计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2023,32(2):295−302 [doi: 10.15888/j.cnki.csa.008935]

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

基于压缩感知和超混沌系统的多图像加密算法①

白牡丹, 赵　莉, 李珊珊

(长安大学 信息工程学院, 西安 710064)
通信作者: 李珊珊, E-mail: sputnik@126.com

摘　要: 为了有效改善传输速率并降低带宽负担, 提出一种基于压缩感知和超混沌系统的多图像加密方案. 首先将多幅原始图像拼接成新的明文图像, 并将部分明文信息与随机正整数结合产生混沌系统初始值, 利用超混沌系统产生的伪随机序列生成加密过程所需的测量矩阵、置乱序列及扩散序列. 其次通过离散小波变换、阈值处理以及并行测量对明文图像进行压缩处理, 有效减少运算数据量, 大大加快运行速率. 最后通过无重复置乱操作和双向加模扩散得到最终的密文图像. 经多个层面的仿真模拟实验, 验证了所提算法能有效抵御剪切攻击, 且具有比较高的安全性.

关键词: 多图像加密; 压缩感知; 超混沌系统; 像素置乱; 扩散

引用格式: 白牡丹,赵莉,李珊珊.基于压缩感知和超混沌系统的多图像加密算法.计算机系统应用,2023,32(2):295–302. http://www.c-s-a.org.cn/1003-3254/8935.html

Multiple-image Encryption Algorithm Based on Compressed Sensing and Hyperchaotic System

BAI Mu-Dan, ZHAO Li, LI Shan-Shan

(College of Information Engineering, Chang'an University, Xi'an 710064, China)

Abstract: To effectively improve the transmission rate and reduce bandwidth burden, this study proposes a multiple-image encryption scheme based on compressed sensing and a hyperchaotic system. Specifically, several original images are spliced into a new plaintext image, and some plaintext information is combined with random positive integers to generate the initial value of the chaotic system. The pseudo-random sequence generated by the hyperchaotic system is utilized to produce the measurement matrix, scrambled sequence, and diffusion sequence the encryption process needs. Then, discrete wavelet transform, thresholding, and parallel measurement are performed to compress the plaintext image, which can effectively reduce the amount of operation data and greatly speed up the operation speed. Finally, the final ciphertext image is obtained by non-repeated scrambling and bidirectional mode-adding diffusion. Multiple levels of simulation experiments verify that the proposed algorithm can effectively resist cropping attacks and offer high security.

Key words: multiple-image encryption; compressed sensing; hyperchaotic system; pixel scrambling; diffusion

现今社会, 随着网络的普及以及智能化的不断发展, 大量数据不断产生并传输, 这就可能涉及到个人身份、公司文件甚至是国家机密等信息, 而信息在传输过程中可能会发生信息丢失或者受到噪声的影响, 更为严重的可能存在信息泄露和信息篡改等安全问题, 这就可能对个人, 社会以及国家造成不可挽回的损失. 因此信息安全问题就显得尤为重要.

为保证多图像在传输过程中的安全性, 研究者通常从频域和空域两方面来实现图像加密. 基于频域的实现方法主要是通过小波变换[1]、梅林变换[2]、傅里叶变换[3] 等频域变换将图像信息从空域转换为变换域, 进而实现多图像加密的方法. 但图像经过频域变换后,

① 收稿时间: 2022-07-04; 修改时间: 2022-07-29; 采用时间: 2022-08-09; csa 在线出版时间: 2022-09-26
CNKI 网络首发时间: 2022-11-15

只提取低频部分来进行图像加密, 这会导致高频部分图像信息丢失, 不能完全恢复原始图像. 之后研究者发现混沌系统具有不可预测以及初值敏感等特性, 故将其作为空间域图像加密的主要手段. 比如, 文献 [4] 提出了一种改进的埃农映射和非线性组合混沌系统的多图像加密方案. 文献 [5] 将 DNA 序列和细胞自动机组合, 提出了基于 DNA 序列和图像矩阵索引的多图像加密方案. 2021 年, Bian 等人[6] 提出了利用托普利茨矩阵鬼影成像和椭圆曲线编码实现多图像加密的方案.

由于传统多图像加密技术中, 大多都是直接采用将多幅明文水平垂直拼接后直接进行加密操作的方法, 这就会导致图像加密过程复杂和运行效率低, 以及在传输过程中占用带宽过大, 致使传输效率过低的问题. 为了解决这种问题, 本文将压缩感知技术[7,8] 和超混沌系统结合实现多图像加密. 通过将随机正整数与明文图像的部分信息结合得到混沌系统的初始值, 利用混沌系统产生加密过程中所需的测量矩阵、置乱序列以及扩散序列, 将加密过程与明文密切相关, 提高密文对明文的敏感性. 利用压缩感知技术对图像进行压缩, 有效降低处理数据量, 提高加密和传输效率.

1 相关知识

1.1 压缩感知技术

压缩感知技术是继奈奎斯特采样理论的又一重要发明, 其不再规定信息采集速度需要超过原信道传输带宽的 2 倍以上, 才能够完全的重构出原始信息. 压缩感知理论更多的是从信息自身的结构特征中出发, 运用信息的稀疏特征, 对信息进行了压缩采集[9,10]. 图 1 为压缩感知技术的理论框架. 在本文中, 通过小波变换和并行测量压缩图像, 通过分段弱正交匹配追踪算法[11] 重构原始图像信息.

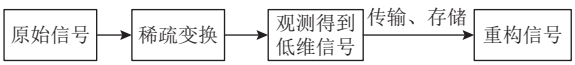

图 1 压缩感知理论框架

1.2 超混沌系统

为了获得更不可预测的伪随机序列, 在本文中选择四维超混沌系统来生成加密过程中所需要的测量矩阵、置乱序列及扩散序列. 四维超混沌系统[12] 的定义如式 (1) 所示:

$$\begin{cases} x_{n+1} = \dfrac{\gamma_1 \sin(\beta_1 x_n)}{\omega_1 \sin(z_n)^2 + \alpha_1} \\ y_{n+1} = \dfrac{\gamma_2 \sin(\beta_2 y_n)}{\omega_2 \sin(x_n)^2 + \alpha_2} \\ w_{n+1} = \dfrac{\gamma_3 \sin(\beta_3 w_n)}{\omega_3 \sin(y_n)^2 + \alpha_3} \\ z_{n+1} = \dfrac{\gamma_4 \sin(\beta_4 z_n)}{\omega_4 \sin(w_n)^2 + \alpha_4} \end{cases} \tag{1}$$

其中, α_i、β_i、γ_i及ω_i均为混沌系统的参数, 每个参数的下标$i = 1,2,3,4$, 且必须满足$\alpha_i,\beta_i,\gamma_i,\omega_i \neq 0$和$\alpha_i\omega_i > 0$. 通过文献 [13] 中求解 Laypunov 指数的方法求得式 (1) 的 4 个 Laypunov 指数分别为: $\lambda_1 = 1.6990$, $\lambda_2 = 1.0605$, $\lambda_3 = 0.7410$和$\lambda_4 = -1.6130$. 可以得出 4 个 Laypunov 指数中有 3 个是大于 0, 表明该系统的确是超混沌系统, 混沌序列的不可预测性更强.

2 多图像加密算法

本文提出了基于压缩感知和超混沌系统的多图像加密算法. 方案中利用随机正整数和明文图像信息产生超混沌系统初始值, 再将混沌序列随机组合构建受控测量矩阵、置乱矩阵和扩散矩阵. 对于拼接后的明文图像而言, 实现了“一图一密”, 使算法具备抵挡选择明文攻击的能力; 其次在并行测量前进行混沌矩阵置乱, 改变图像在水平和垂直方向上的像素位置, 使得系数矩阵不平衡的稀疏度得以改善; 最后通过无重复置乱和双向加模扩散操作得到密文. 具体加密流程图见图 2.

2.1 混沌系统初始值预处理

步骤 1. 设 4 幅明文图像 $I1$、$I2$、$I3$、$I4$ 的大小为 $m \times n$, 通过水平垂直拼接为原来长宽的 2 倍, 拼接后图像为 C, 其尺寸为$M \times N$, 对明文图像的信息经过式 (2) 处理, 得到 4 个参数a_1, a_2, a_3, a_4.

$$\begin{cases} t = round(M \times r) \\ a_1 = \displaystyle\sum_{i=1}^{t}\sum_{j=1}^{t} C(i,j)/(t \times t) \\ a_2 = \displaystyle\sum_{i=1}^{t/2}\sum_{j=1}^{t/2} C(i,j)/(t/2 \times t/2) \\ a_3 = \displaystyle\sum_{i=1}^{M}\sum_{j=1}^{N} C(i,j)/(M \times N) \\ a_4 = floor\left(\displaystyle\sum_{i=1}^{M}\sum_{j=1}^{N} C(i,j)/(M \times N)\right) \end{cases} \tag{2}$$

其中, r 表示压缩率 ($0<r<1$), i 和 j 是图像像素在平面坐标系中对应的横坐标和纵坐标, 其中 $i=1,2,\cdots,M$, $j=1,2,\cdots,N$, *round* 表示四舍五入操作, *floor* 表示取整处理.

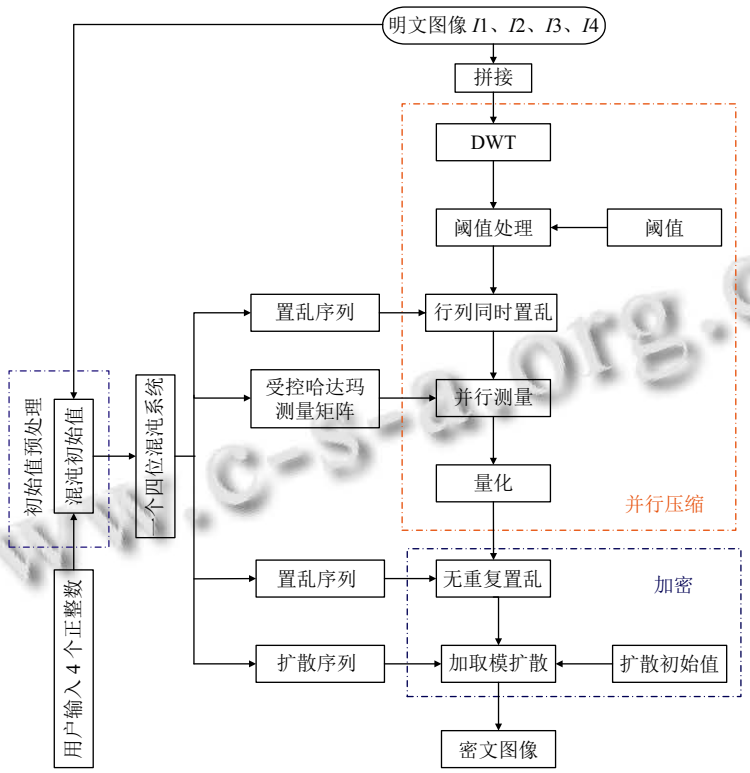

图 2 加密流程图

步骤 2. 用户输入 4 个随机正整数 k_1、k_2、k_3 和 k_4, 分别将其对 4 进行取模运算得到处理后的 4 个参数 k'_1、k'_2、k'_3和k'_4.

步骤 3. 混沌系统最初初始值为 x_0、y_0、w_0 和 z_0, 结合步骤 1–2 求得的参数, 采用式 (3) 计算混沌系统迭代时的初始值x'_0、y'_0、w'_0和z'_0, 其中 mod 为取模运算.

$$\begin{cases} x'_0 = \mathrm{mod}(a_1 \times 10\text{^}k'_1 + x_0, 1) \\ y'_0 = \mathrm{mod}(a_2 \times 10\text{^}k'_2 + y_0, 1) \\ w'_0 = \mathrm{mod}(a_3 \times 10\text{^}k'_3 + w_0, 1) \\ z'_0 = \mathrm{mod}(a_4 \times 10\text{^}k'_4 + z_0, 1) \end{cases} \tag{3}$$

2.2 并行压缩

本阶段实现了图像并行压缩过程, 假设待加密的明文图像 C 的尺寸为$M \times N$, 本阶段并行压缩的详细过程如下.

步骤 1. 通过离散小波变换得到一个小波变换基矩阵. 利用式 (4) 对明文图像 C 进行稀疏变换, 获得与明文图像同尺寸的稀疏系数矩阵 $C1$, 式中的符号 T 代表转置操作.

$$C1 = Psi \times C \times Psi^{\mathrm{T}} \tag{4}$$

步骤 2. 根据预先设置的阈值 Ts, 将系数矩阵 $C1$ 中所有不大于阈值 Ts 的值通通变换为零, 得到的矩阵记作 $C2$. 根据迭代初始值将混沌系统迭代运行 MN+500 次, 前 500 次伪随机序列舍弃以获得具有较好混沌特性的伪随机序列, 进而得到 4 个伪随机序列 X、Y、Z、W.

步骤 3. 采用文献 [13] 中提出的混沌矩阵置乱方法置乱 $C2$, 其中将伪随机序列 X 重建为与明文图像相同大小的二维矩阵 CX 作为混沌矩阵, 置乱后的矩阵为 $C3$.

步骤 4. 将混沌序列 W 中的前 t 个值进行升序排列, 排列后得到一个新的索引序列 T_W. 通过式 (5), 利用 T_W 和部分哈达玛矩阵$H_W \in R^{N \times M}$生成一个受控测量矩阵$Phi \in R^{t \times M}$.

$$Phi_i = H_{W(T_W(i))},\ i = 1,2,\cdots,t \tag{5}$$

步骤 5. 用*Phi*对矩阵 *C*3 进行压缩感知[14] 的并行测量, 得到压缩后的矩阵$C4 \in R^{t \times M}$. 接着对压缩矩阵进行线性量化, 得到最后的压缩图像 *C*5, 具体如式 (6):

$$C5 = round\left(255 \times \frac{C4 - min}{max - min}\right) \tag{6}$$

其中, 参数 *min* 和 *max* 分别指压缩矩阵 *C*4 中的最小值和最大值, *round* 为四舍五入操作.

2.3 二次加密

步骤 1. 将压缩图像 *C*5 按列展开为一维向量, 记作 *C*6. 对 *Y* 序列经过式 (7) 的处理, 接着过滤掉 *Y* 中重复出现的数值, 然后将 1–$t \times N$ 之间没有在 *Y* 中存在的正整数按升序的规律插入到 *Y* 的末端, 得到序列值唯一的 *Y* 序列, 再按式 (8) 的规则进行交换位置, 得到无重复置乱后的一维向量 *C*7.

$$Y = \mathrm{mod}\left(floor\left((Y(1:t \times N) + 50) \times 10^{15}\right), t \times N\right) + 1 \tag{7}$$

$$C6(Y_i) = C6(Y_{t \times N - i + 1}) \tag{8}$$

其中, $i = 1, 2, \cdots, t \times N$.

步骤 2. 将 4 个伪随机序列 *X*、*Y*、*Z*、*W* 根据排列组合的基本原理组合成为 4*MN* 长度的混合序列. 本文中采用其中两个伪随机序列, 分别是$C_{XYWZ} = \{X, Y, W, Z\}$和$C_{ZYXW} = \{Z, Y, X, W\}$.

步骤 3. 将伪随机序列 C_{XYWZ} 和 C_{ZYXW} 分别代入式 (9) 和式 (10), 生成双向扩散操作所需的伪随机数向量$[Sm1, Qm1] \in R^{(t \times N) \times 2}$和$[Sm2, Qm2] \in R^{(t \times N) \times 2}$.

$$\begin{cases} Sm = \mathrm{mod}\left(round(C_{XYWZ} \times pow2(16)), L\right) \\ Sm1 = Sm^{1:t \times N} \\ Sm2 = Sm^{2 \times t \times N + 1:3 \times t \times N} \end{cases} \tag{9}$$

$$\begin{cases} Qm = \mathrm{mod}\left(round(C_{ZYXW} \times pow2(8)), L\right) \\ Qm1 = Qm^{1:t \times N} \\ Qm2 = Qm^{2 \times t \times N + 1:3 \times t \times N} \end{cases} \tag{10}$$

其中, *L*=256 表示灰度级水平, *pow*2 表示以 2 为基底的幂函数.

步骤 4. 用户输入正向扩散和逆向扩散的初始值 (*Bm*0, *Cm*0), 通过式 (11)–式 (12) 得到扩散后的一维向量 *C*8.

$$\begin{cases} Bm_i = \mathrm{mod}\left(Bm0 + Sm1_i + Qm1_i + C7_i, L\right), \ i = 1 \\ Bm_i = \mathrm{mod}\left(Bm_{i-1} + Sm1_i + Qm1_i + C7_i, L\right), \\ \qquad i = 2, 3, \cdots, t \times N \end{cases} \tag{11}$$

$$\begin{cases} C8_i = \mathrm{mod}\left(Cm0 + Sm2_i + Qm2_i + Bm_i, L\right), \ i = t \times N \\ C8_i = \mathrm{mod}\left(C8_{i+1} + Sm2_i + Qm2_i + Bm_i, L\right), \\ \qquad i = t \times N - 1, \cdots, 1 \end{cases} \tag{12}$$

步骤 5. 把一维向量 *C*8 重建为 $t \times N$ 大小的二维矩阵 *C*9, 即密文图像.

3 相应的解密算法

解密就是把对应的加密过程的逆过程, 其具体解密流程简述如下.

步骤 1. 将密文图像 *C*9 按列展开为一维向量 *C*8. 利用伪随机数向量$[Sm1, Qm1]$和$[Sm2, Qm2]$, 对向量 *C*8 进行逆加模扩散操作, 从而得到无重复置乱后的一维向量 *C*7.

步骤 2. 利用伪随机序列 *Y* 中前 $t \times N$ 的序列片段对一维向量 *C*7 进行无重复置乱的反过程, 得到重排后的一维向量 *C*6. 并将 *C*6 重建为二维矩阵 *C*5, 即压缩图像.

步骤 3. 对压缩图像 *C*5 实施逆量化, 得到压缩矩阵 *C*4, 并使用分段弱正交匹配追踪重构算法按列从矩阵 *C*4 中重构出矩阵 *C*3. 再对其进行混沌矩阵置乱还原, 得到矩阵 *C*1.

步骤 4. 利用离散小波变换的反变换从矩阵 *C*1 恢复出大小为 $M \times N$ 的明文图像 *C*, 并对其进行分割, 得到 4 幅原始图像 *I*1、*I*2、*I*3、*I*4.

4 仿真实验及安全性分析

本文采用 4 幅大小为 256×256 的灰度图像进行实验, 分别为: Lena、Cameraman、Peppers 和 Woman. 实验主机环境为 Intel Core I7-6700, 机带 RAM 为 8 GB, 具有 3.41 GHz 的处理器, 以及 64 位 Windows 10 操作系统. 实验使用 Matlab R2019b 软件实现仿真测试. 系统的密钥由混沌系统初始值预处理前的值 x_0、y_0、w_0 和 z_0、加模扩散的两个初始值 *Bm*0 和 *Cm*0、用户自定义的 4 个参数 k_1、k_2、k_3 和 k_4 组成. 实验是在阈值 *Ts*=25、x_0=0.5、y_0=0.4、w_0=0.3、z_0=0.6、*Bm*0=*Cm*0=0、k_1=5、k_2=30、k_3=8 和 k_4=20, 压缩率 *r*=0.25 的基础上进行的.

4.1 加解密结果图

为了直观的观测加解密效果, 本节对其进行仿真实验, 结果如图 3 所示, 其中图 3(a)–图 3(d) 为原始图像, 图 3(e) 为密文图像, 图 3(f)–图 3(i) 为 4 幅解密图

像. 从结果图中可以看出, 密文像素分布均匀, 并且在视觉上解密图像难以和明文图像进行区分.

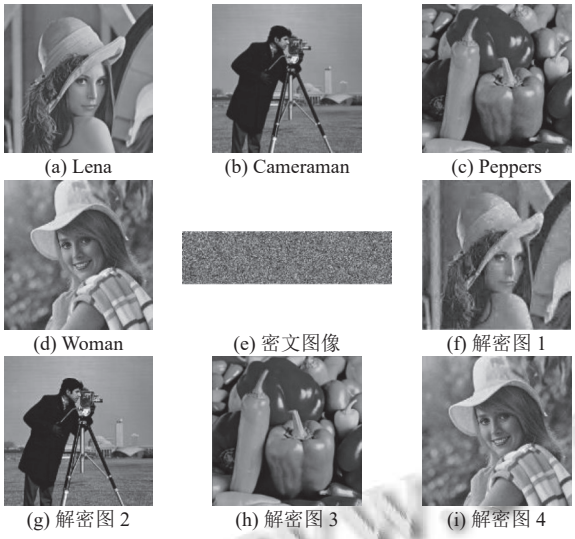

图 3 加解密效果图

4.2 密钥空间

本文提出的加密算法, 密钥包括混沌系统初始值预处理前的值 x_0、y_0、w_0 和 z_0、加模扩散的两个初始值 $Bm0$ 和 $Cm0$ 以及用户自定义的 4 个参数 k_1、k_2、k_3 和 k_4. 在本文提出的方案中, 整个系统是在灰度级为 256、双精度和 64 位 Windows 10 操作系统下进行的. 根据 IEEE 浮点标准[15], 64 位双精度计算精度为 10^{15}. 由此计算可得本章算法所拥有的密钥空间大小为 $(10^{15})^{10} = 10^{150}$, 其值高出$2^{100}$很多, 说明面对穷举攻击有足够的抵御能力.

4.3 信息熵

信息熵是反映加密效果的一个重要指标, 用于判断图像内部各像素灰度值的出现是否接近等概率, 体现了加密体系的混乱程度. 图像的信息熵越大, 成功抵御熵攻击的概率就越大. 表 1 统计了明文图像的信息熵, 并将其与文献 [16–18] 进行了比较. 对比文献 [16], 本文算法具有较高的信息熵; 而由于本文没有采用较为复杂的像素置乱方法, 故信息熵略低于文献 [17,18].

4.4 相邻像素相关性

本节以 Lena 原始图像为例, 对比了明文与密文像素点间相关关系密切程度的分布情况如图 4 所示. 图 4(a)–图 4(c) 表示明文图像 Lena 的相关部分, 图 4(d)–图 4(f) 显示密文图像的相关部分. 表 2 用真实数据更加准确的对比了明文与密文的像素相关性.

表 1 不同算法下相同图像的信息熵对比

图像	信息熵
Lena	7.4464
Cameraman	7.0911
Peppers	7.5715
Woman	7.2695
密文	7.9975
文献[16]密文	7.9961
文献[17]密文	7.9993
文献[18]密文	7.9994

表 2 各图像相邻位置像素点间的相关系数

图像	相关系数		
	水平	垂直	对角
Lena	0.9260	0.9607	0.9032
Cameraman	0.9335	0.9592	0.9087
Peppers	0.9569	0.9636	0.9325
Woman	0.9455	0.9625	0.9180
密文	0.0013	0.0002	-1.5430×10^{-4}
文献[19]密文	−0.0036	0.0026	0.0012
文献[20]密文	−0.0003	0.0011	0.0013

由图 4 可以看出: 明文图像 Lena 相邻之间的像素相关性分布非常集中, 整体呈现线状分布; 而密文图像像素点分布散落分布在整个区域内, 意味着加密后图像内部相邻像素间近乎没有相关关系. 结果表明, 本文提出的加密算法可以有效地消除明文图像内部相邻像素间密切的相关关系.

由表 2 仿真数据可以得出: 明文图像的像素相关性非常趋近于 1, 而经过加密算法的密文图像像素分布均匀, 整个结果数值表明本文提出的加密算法能够有效扰乱图像像素分布情况. 对比文献 [19,20], 本文所提算法的像素相关系数更小, 密文像素分布更随机.

4.5 差分攻击分析

一个良好的加密系统应满足密文与明文之间像素差异很大. 攻击者无法通过改变图像中某个像素来分析密文之间的差异, 进而无法判断加密体系中的具体过程. 对差分攻击进行分析时, 常像素数目变化率 (number of pixels change rate, NPCR) 和统一平均变化强度 (unified average change intensity, UACI)[21–24] 进行测量. 在本节实验中, 通过改变明文图像中一个像素值, 来计算密文之间的 NPCR 和 UACI, 结果如表 3 所示. 根据不同大小图像对应的理论临界值, 可以判断本文算法的 NPCR 和 UACI 均在有效范围内, 表明算法可以有效抵御差分攻击. 对比文献 [21,25], 本文所提算法优于其他方案. 因此, 该方案能够抵抗差分攻击, 且比其他多图像加密方案更强.

表 3 不同方案加密不同图像的 NPCR 和 UACI

算法	图像	NPCR	UACI
本文算法	Lena	0.9979	0.3477
	Cameraman	0.9977	0.3393
	peppers	0.9973	0.3433
	Woman	0.9976	0.3406
文献[21]	Lena	0.9379	0.1678
	Baboon	0.9366	0.1659
	Pepper	0.9369	0.1670
	Kodim04	0.9364	0.1664
	Kodim18	0.9357	0.1652
文献[25]	Lena	0.9957	0.3358
	Trees	0.9926	0.3332
	House	0.9954	0.3359
	Child	0.9963	0.3344

4.6 鲁棒性分析

由于网络传输过程中, 会导致图像丢失部分的图像信息, 因此本节通过切割部分密文来模拟在传输过程中受到的影响, 并通过峰值信噪比 (peak signal to noise ratio, PSNR) 和结构相似性 (structural similarity, SSIM)[26] 两个指标对其进行结果分析. 在本节实验中, 将密文图像分别在左上角、中间和右下角位置丢失 8×8、16×16 和 32×32 大小的数据来模拟数据丢失, 以 Lena 图为例计算 SSIM 和 PSNR 值. 实验结果如表 4 所示, 表显示了不同位置丢失不同尺寸数据时的 SSIM 和 PSNR 值.

表 4 不同尺寸和位置的数据丢失后的 SSIM 和 PSNR

尺寸	指标	左上	中间	右下	平均值
8 × 8	SSIM	0.9523	0.9529	0.9146	0.9521
	PSNR (dB)	34.3290	34.4389	32.2379	33.7625
16 × 16	SSIM	0.8655	0.8690	0.7810	0.8452
	PSNR (dB)	32.2719	32.3378	29.3478	33.3261
32 × 32	SSIM	0.7089	0.7139	0.6128	0.6819
	PSNR (dB)	30.8931	30.9302	28.9431	29.7173

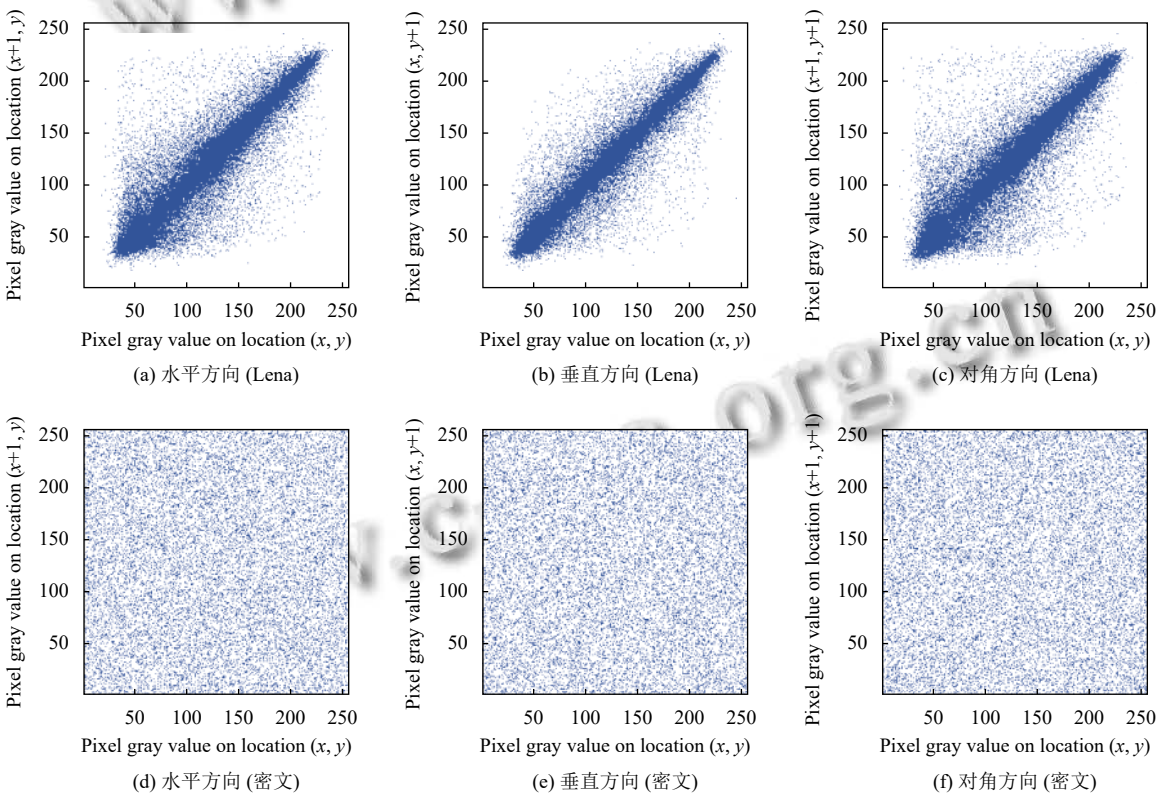

图 4 密文及 Lena 图的相邻像素相关性分布图

从结果可以看出: 随着图像丢失的数据越来越多, SSIM 和 PSNR 值逐渐减小; 当数据丢失的位置发生变化时, SSIM 和 PSNR 变化不大, 意味着该算法能够在受位置影响较小的情况下抵抗数据丢失攻击. 总而言之, 即使在传输过程中丢失部分密文信息, 通过正确的密钥信息, 解密图像内容依然可以进行分辨, 表明所提出的算法具有一定的抗剪切攻击性能.

5 结语

本文将压缩感知技术与超混沌系统结合实现多图像加密算法. 与其他算法不同的是该算法通过明文图像信息产生超混沌系统初始值, 达到“一图一密”的密钥模型, 增强了密文抵挡选择明文攻击的能力; 其次在并行测量前进行混沌矩阵置乱, 改变图像在水平和垂直方向上的像素位置, 缩小了系数矩阵中所有列向量存在的稀疏度差异, 最后对压缩后的图像数据进行无重复置乱和双向加模扩散操作, 再次改变图像像素值及像素位置, 使图像像素分布更均匀, 削弱了第一次行列置乱可能导致的像素分布不均匀情况以及量化误差对鲁棒性的影响.

通过仿真实验数据可得, 本文算法的密钥空间足够大, 可以有效抵抗穷举攻击; 利用 Lena 图对比明文与密文之间像素分布情况, 可以发现密文像素均匀地分布在整个相位空间内, 表明本文算法可以有效扰乱像素分布; 通过改变明文中某一个像素值来计算 NPCR 和 UACI 指标, 数据显示两指标均在有效范围内, 表明密文对明文具有强敏感性, 可以抵御差分攻击; 在鲁棒性分析实验中, 通过切割部分密文来模拟信息在传输过程中受到的影响, 结果显示该算法能够在受位置影响较小的情况下抵抗数据丢失攻击. 通过对比相似文献, 本文算法在以上指标中具有较好优势, 但由于方案中置乱操作略为简单, 导致密文信息熵略低于其他文献, 表明算法成功抵御熵攻击的概率较低, 在以后的研究过程中将从提高信息熵入手.

参考文献

1 朱薇, 杨庚, 陈蕾, 等. 基于小波变换和改进双随机相位编码的多图像加密算法. 南京邮电大学学报 (自然科学版), 2014, 34(5): 87–92. [doi: 10.14132/j.cnki.1673-5439.2014.05.023]

2 Pan SM, Wen RH, Zhou ZH, *et al*. Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional Mellin transform. Multimedia Tools and Applications, 2017, 76(2): 2933–2953. [doi: 10.1007/s11042-015-3209-x]

3 穆晓芳, 亓慧, 李晓宾. 基于傅里叶域向量计算的多图像联合加密算法 (英文). 机床与液压, 2019, 47(18): 126–131. [doi: 10.3969/j.issn.1001-3881.2019.18.022]

4 Kari AP, Navin AH, Bidgoli AM, *et al*. A novel multi-image cryptosystem based on weighted plain images and using combined chaotic maps. Multimedia Systems, 2021, 27(5): 907–925. [doi: 10.1007/s00530-021-00772-y]

5 Enayatifar R, Guimarães FG, Siarry P. Index-based permutation-diffusion in multiple-image encryption using DNA sequence. Optics and Lasers in Engineering, 2019, 115: 131–140. [doi: 10.1016/j.optlaseng.2018.11.017]

6 Bian ZX, Zhang LH, Ye HL, *et al*. Multiple-image encryption based on Toeplitz matrix ghost imaging and elliptic curve cryptography. Laser Physics Letters, 2021, 18(5): 055206. [doi: 10.1088/1612-202X/abf5cc]

7 杜鑫昌, 高瑜翔, 曹远杰, 等. 基于混沌压缩感知和 DNA 编码的多图像加密算法. 无线电工程, 2022, 52(3): 476–483. [doi: 10.3969/j.issn.1003-3106.2022.03.019]

8 Ni RJ, Wang F, Wang J, *et al*. Multi-image encryption based on compressed sensing and deep learning in optical gyrator domain. IEEE Photonics Journal, 2021, 13(3): 7800116.

9 田强宝, 谢冬. 基于压缩感知和随机像素置换的多图像联合加密方案. 杭州师范大学学报 (自然科学版), 2020, 19(2): 208–214.

10 罗玉玲, 梁钰婷, 张顺生. 基于压缩感知的混沌图像加密研究综述. 广西师范大学学报 (自然科学版), 2022: 1–10. https://kns.cnki.net/kcms/detail/detail.aspx?dbcode=CJFQ&dbname=CAPJLAST&filename=GXSF20220512001&v=MTAxMTA4PUlqWFlhTEc0SE5QTXFvNUhaT3NPWXc5TXptUm42ajU3VDNmbHFXTTBDTEw3UjdxZFplWm1GaXZsVnJ2UElG. (2022-05-13).

11 Blumensath T, Davies ME. Stagewise weak gradient pursuits. IEEE Transactions on Signal Processing, 2009, 57(11): 4333–4346. [doi: 10.1109/TSP.2009.2025088]

12 杨可心, 吴昭辉, 郝瑞斌, 等. 四维混沌系统及其在图像加密中的应用. 计算机应用研究, 2020, 37(11): 3433–3436.

13 Hua ZY, Jin F, Xu BX, *et al*. 2D logistic-sine-coupling map for image encryption. Signal Processing, 2018, 149: 148–161. [doi: 10.1016/j.sigpro.2018.03.010]

14 蒋东华, 刘立东, 陈颖频, 等. 基于分数阶 Chen 超混沌系统和压缩感知的可视化图像加密算法. 小型微型计算机系统, 2021: 1–9. http://kns.cnki.net/kcms/detail/21.1106.TP.20210923.1457.014.html. (2021-09-24).

15 孟浩, 李博, 杨耀森. 基于有限素域乘法群与倾斜帐篷的图像加密算法. 计算机应用与软件, 2020, 37(2): 282–287. [doi: 10.3969/j.issn.1000-386x.2020.02.044]

16 Bisht A, Dua M, Dua S. A novel approach to encrypt multiple images using multiple chaotic maps and chaotic discrete fractional random transform. Journal of Ambient Intelligence and Humanized Computing, 2019, 10(9): 3519–3531. [doi: 10.1007/s12652-018-1072-0]

17 Patro KAK, Soni A, Netam PK, *et al*. Multiple grayscale image encryption using cross-coupled chaotic maps. Journal of Information Security and Applications, 2020, 52: 102470. [doi: 10.1016/j.jisa.2020.102470]

18 Ul Haq T, Shah T. Algebra-chaos amalgam and DNA transform based multiple digital image encryption. Journal of Information Security and Applications, 2020, 54: 102592. [doi: 10.1016/j.jisa.2020.102592]

19 Zarebnia M, Pakmanesh H, Parvaz R. A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images. Optik, 2019, 179: 761–773. [doi: 10.1016/j.ijleo.2018.10.025]

20 Zhang XQ, Hu YM. Multiple-image encryption algorithm based on the 3D scrambling model and dynamic DNA coding. Optics & Laser Technology, 2021, 141: 107073.

21 Liu JY, Yang DD, Zhou HB, *et al*. A digital image encryption algorithm based on bit-planes and an improved logistic map. Multimedia Tools and Applications, 2018, 77(8): 10217–10233. [doi: 10.1007/s11042-017-5406-2]

22 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.

23 王永, 江功坤, 尹恩民. 基于二维耦合映像格子模型的图像加密. 西南交通大学学报, 2021, 56(6): 1337–1345, 1354.

24 赵洪祥, 谢淑翠, 张建中, 等. 基于改进型 Henon 映射的快速图像加密算法. 计算机应用研究, 2020, 37(12): 3726–3730.

25 Zhang L, Zhang XQ. Multiple-image encryption algorithm based on bit planes and chaos. Multimedia Tools and Applications, 2020, 79(29): 20753–20771.

26 Xu QY, Sun KH, Cao C, *et al*. A fast image encryption algorithm based on compressive sensing and hyperchaotic map. Optics and Lasers in Engineering, 2019, 121: 203–214. [doi: 10.1016/j.optlaseng.2019.04.011]

(校对责编: 牛欣悦)