
C_6	917	22.39
C_7	842	20.56
C_8	789	19.26

2.2.2 基于多维混沌系统的图像加密算法

置乱过程单一的图像加密算法往往具有密文图像的安全性较差的缺陷, 进而无法对明文图像的信息进行有效的保护. 本文在一般的单次置乱图像加密算法的基础上, 引入了二次置乱加密以保证加密算法的安全性. 其中, 一次置乱加密算法的流程图如图 3 所示.

引入如 (3) 式所示的四阶 Colpitts 混沌系统[13] 作为图 3 中的混沌系统 1, 取系统初值为 [0.01, 0.02, 0.03, 0.04].

$$\begin{cases} \dot{x} = \alpha_1 (-x + y - \dot{z}) - \beta_F f(y) + \alpha_2, \\ \dot{y} = \beta_1 (x + z) - \beta_2 y - \beta_4, \\ \dot{z} = \gamma_1 (-x + y - z) - \gamma_2 w + \gamma_3, \\ \dot{w} = \delta z, \end{cases} \tag{3}$$

式中, $\alpha_1 = 2.86$, $\alpha_2 = 19.0$, $\beta_F = 200$, $\beta_1 = 2.86$, $\beta_2 = 3.11$, $\beta_3 = 1$, $\beta_4 = 17.38$, $\gamma_1 = 57.14$, $\gamma_2 = 20.0$, $\gamma_3 = 381$, $\delta = 5.48$; $f(y) = 0.5(y - 1 + |y + 1|)$ 为非线性函数.

对 Colpitts 混沌系统进行一段时间的迭代后共可得到四组等长的伪随机序列 x_i, y_i, z_i, w_i[14], 随机选取其中的三组混沌序列在某个随机时刻的取值 x_t, y_t, z_t, 将这三个随机数的值限制在区间 [0.01 0.1] 内得到初始密钥 $[x_0, y_0, z_0]$. 此时引入如 (4) 式所示的三阶 Chen 混沌系统[15] 作为图 3中的混沌

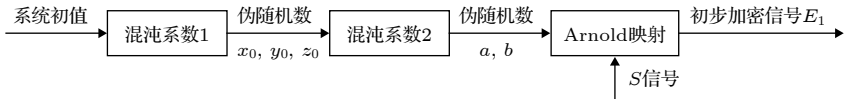


图 3 一次置乱加密流程图

Fig. 3. One scrambling encryption algorithm flow chart.

系统 2, 其系统初值即为 $[x_0, y_0, z_0]$.

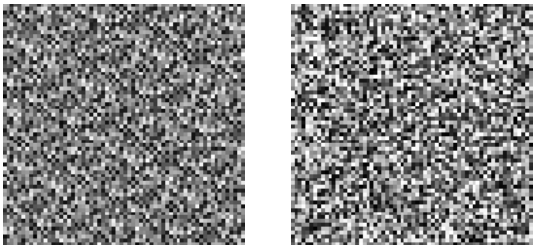
$$\begin{cases} \dot{x} = \alpha\left[\dot{y} - f(x)\right], \\ \dot{y} = x - y + z, \\ \dot{z} = -\beta y, \end{cases} \tag{4}$$

式中, $\alpha = 10$, $\beta = 15$, $m_0 = -1/7$, $m_1 = 2/7$, $f(x)=m_1x+0.5(m_0-m_1)(|x+1|+|x-1|)$ 为三段非线性函数.

对 Chen 系统进行一段时间的迭代得到三组等长的伪随机序列 x_i, y_i, z_i, 在这三组伪随机序列中随机选取两个数取整后得到 a, b, 代入如 (5) 式所示的数字化 Arnold 映射中:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod}N)+1. \tag{5}$$

在人为指定映射迭代的次数后 (一般为 2—3 次), 根据 (5) 式对 S 信号进行错切变换及切割回填操作实现对 S 信号的初步加密, 得到初步加密信号 E_1, 如图 4(a) 所示.



(a) (b)

图 4 S 信号的密文图像 (a) 一次置乱密文图像; (b) 二次置乱密文图像

Fig. 4. Ciphertext image of the S signal: (a) Scrambling ciphertext image once; (b) secondary scrambling ciphertext image.

在完成 S 信号的一次置乱加密后, 根据如图 5 所示的二次置乱加密流程图对 S 信号进行二次置乱加密.

其中, 密钥流 k 由下列公式计算得到:

$$\begin{aligned} k_{3(i-1)+1} &= \left(|x_i - [x_i]| \times 10^{14}\right) \bmod 256, \\ k_{3(i-1)+2} &= \left(|y_i - [y_i]| \times 10^{14}\right) \bmod 256, \\ k_{3(i-1)+3} &= \left(|z_i - [z_i]| \times 10^{14}\right) \bmod 256, \end{aligned} \tag{6}$$

式中 $[x_i]$ 表示对 x_i 进行向下取整操作. 通过该加密算法所得的密文图像 E_2 如图 4(b) 所示, 可以看到其在视觉效果上较好地实现了隐藏明文图像信息的功能. 该加密算法的性能将在下一节的算法性能分析中进行讨论, 其对应的解密过程为加密过程的逆运算.

2.2.3 图像重构: 基于小波包变换的逆运算

针对原始图像的重构需结合未经处理的图像信号分量以及经压缩、加密算法处理后的各类图像信号分量, 图像的重构过程如图 6 所示.

对于 Lena 图像, 由于其经小波包变换后的图像信号分量不包含 Z_i 信号, 因此, 其重构过程中只需结合解密后的图像信号分量, 解压后的图像信号分量以及 O_i 图像信号分量进行二阶离散逆小波包变换即可实现可对 Lena 图像的完全重构, Lena 图像与其重构图像如图 7 所示.

为方便之后对算法性能进行对比分析, 本文还对除 Lena 图像以外的 2 幅图像进行了相同的操作, 结果如图 8 所示.

3 算法性能分析

3.1 密钥空间分析

对于一种加密算法而言, 密钥空间是其加密性能的一种直观的体现, 一般情况下, 密钥空间范围越大的加密算法, 在应对蛮力攻击等非法解密手段时往往能够表现出良好的抵御性能. 本文中所使用的加密算法在保证混沌系统始终位于混沌状态的前提下, 利用 4 阶 Colpitts 超混沌系统产生 Chen 系统的控制参数 c 及初始值 x_0, y_0, z_0, 虽然数字仿

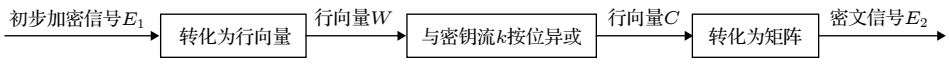


图 5 S 信号二次置乱加密流程图

Fig. 5. Secondary scrambling encryption flow chart of S signal.

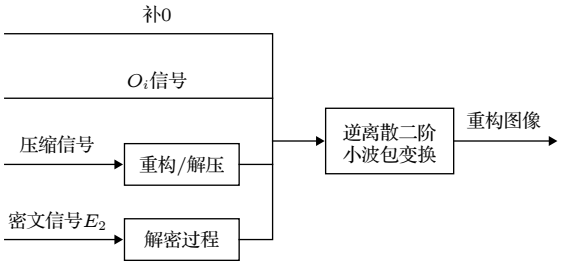


图 6 图像重构流程图

Fig. 6. Image reconstruction flow chart.

图 7 Lena 图像的明文图像、重构图像 (a) 原始图像; (b) Lena 重构图像

Fig. 7. Original, reconstructed image of Lena: (a) Original image; (b) reconstructed image.

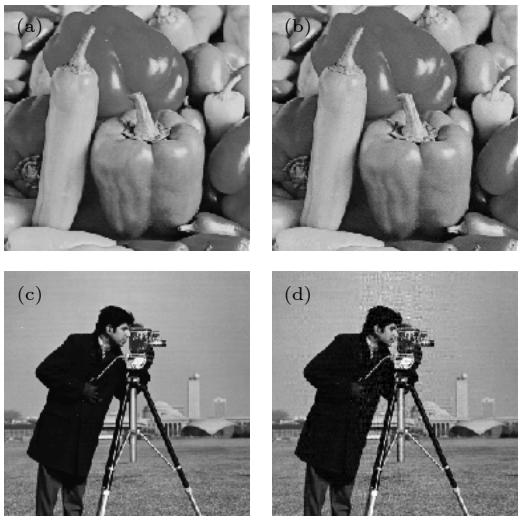


图 8 更多加密方案运行实例 (a) Pepper 原始图像; (b) Pepper 重构图像; (c) Cameraman 原始图像; (d) Cameraman 重构图像

Fig. 8. More encryption scheme running examples: (a) Original image of Pepper; (b) reconstructed image of Pepper; (c) original image of Cameraman; (d) reconstructed image of Cameraman.

真降低了混沌系统的随机性, 但是作为 4 阶超混沌系统, 它在足够的计算精度下同样具有较大范围的密钥空间. 同时, 当 Colpitts 混沌系统的控制参数及初始值发生变化时, Chen 系统的控制参数及初始值也会相应地发生变化, 故之后用于图像加密的密钥流也会发生变换. 除此之外, Colpitts 系统的迭代次数也会影响 Chen 系统密钥流的产生. 因此, 本文加密算法的密钥空间是比较广泛的, 蛮力攻击无法实现对被加密图像的有效解密.

3.2 相关性分析

在密码学中, 混淆 (confusion) 与扩散 (diffusion) 是加密文件的两种主要方法. 对于一般的数字图像, 其相邻像素点之间会表现出很高的相关性, 然而, 对于一幅理想的密文图像, 其相邻像素点之间应该不具有任何相关性, 即各方向上相邻像素点间的相关系数为 0. 因此, 密文图像在各方向上相邻像素点间的相关系数可以作为评价一个图像加密算法优劣的重要指标.

一般在水平方向、垂直方向和斜线方向来计算一幅数字图像相邻像素点间的相关系数, 相关系数 R 的计算公式如下:

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{7}$$

其中, $D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2$表示序列 x 的方差 (variance), $\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))\times(y_i-E(y))$表示 x, y 的协方差, $E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i$ 表示序列 x 的均值.

表 2 列出了本文所使用的三幅图像的 S 信号在加密前后在三个方向上的相关系数. 此外, 表 2 中还列出了参考文献 [16,17] 中的明文图像 (S 信号)、密文图像对应的三个方向上的相关系数作为对比. 其中, 每一项绝对值最小的相关系数已用蓝色粗体标出.

此外, 为更加直观地表示数字图像相邻像素点间的相关性, 本文引入了数字图像的相关性分布图, Lena, Pepper, Cameraman 的明文图像 (S 信号)、密文图像在三个方向上的相关性分布图如图 9—图 11 所示.

结合表 2 中数据及相关性分布图可知, 经由本文加密算法得到的密文图像的像素点在三个方向上均近似地表现为随机分布, 有效地对明文图像进行了置乱. 同时, 比较由本文算法与参考文献 [16,17] 的算法得到的密文图像的相关系数, 由表 2 中的数据可以直观地看到, 本文的加密算法相较于参考文献 [16,17] 中的加密算法使得图像的像素点更趋近于理想的随机分布, 增强了保密性.

表 2 比较不同加密方案的相关系数

Table 2. Comparisons for the correlation coefficients of different encryption scheme.

图像	明文图像			密文图像		
	水平	竖直	斜线	水平	竖直	斜线
Lena (本文)	0.9189	0.7339	0.8097	**–0.0002**	**–0.0004**	**0.0001**
Lena[16]	0.9180	0.7345	0.8083	0.0032	0.0025	–0.0173
Lena[17]	0.9151	0.8097	0.7484	–0.0274	0.0051	–0.0117
Pepper (本文)	0.8849	0.7567	0.8323	**–0.0003**	**–0.0004**	**0.0003**
Pepper[16]	0.8827	0.8374	0.7482	0.0210	0.0010	0.0071
Pepper[17]	0.8864	0.8398	0.7466	0.0070	–0.0198	–0.0228
Cameraman (本文)	0.9275	0.8364	0.8866	**0.0004**	**0.0001**	**0.0002**
Cameraman [16]	0.9339	0.8898	0.8459	–0.0035	–0.0014	0.0159
Cameraman[17]	0.9280	0.8835	0.8411	0.0277	0.0141	0.0281

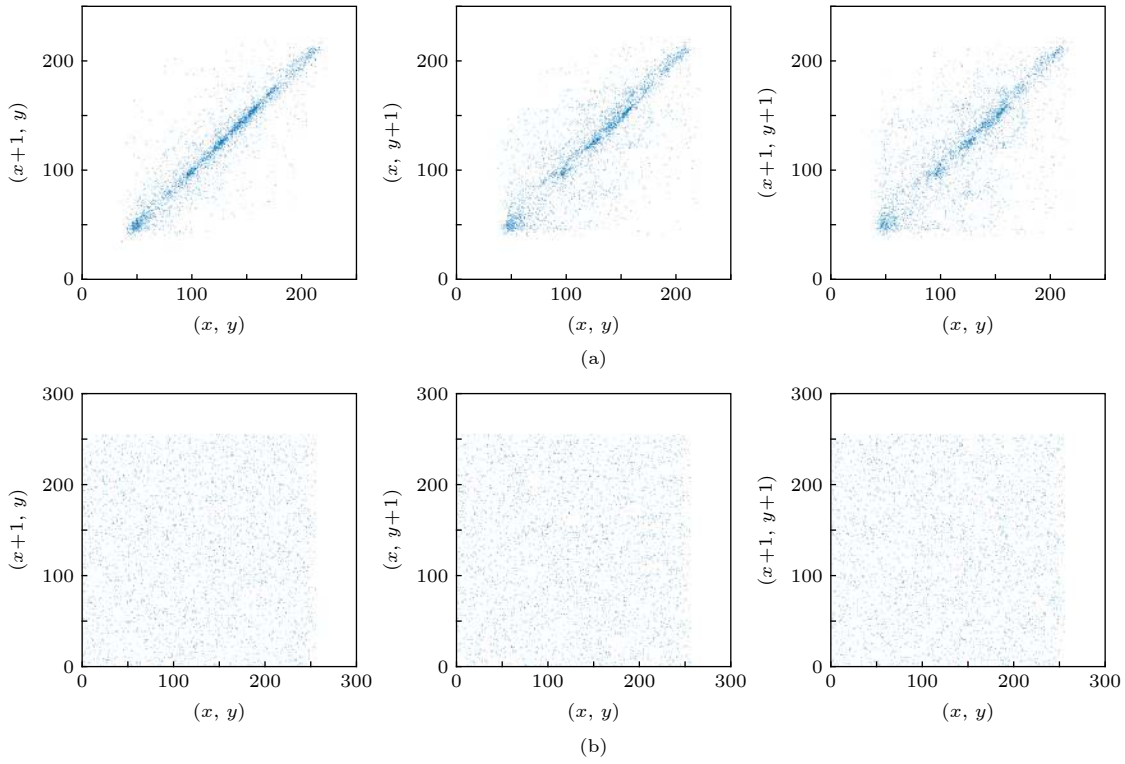


图 9 Lena 图像的明文 (S 信号)、密文图像在水平、竖直、斜线三个方向的相关分布图 (a) 明文图像相关分布图; (b) S 信号的密文图像相关分布图

Fig. 9. Correlation distribution of plaintext, ciphertext image in horizontal, vertical and oblique directions of S signal of Lena: (a) Correlation distribution of plaintext of S signal; (b) correlation distribution of ciphertext of S signal.

3.3 信息熵分析

信息熵反映了一幅数字图像所包含的信息的不确定性. 对于一幅数字图像而言, 其信息熵越大, 表示其所包含的信息的不确定性越大, 数字图像的信息熵的定义式如下:

$$IE = -\sum_{i=0}^{L} p(i)\log_2 p(i), \tag{8}$$

其中, L 表示一幅图像的灰度等级, $p(i)$ 表示灰度值 i 出现的概率. 对于一幅灰度等级 $L = 256$ 的密文图像而言, IE 的理论值为 8, 在这种情况下, 该密文图像在未经解密的情况下将不会泄露任何有用信息. 表 3 记录了三种加密方案下三幅图像的明文图像 (S 信号)、密文图像的信息熵, 每幅密文图像对应的最大信息熵已用蓝色粗体标出.

观察表 3 中的数据 ("—"表示相同数值), 三种

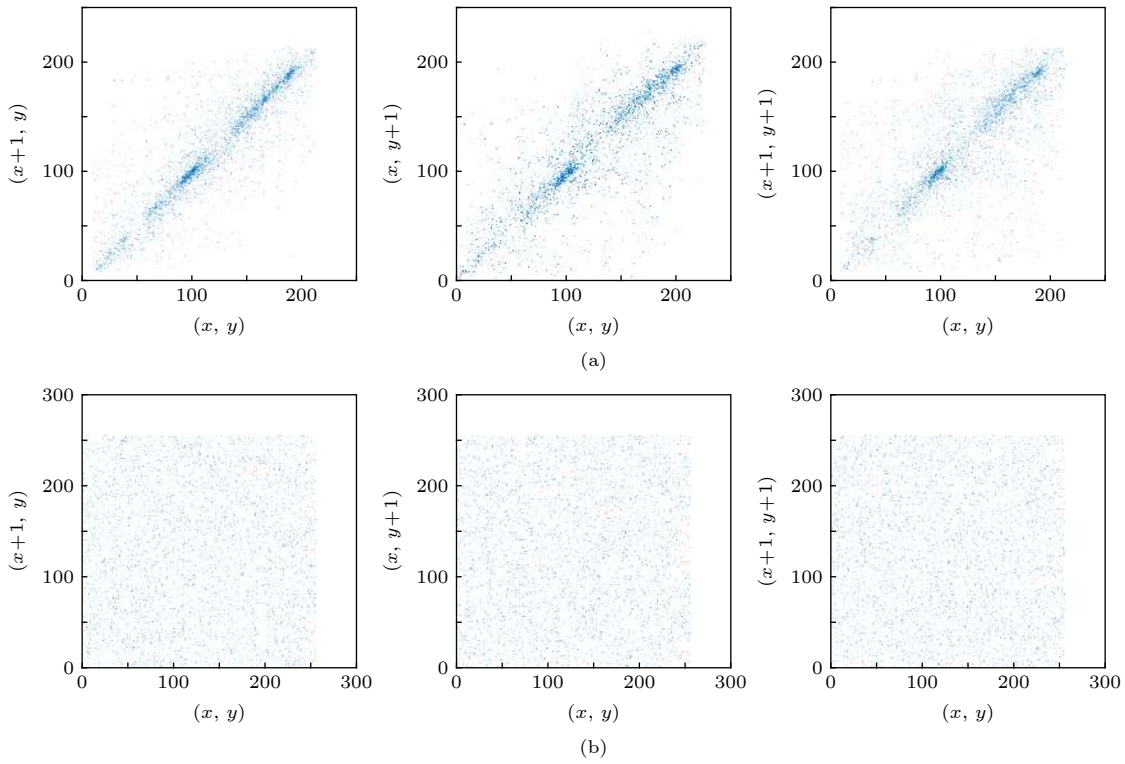


图 10 Pepper 图像的明文 (S 信号)、密文图像在水平、竖直、斜线三个方向的相关分布图 (a) 明文图像相关分布图; (b) S 信号的密文图像相关分布图

Fig. 10. Correlation distribution of plaintext, ciphertext image in horizontal, vertical and oblique directions of S signal of Pepper: (a) Correlation distribution of plaintext of S signal; (b) correlation distribution of ciphertext of S signal.

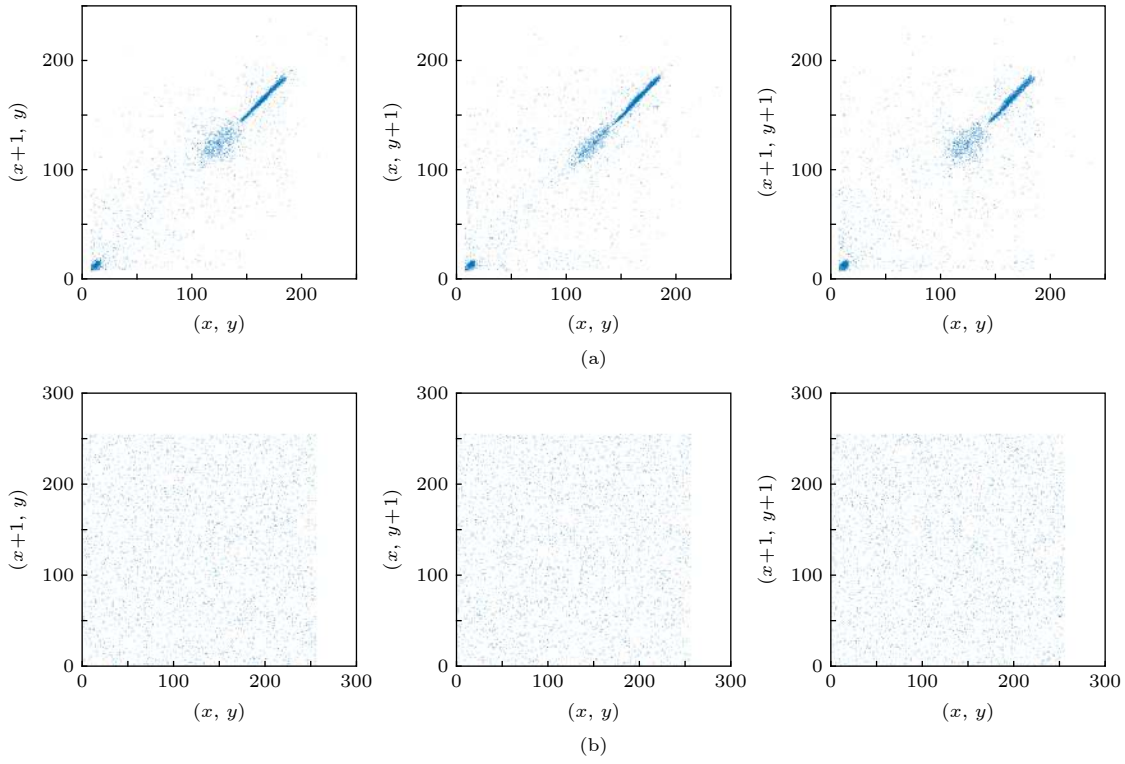


图 11 Cameraman 图像的明文 (S 信号)、密文图像在水平、竖直、斜线三个方向的相关分布图 (a) 明文图像相关分布图; (b) S 信号的密文图像相关分布图

Fig. 11. Correlation distribution of plaintext, ciphertext image in horizontal, vertical and oblique directions of S signal of Cameraman: (a) Correlation distribution of plaintext of S signal; (b) correlation distribution of ciphertext of S signal.

加密方案下密文图像的信息熵均接近理想值 8, 本文所提出的加密算法在加密 Lena, Pepper 的 S 信号时均得到了最大的信息熵值. 此外, Cameraman 的 S 信号经由本文加密算法处理得到的密文图像的信息熵数值也是十分接近最大值的. 因此, 可以认为本文的加密方案能够较好地对明文图像 (S 信号) 的像素点进行置乱, 掩盖明文图像信息.

表 3 比较不同加密方案的信息熵

Table 3. Comparisons for the entropy of different encryption scheme.

加密方案	明文图像	密文图像
Lena (本文)	7.3035	**7.9544**
Lena[16]	—	7.9642
Lena[17]	—	7.9531
Pepper (本文)	7.4344	**7.9633**
Pepper[16]	—	7.9586
Pepper[17]	—	7.9543
Cameraman (本文)	6.9571	7.9554
Cameraman[16]	—	**7.9636**
Cameraman[17]	—	7.9538

3.4 直方图分析

灰度直方图 (histogram) 是灰度级的函数, 它表示图像中具有每种灰度级的像素的个数, 反映图像中每种灰度出现的频率[18]. 一般而言, 灰度直方图的横坐标是灰度级, 纵坐标是该灰度级出现的频率, 它是图像的最基本的统计特征[7]. 本节将基于图像的 S 信号对应的明文、密文的直方图, 对本文的加密算法进行评价, 各图像对应的灰度直方图如图 12 所示.

观察图 12 可以发现, 本文的加密算法对明文图像的灰度分布进行了一个较好的均衡过程, 使得密文图像的灰度值比较均匀地分布于整个灰度值区间上, 隐藏了明文图像的灰度分布特性.

3.5 差分攻击分析[19]

差分攻击分析是密码分析领域最常用的一种破译手段, 这种方法通过对明文进行轻微修改以获得相应的密文, 并通过修改后的密文与原密文之间的差异联系来破译密码系统. 本节中通过引入像素改变率 (number of pixel change rate, NPCR)、一

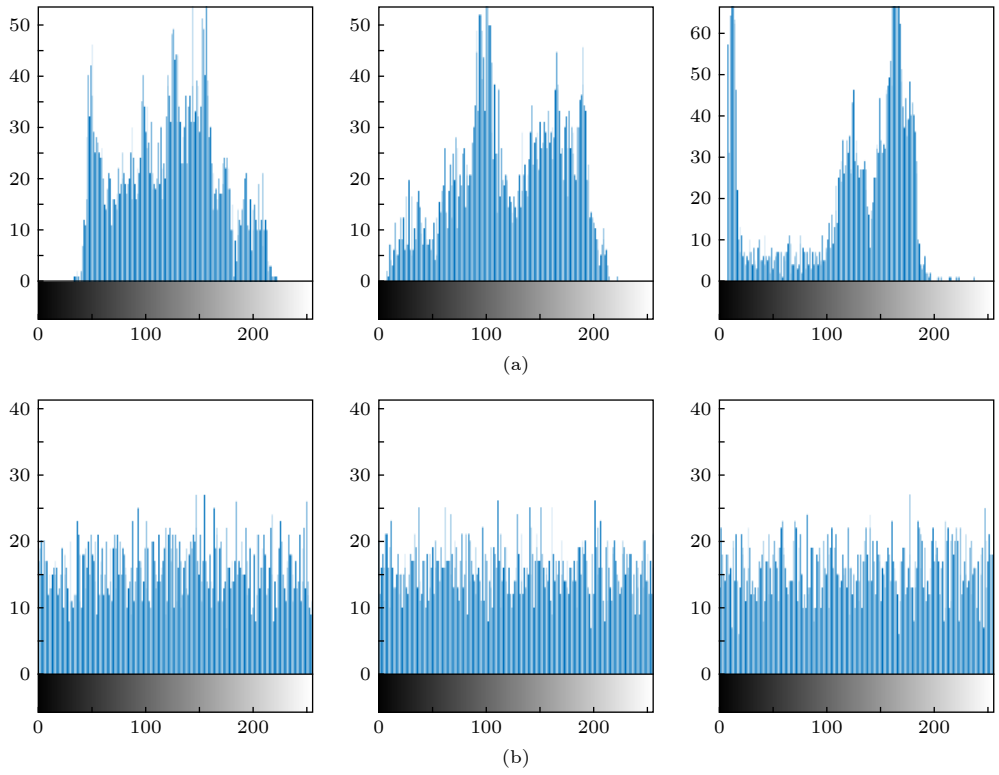


图 12 Lena, Pepper, Cameraman 图像的 S 信号的明文、密文的灰度直方图 (a) S 信号的明文灰度直方图; (b) S 信号的密文图像相关分布图

Fig. 12. Gray histogram of plaintext and ciphertext of S signal of Lena, Pepper, Cameraman: (a) Gray histogram of plaintext of S signal; (b) gray histogram of plaintext of ciphertext of S signal.

致平均改变密度 (unified average changing intensity, UACI)、块平均改变密度 (block average changing intensity, BACI) 等三个指标定量分析加密方案抵抗差分攻击的性能.

设 P_1, P_2 是两幅仅有一位像素点不同的密文图像, 定义密文图像 P_1, P_2 的 NPCR 如下:

$$\begin{aligned}&\mathrm{NPCR}\left(P_1,P_2\right)\\&=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(\left|\mathrm{Sign}\left(P_1\left(i,j\right)\right)-P_2\left(i,j\right)\right|\times 100\%\right),\end{aligned}\tag{9}$$

其中 $P_1(i, j)$ 为密文图像 P_1 中位置 (i, j) 处的像素值, $P_2(i, j)$ 为密文图像 P_1 中位置 (i, j) 处的像素值, Sign$(\cdot)$ 为符号函数, 其函数表达式如下:

$$\mathrm{Sign}\left(x\right)=\begin{cases}1, & x\geqslant 0,\\ 0, & x=0,\\ -1, & x\leqslant 0.\end{cases}\tag{10}$$

对于两幅尺寸相等, 灰度级为 255 的随机图像, 这两幅图像在一点处的像素值相等的概率 $P_0=\dfrac{1}{256}$, 反之不同的概率 $P_1=1-P_0=\dfrac{255}{256}$, 且由于点的选取的任意性, 可将两幅图像的 NPCR 的期望值近似为 $\dfrac{255}{256}\approx 0.9961$.

然而, 若两幅图像在每个对应位置处的像素值均只有微小差别, 此时虽然两幅图像的 NPCR 为理想值, 但是两幅图像在视觉上的差别较小, 这说明以 NPCR 作为衡量两幅图像差别的指标具有片面性. 因此, 本文引入 UACI 来弥补这一不足, UACI 定义为

$$\mathrm{UACI}=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|P_1\left(i,j\right)-P_2\left(i,j\right)\right|}{255-0}\times 100\%.\tag{11}$$

然而, 当 NPCR=1, UACI≈0.3346 (理论值) 时, 两幅图像仍有可能出现近似的效果, 故本文再引入 BACI 来解决这一问题, BACI 定义式如下:

$$\begin{aligned}&\mathrm{BACI}\left(P_1,P_2\right)\\&=\frac{1}{\left(M-1\right)\left(N-1\right)}\sum_{i=1}^{(M-1)(N-1)}\frac{m_i}{255}\times 100\%,\end{aligned}\tag{12}$$

其中, m_i 由下式定义:

$$\begin{aligned}m_i=\frac{1}{6}&\left(\left|d_{i1}-d_{i2}\right|+\left|d_{i1}-d_{i3}\right|+\left|d_{i1}-d_{i4}\right|\right.\\&\left.+\left|d_{i2}-d_{i3}\right|+\left|d_{i2}-d_{i4}\right|+\left|d_{i3}-d_{i4}\right|\right),\end{aligned}\tag{13}$$

(13) 式中, d_{i1}, d_{i2}, d_{i3}, d_{i4} 是矩阵 $\boldsymbol{D}_i=\begin{pmatrix}d_{i1} & d_{i2}\\ d_{i3} & d_{i4}\end{pmatrix}$ 中的元素, 而矩阵 $\boldsymbol{D}_i$ 是由矩阵 $\boldsymbol{D}=|P_1-P_2|$分解成的 $(M–1)\times(N–1)$ 个尺寸为 2×2 的子矩阵得到的, 分析可得 BACI 的理论值为 0.2840. 针对不同图像计算的 NPCR, UACI, BACI 的数值在表 4 中列出.

表 4 修改 1 bit 像素点后不同图像 (S 信号) 的 NPCR, UACI, BACI

Table 4. NPCR, UACI, BACI of different images after changed 1 bit.

图像	NPCR	UACI	BACI
Lena	0.9954	0.3303	0.2682
Pepper	0.9944	0.3305	0.2657
Cameraman	0.9966	0.3394	0.2684

由表 4 中数据可知, 在一定的误差范围内, 针对 Lena, Pepper, Cameraman 图像的 NPCR, UACI, BACI 的数值均接近指标的理想值, 这说明本文所提出的加密算法能够较好地抵御差分攻击.

3.6 鲁棒性分析

对于数字图像加密方案而言, 噪声与非法攻击一直是影响图像重构质量的首要因素, 因此本节将基于三幅图像, 通过向密文图像引入噪声及裁剪像素的方式分析本文加密方案的鲁棒性.

图 13 显示了向三幅图像对应的 S 信号密文中嵌入密度为 0.05 的椒盐噪声后, 以带噪声的密文图像为基础对图像进行重构的结果. 图 14 显示了对三幅图像的 S 信号的密文进行像素剪切, 以裁剪后的密文图像为基础对图像进行重构的结果. 为突出差异性, 本文采用了两种形状的剪切, 使得密文图像以不同的形状丢失了大约 12.5% 的像素值. 对比受到噪声污染或剪切攻击的重构图像与正常情况下的重构图像 (与图 6、图 7 对比), 尽管噪声污染和剪切攻击在最终的重构图像上产生了一定的影响, 但是算法仍能够保证图像的基本信息不被损坏, 即图像的布局和轮廓信息依然是可见的, 这说明本文所提出加密方案能够抵抗一定程度的噪声污染及剪切攻击.

3.7 选择明文攻击分析

在密码学中, 一个合格的加密算法至少能够抵抗选择明文攻击 (chosen plain-text attack,

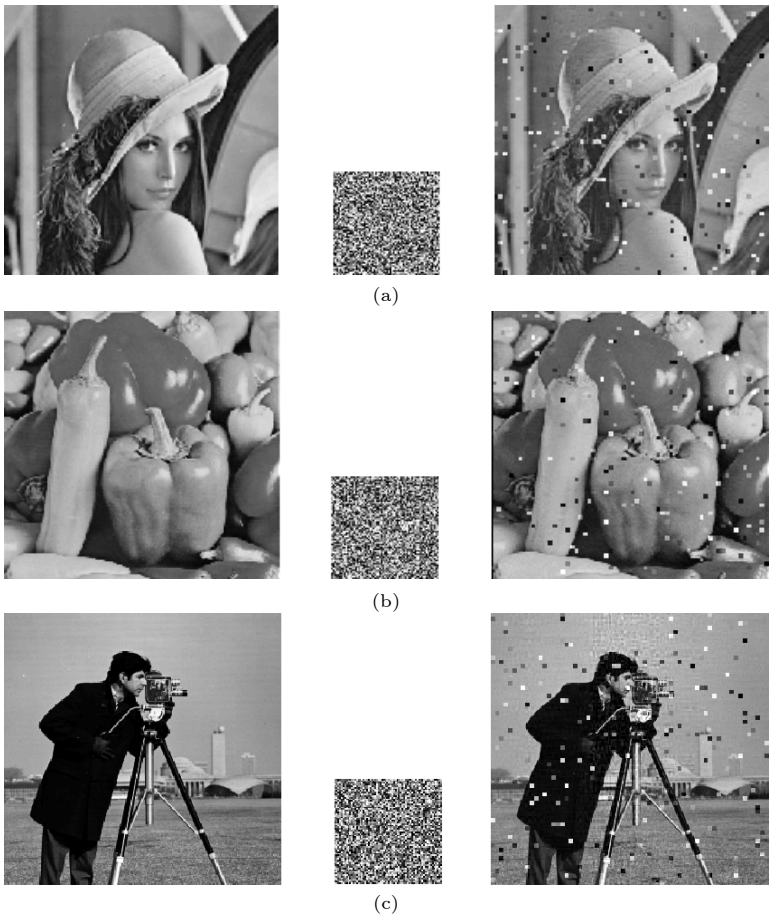


图 13 不同图像的 S 信号嵌入噪声后的重构结果 (a) Lena 原始图像、嵌入噪声的 S 信号密文、重构图像; (b) Pepper 原始图像、嵌入噪声的 S 信号密文、重构图像; (c) Cameraman 原始图像、嵌入噪声的 S 信号密文、重构图像

Fig. 13. Reconstruction results of S signals of different images embedded with noise: (a) Reconstruction results of Lena with corresponding Cipher S signal embedded noise; (b) reconstruction results of Pepper with corresponding Cipher S signal embedded noise; (c) reconstruction results of Cameraman with corresponding Cipher S signal embedded noise.

CPA)[20,21], 本节将通过一个简单的过程来验证本文的加密算法能够抵御选择明文攻击.

定义 P_1 为像素点全部为 0 的灰度图像, P_2 为仅一个像素点与 P_1 不同的灰度图像, 且 P_1, P_2 的尺寸相同. 使用本文提出的加密算法对 P_1, P_2 分别进行加密得到其对应的密文图像 C_1, C_2. 此时, 定义 $P_3 = |P_1 - P_2|$, $C_3 = |C_1 - C_2|$, 上述 6 幅图像如图 15 所示.

由图 15 可知, 在使用本文加密算法对图像加密的前提下, 外界无法通过选择明文攻击从而获取任何有效信息, 进一步说明了本文加密方案的有效性.

3.8 图像重构质量分析

图像的重构质量是判断一种图像处理算法是否合格的重要指标, 本文所提出的加密方案在压缩与重构、加密与解密两个环节中均对图像进行了较多的处理和干预, 因此, 本节通过引入一些数值指标作为根据来衡量本文加密方案的图像重构质量.

权重峰值信噪比 (weighted peak signal to noise ratio, wPSNR) 是用于衡量图像重构质量的有力指标, wPSNR 的定义式如下:

$$\text{wPSNR} = 10\log\left(f_{\max}^2/\text{wMSE}^2\right), \tag{14}$$

其中, wMSE 被称为权重均方差 (weighted mean squared error), 其表达式如下:

$$\text{wMSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} w(x,y)\left[\left(\hat{f}(x,y) - f(x,y)\right)^2\right]^{\frac{1}{2}}, \tag{15}$$

其中, $f(x,y)$, $f'(x,y)$ 分别表示原始图像、重构图像在 (x, y) 位置处的像素值, $w(x, y)$ 表示图像位于 (x, y) 处的像素点所在子带的权重系数.

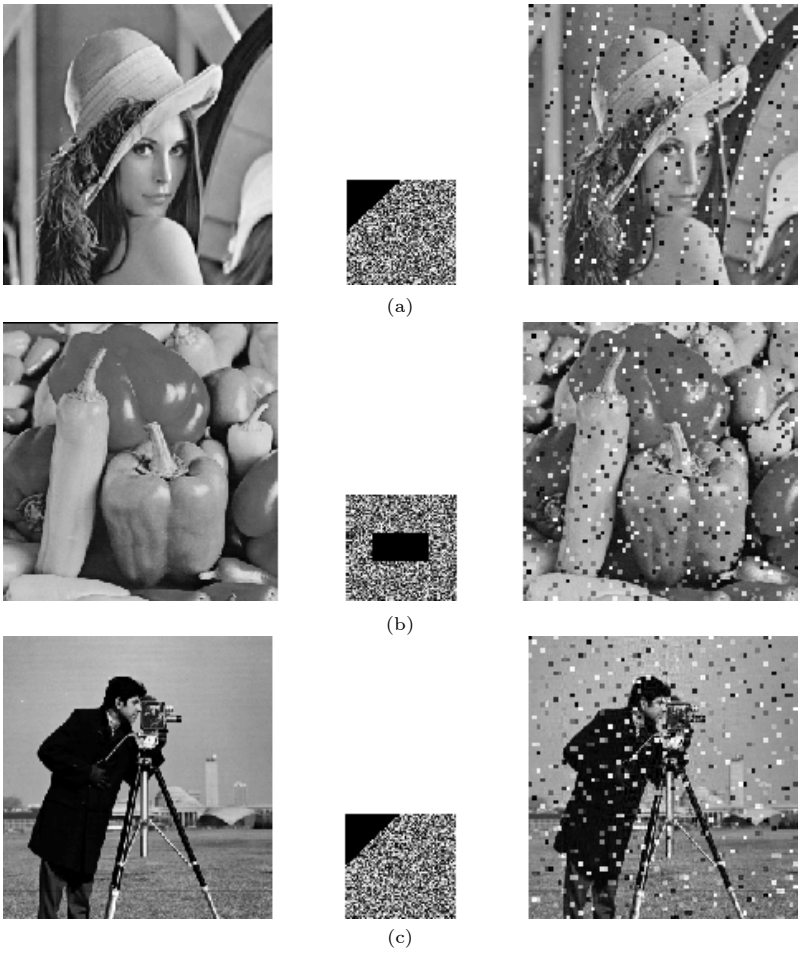


图 14 不同图像的 S 信号像素剪切后的重构结果 (a) Lena 原始图像、剪切 12.5% 像素点后的 S 信号密文、重构图像; (b) Pepper 原始图像、剪切 12.5% 像素点后的 S 信号密文、重构图像; (c) Cameraman 原始图像、剪切 12.5% 像素点后的 S 信号密文、重构图像

Fig. 14. Reconstruction results of S signals of different images after pixel shearing: (a) Reconstruction results of Lena with corresponding Cipher S signal with 12.5% pixels lost; (b) reconstruction results of Pepper with corresponding Cipher S signal with 12.5% pixels lost; (c) reconstruction results of Cameraman with corresponding Cipher S signal with 12.5% pixels lost.

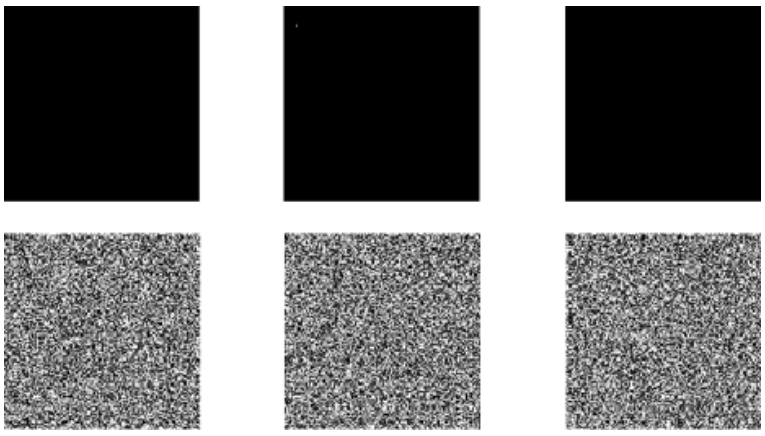


图 15 针对本文加密算法的选择明文攻击

Fig. 15. The CPA against the encryption algorithm in this paper.

除此之外, 本节还引入了结构相似度 (structural similarity, SSIM)[19] 这一指标来衡量图像质量的损坏程度, 通过计算原始图像以及重构后图像的 SSIM 予以评价, SSIM 的定义式为:

$$\mathrm{SSIM}(X,Y)=L(X,Y)\times C(X,Y)\times S(X,Y), \tag{16}$$

$$L(X,Y)=\frac{2u_xu_y+C_1}{u_x^2+u_y^2+C_1}, \tag{17}$$

$$C(X,Y)=\frac{2\sigma_x\sigma_y+C_2}{\sigma_x^2+\sigma_y^2+C_3}, \tag{18}$$

$$S(X,Y)=\frac{\sigma_{xy}+C_3}{\sigma_x\sigma_y+C_3}, \tag{19}$$

$$\begin{cases} u_x=\dfrac{1}{M\times N}\displaystyle\sum_{i=1}^{M}\sum_{j=1}^{N}X(i,j), \\ \sigma_x=\dfrac{1}{M\times N-1}\displaystyle\sum_{i=1}^{M}\sum_{j=1}^{N}(X(i,j)-u_x)^2, \\ \sigma_{xy}=\dfrac{1}{M\times N-1}\displaystyle\sum_{i=1}^{M}\sum_{j=1}^{N}(X(i,j)-u_x)(Y(i,j)-u_y), \end{cases} \tag{20}$$

式中 $C_1=(k_1\times l)^2$, $C_2=(k_2\times l)^2$, $C_3=C_1/2$, $k_1=0.01$, $k_2=0.01$, $l=255$, u_x 和 u_y 分别是图像 X 和 Y 的均值, σ_x 和 σ_y 分别是图像 X 和 Y 的方差, σ_{xy} 是图像 X 和 Y 的协方差.

表 5 列出了在压缩比为 4:3 时, 三幅图像的原始图像及重构图像的 wPSNR 和 SSIM. 分析表中的结果可知, 本文提出的图像加密方案在允许的误差范围下能够较好地对图像进行重构. 当然, 对于 Cameraman 这类带有纯色背景的图像, 其重构效果从会差于具有像 Lena, Pepper 这类包含更复杂的结构、信息的图像.

表 5 本文算法处理下不同图像的 wPSNR 和 SSIM
Table 5. wPSNR and SSIM of different images after processed by scheme in this paper.

图像	wPSNR	SSIM
Lena	48.90	0.9898
Pepper	50.33	0.9927
Cameraman	43.34	0.9736

3.9 时间复杂度分析

在计算机科学中, 算法的时间复杂度是一个函数, 它定性地描述了一个算法的运行时间. 因此, 算法的时间复杂度也是衡量一个算法整体性能的必不可少的指标. 使用本文加密方案处理三幅图像所耗时间如表 6 所示.

由表 6 中数据可知, 在使用本文的图像加密算法处理不同的图像时, 除针对 C_i 信号的压缩及重构过程的耗时存在较大波动外, 其余阶段的耗时均处在一个相对稳定的水平. 分析可知在对 C_i 信号的压缩及重构过程中, 算法时间复杂度与 C_i 信号的数量表现为正相关的关系, 在一定程度上会降低算法的运行效率, 这是需要进一步研究并解决的问题. 综上所述, 本文算法在处理尺寸中等或偏小的图像时, 算法效率较高, 若图像的 C_i 信号数量较多, 算法效率会降低.

表 6 本文算法处理不同图像时的时间复杂度
Table 6. Algorithm proposed deals with the time complexity of different images.

图像	WPT分解及分类	压缩及重构	加密及解密	整体重构	总耗时/s
Lena	0.600 s	8.893 s	1.098 s	0.377 s	10.968
Pepper	0.734 s	7.815 s	1.105 s	0.362 s	10.016
Cameraman	0.617 s	3.908 s	1.901 s	0.353 s	6.799

4 总 结

本文提出了一种基于压缩感知及多维混沌系统的图像加密方案, 通过引入多维混沌系统有效地增强了密文图像的可靠性, 使其相关系数以及信息熵等反映密文图像保密性能的指标更趋近于理想值. 此外, 本文引入新兴的压缩感知理论, 将其运用在图像的压缩处理阶段, 有效地减少了包括加密数据量以及运行时间在内的算法整体的运行成本, 提高了算法的可行性. 除此之外, 本文借助包括阈值处理及分类处理等图像的预处理算法也充分提高了算法的运行效率, 使得算法运行的时间成本保持在较低水平. 在实验验证环节, 本文通过对三幅图像的处理, 结合实验结果验证了本文所提出的算法的可行性及进步性, 同时也为压缩感知理论与混沌理论的结合在信息安全领域应用提供了一定的参考.

参考文献

[1] Wu C M 2014 *Acta Phys. Sin.* **63** 090504 (in Chinese) [吴成

茂 2014 物理学报 **63** 090504]
[2] Lin Q, Wang Y J, Wang J 2016 *Sci. China: Technol. Sci.* **46** 910 (in Chinese) [林青, 王延江, 王珺 2016 中国科学: 技术科学 **46** 910]
[3] Li J, Xian F, Zhang J P 2019 *Int. Electr. Elem.* **27** 84 (in Chinese) [李静, 向菲, 张军朋 2019 电子设计工程 **27** 84]
[4] Donoho D L 2006 *IEEE Trans. Inform. Theory* **52** 1289
[5] Chai X L, Zheng X Y, Gan Z H, Han D J, Chen Y R 2018 *Signal Process* **148** 124
[6] Zhu S Q, Zhu C X, Wang W H 2018 *IEEE Access.* **6** 67095
[7] Lü X P, Liao X F, Yang B 2018 *Multimed Tools Appl.* **77** 28633
[8] Hilton M L 1997 *IEEE Trans. Bio-Med. Eng.* **44** 394
[9] Zhang X, Zhang D Y, Zhang L H, Pan D 2016 *Meteorol. Hydrol. Mar. Instrum.* **33** 38 (in Chinese) [张祥, 张达永, 张刘辉, 潘栋 2016 气象水文海洋仪器 **33** 38]
[10] Goklani H S 2017 *Int. J. Image, Graphics and Signal Processing* **9** 30
[11] Huang R, Rhee K H, Uchida S 2012 *Multimed Tools Appl.* **7** 2
[12] Zhou N, Pan S, Cheng S, et al. 2016 *Opt. Laser Technol.* **82** 121
[13] Yu S M 2008 *Acta Phys. Sin.* **57** 3374 (in Chinese) [禹思敏 2008 物理学报 **57** 3374]
[14] Yu S M 2011 *Chaotic Systems and Chaotic Circuits* (Xi' an: Xi 'an University of Electronic Science and Technology Press) pp136–137 (in Chinese) [禹思敏 2011 混沌系统与混沌电路 (西安:西安电子科技大学出版社) 第136—137页]
[15] Chen G R 1999 *Int. J. Bifurcat. Chaos* **9** 1465
[16] Wang M T, Guo Y Q 2017 *Electr. Technol.* **46** 69 (in Chinese) [王鸣天, 郭玉奇 2017 电子技术 **46** 69]
[17] Li C Q 2013 *Nonlinear Dyn.* **73** 2083
[18] Gao Z H, Xu W B 2011 *MATLAB-Based Image Processing Case Tutorial* (Beijing: Tsinghua University Press) pp99–101 (in Chinese) [高展鸿, 徐文波 2011 基于MATLAB的图像处理案例教程 (北京: 清华大学出版社) 第99—101页]
[19] Zhang Y 2016 *Chaotic Digital Image Crptosystem* (Beijing: Tsinghua University Press) pp50–59 (in Chinese) [张勇 2016 混沌数字图像加密 (北京: 清华大学出版社) 第50—59页]
[20] Wang J, Jiang G P 2011 *Acta Phys. Sin.* **60** 060503 (in Chinese) [王静, 蒋国平 2011 物理学报 **60** 060503]
[21] Zhang Y, Xiao D 2013 *Opt. Lasers Eng.* **51** 472

Multi-process image encryption scheme based on compressed sensing and multi-dimensional chaotic system*

Shi Hang [1)6)] Wang Li-Dan [1)2)3)4)5)†]

1) (*Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing*, *Chongqing* 400715, *China*)

2) (*School of Electronics and Information Engineering*, *Southwest University*, *Chongqing* 400715, *China*)

3) (*Brain-inspired Computing & Intelligent Control of Chongqing Key Lab*, *Chongqing* 400715, *China*)

4) (*National & Local Joint Engineering Laboratory of Intelligent Transmission and Control Technology*, *Chongqing* 400715, *China*)

5) (*Chongqing Brain Science Collaborative Innovation Center*, *Chongqing* 400715, *China*)

6) (*School of Westa*, *Southwest University*, *Chongqing* 400715, *China*)

(Received 16 April 2019; revised manuscript received 15 July 2019)

Abstract

With the rapid development of computer science, the storage and dissemination of information are often carried out between various types of computer hardwares and various networks. The traditional information encryption scheme has gradually disappeared. Therefore, computer-based information encryption algorithms have gradually become a research hotspot in recent years. By combining the theory of wavelet packet transform, compressed sensing and chaotic system, a multi-process image encryption scheme based on compressed sensing and multi-dimensional chaotic system is proposed. The encryption scheme implements compression and encryption for grayscale images and corresponding decompression and decryption process. The wavelet packet transform theory is applied to the image preprocessing stage to perform wavelet packet decomposition on the original image. At the same time, the image signal components obtained by the decomposition are classified according to the threshold processing method, and the characteristics of the image signal components are processed in the subsequent processing. They are compressed, encrypted, or reserved in a differentiated manner. In the image compression stage, by introducing the compressed sensing algorithm to overcome the shortcomings of the traditional Nyquist sampling theorem, such as high sampling cost and low reconstruction quality, the compression efficiency and compression quality are improved while the ciphertext image reconstruction quality is guaranteed. In the image encryption stage, the encryption scheme combines multi-class and multi-dimensional chaotic systems to confuse and scramble the related image signal components, and introduces a high-dimensional chaotic system to make the encryption scheme have a large enough key space to further enhance the ciphertext image reliability. Finally, the complete reconstruction of the original image is achieved by applying the inverse of compression, encryption and wavelet packet transform. The simulation results show that the image encryption scheme effectively protects the basic information about ciphertext images by virtue of algorithm robustness against external interference, and does not reveal any useful information when dealing with cracking methods such as plaintext attacks. In addition, the information entropy and correlation coefficient of ciphertext images encrypted by this encryption scheme are closer to ideal values than those of the encryption algorithm in the references, and its encryption performance is significantly improved.

Keywords: digital image, encryption, wavelet packet transform, compressed sensing

PACS: 05.45.Ac, 05.45.Vx, 05.45.Gg **DOI:** 10.7498/aps.68.20190553

* Project supported by the National Key Research & Development Program of China (Grant No. 2018YFB1306600), the National Natural Science Foundation of China (Grant Nos. 61571372, 61672436, 61601376), the Fundamental Science and Advanced Technology Research Foundation of Chongqing, China (Grant Nos. cstc2017jcyjBX0050, cstc2016jcyjA0547), and the Fundamental Research Funds for the Central Universities, China (Grant Nos. XDJK2016A001, XDJK2017A005).

† Corresponding author. E-mail: ldwang@swu.edu.cn