

引用格式: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[J]. 微电子学与计算机,2019,36(10):96-102. [ZHU L Y,ZHANG X,ZHANG L. Design of image encryption scheme based on parallel compressive sensing and chaotic map[J]. Microelectroncs&Computer,2019,36(10):96-102.]

基于并行压缩感知与混沌映射的图像加密方案设计

朱礼亚¹,张 曦²,张 亮¹

(1 长安大学 电子与控制工程学院,陕西 西安 710064;2 空军工程大学 航空工程学院,陕西 西安 710038)

摘 要:为实现灰度图像的同步加密与压缩,将并行压缩感知技术与混沌理论相结合,提出了一种兼顾压缩性能与安全性能的加密方案.明文图像的小波系数矩阵在经过 Arnold 置乱之后,利用受控的随机分块权重测量矩阵进行线性压缩,然后进行量化和双向扩散得到密文图像.在加密过程中,Lorenz 混沌系统产生的伪随机序列作为置乱、构造测量矩阵以及扩散过程的密码流.通过置乱稀疏系数及构造具备良好重建性能的测量矩阵,方案的压缩性能得到有效提升.通过一系列安全性能分析,验证了方案的可靠性及鲁棒性.

关键词:加密系统;压缩感知;混沌映射;置乱;扩散

中图分类号: TP309.7

文献标识码: A

文章编号: 1000—7180(2019)10—0096—07

Design of image encryption scheme based on parallel compressive sensing and chaotic map

ZHU Li-ya¹,ZHANG Xi², ZHANG Liang¹

(1 School of Electrics and Control Engineering, Chang' an University, Xi'an, 710064, China;

2 School of Aeronautics and Astronautics Engineering,Air Force Engineering University, Xi'an, 710038, China)

Abstract: To encrypt and compress the gray image simultaneously, a novel encryption scheme based on parallel compressive sensing and chaotic theory is proposed, which can form a balance between compression and security performance. Firstly, the wavelet coefficients of plain image are scrambled by Arnold permutation algorithm, and then compressed by the key-controlled partial random block weighing matrix. Finally, the cipher image is obtained after quantization and diffusion. Lorenz chaotic system is introduced to generate the key stream for permutation, construction of measurement matrix and diffusion. Via scrambling the sparse coefficients and constructing the measurement matrix with high reconstruction performance, the compression performance of scheme is enhanced. Moreover, the security and robustness are demonstrated by the security analyses.

Key words: cryptosystem; compressive sensing; chaotic map; permutation; diffusion

1 引言

压缩感知理论^[1]利用信号在时域或频域上的稀疏先验性,通过线性测量进行压缩采样,并通过凸优化求解过程进行信号重建,突破了传统的奈奎斯特采样定理的限制,实现了信号采样与压缩的同步进

行,在信息论、模式识别、光学成像、无线通信等领域得到了广泛的应用,同时也为图像加密与压缩的有机结合提供了可能.

近年来,国内外学者将压缩感知应用在图像加密领域,利用测量矩阵的计算安全性,实现了图像的同时加密与压缩^[2-4].需要指出的是,利用压

压缩感知对明文图像进行加密,实质上是把测量矩阵作为加密工具,将对应的测量结果作为密文.即使该方法已被证实具有足够的计算安全性^[5],可以抵御暴力统计攻击,但其本质上属于线性测量过程,因此无法抵抗已知明文攻击和选择明文攻击^[6].因此,为保证加密方案具有足够的安全性,必须将压缩感知与传统的扩散加密算法相结合.此外,在保证加密方案安全性的前提下,通过对压缩感知理论中稀疏基、测量矩阵及重构算法的进一步改进,可有效提升同等压缩率下恢复图像的质量.因此,在基于压缩感知的图像加密方案设计过程中,需要平衡好压缩性与安全性之间的关系,同时兼顾方案的可实现性.

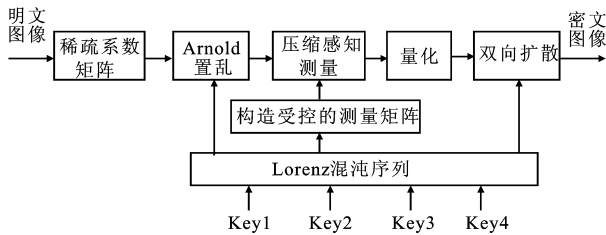


图1 加密方案流程图

2 加密方案

2.1 总体方案设计

本方案是将压缩感知与传统加密算法有机融合,在保证安全性的前提下,致力于压缩性能的提升与硬件的可实现性.张玉书等已经证明^[7],将明文图像在稀疏基下的系数矩阵先进行置乱,再进行压缩感知测量,可有效放松测量矩阵的有限等距性能 RIP(restricted isometry property),从而提升恢复图像的质量.基于此,我们提出的加密方案包括明文图像稀疏表示、系数置乱、压缩感知测量、量化及扩散5个主要部分.其中,置乱、压缩感知测量及扩散过程由Lorenz混沌系统产生的密码流控制,混沌系统的初始值可作为密钥通过秘密信道传送给接收方.本方案的加密流程如图1所示.下面对方案中涉及到的关键技术进行介绍.

2.1.1 Lorenz超混沌系统

作为典型的高维混沌系统,Lorenz超混沌系统具有两个正的李雅普诺夫指数,因而具有更复杂的动力学行为,其动力学方程为^[8]:

$$\begin{cases} \dot{x} = a(y-x) + \omega \\ \dot{y} = cx - y - xz \\ \dot{z} = xy - bz \\ \dot{\omega} = -yz + r\omega \end{cases} \quad (1)$$

式中,当 $a=10, b=8/3, c=28, r=-1$ 时,系统处于超混沌态,此时混沌系统的四个初值应满足 $x_0 \in (-40, 40), y_0 \in (-40, 40), x_0 \in (1, 81), \omega_0 \in (-250, 250)$.通过对此方程用欧拉法进行离散化,得到一组浮点数,去掉前1000个过渡态后,再将其转换为整数输出,得到对应的伪随机整数序列,并作为后续加密过程的密码流.

2.1.1 置乱

置乱是指单纯的改变图像的像素点位置,而不改变其像素值.在本方案中,明文图像经过稀疏基分解后,得到的是二维系数矩阵,因此可利用Arnold变换进行像素点的置乱,其表达式如下所示:

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_{n-1} \\ y_{n-1} \end{bmatrix} \bmod \begin{bmatrix} M \\ N \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad (2)$$

式中, (x_{n-1}, y_{n-1}) 与 (x_n, y_n) 分别表示置乱前、后的像素点位置; a 和 b 是混沌系统产生的伪随机整数序列; M 和 N 表示图像的尺寸大小.

2.1.3 量化

经过压缩感知测量之后的输出矩阵,其值一般超出 $[0, 255]$ 的灰度区间,因此,在扩散过程之前必须进行量化.量化实质上是对测量值进行线性缩放并取整,将其限制在 $[0, 255]$ 范围内.量化过程表述如下:

$$coff1 = \frac{255}{C_{\max} - C_{\min}} \quad (3)$$

$$coff2 = \frac{255 \times C_{\min}}{C_{\max} - C_{\min}} \quad (4)$$

$$Q_i = \text{round}(coff1 \times C_i - coff2) \quad (5)$$

式中, Q_i 与 C_i 分别表示量化过程中输出和输入图像的像素值; $C_{\max}$ 和 $C_{\min}$ 表示输入图像的最大值与最小值; round 表示取整操作.

相对应的,解密过程之前要进行量化的逆运算,其表达式如下:

$$P_i = \frac{C_i + coff2}{coff1} \quad (6)$$

这里,两个辅助参数 $coff1$ 和 $coff2$ 由发送方通过秘密信道传送给接收方,某种程度上也承担着密钥的作用.

2.1.4 扩散

扩散是指在不改变像素点位置的前提下,改变图像对应的像素值,使得某一位置的像素信息隐藏在尽可能多的像素点中.为获得更好的扩散效果,本方案中执行了前向和后向两次扩散过程,前向扩散及其逆算法为^[9]:

$$C_i = (C_{i-1} + S_i + P_i) \bmod 256 \quad (7)$$

$$P_i = (2 \times 256 + C_i - C_{i-1} - S_i) \bmod 256 \quad (8)$$

后向扩散及其逆算法为^[9]:

$$C_i = (C_{i+1} + S_i + P_i) \bmod 256 \quad (9)$$

$$P_i = (2 \times 256 + C_i - C_{i+1} - S_i) \bmod 256 \quad (10)$$

式中, P_i 代表明文图像的像素值; S_i 表示混沌系统生成的伪随机整数序列; C_i 、 C_{i-1} 和 C_{i+1} 分别表示密文图像的当前像素值、前向扩散和后向扩散的前一像素值.

2.2 构造受控的测量矩阵

为获得更好的信号重建性能,测量矩阵应满足:

(1) 普适性,即对于大部分稀疏基都具有不相关性;
(2) 实用性,包括快速计算、低存储量、硬件易实现等.在加密压缩过程中,将整个测量矩阵作为密钥是不现实的,因此在构造过程中,要利用尽可能少的密钥消耗量控制并构造测量矩阵.文献[10]提出了一种部分随机分块权重测量矩阵 PRBWM (Partial Random Block Weighing Matrix) 的构建方法,该矩阵在离散余弦变换、离散小波变换以及部分傅立叶变换下均表现出良好的重建性能,且主要由 0、1、-1 数值构成,便于存储和硬件实现,其构造的具体步骤如下:

(1) 构造一个大小为 $n \times n$ 的哈达玛矩阵;

(2) 将哈达玛矩阵的每个列向量与其转置相乘,得到一组矩阵集合 $\bar{\mathbf{P}} = \{\mathbf{P}_1 \ \mathbf{P}_2 \ \cdots \ \mathbf{P}_n\}$, 这里 $\mathbf{P}_i = \mathbf{R}^T \mathbf{T}_i \mathbf{R}_i$, $\mathbf{R}_i$ 为哈达玛矩阵的列向量;

(3) 构建一个大小为 $N/n \times N/n$ ($N/n \geq n$) 的循环矩阵:

$$\mathbf{L} = \begin{bmatrix} s_1 & s_2 & \cdots & s_{N/n} \\ s_{N/n} & s_1 & \cdots & s_{N/n-1} \\ \vdots & \vdots & \ddots & \vdots \\ s_2 & s_3 & \cdots & s_1 \end{bmatrix}$$

(4) 用矩阵集合中的矩阵 $\mathbf{P}_1$ 、 $\mathbf{P}_2$ 、 $\cdots$ 、 $\mathbf{P}_n$ 分别替换 $\mathbf{L}$ 矩阵中的元素 s_1 、 s_2 、 $\cdots$ 、 s_n , 剩余元素用零矩阵填充,得到一个 $N \times N$ 的矩阵 $\mathbf{L}_1$;

(5) 利用长度为 N 的伪随机整数序列作为索引,置乱矩阵 $\mathbf{L}_1$ 的列向量;

(6) 设压缩率为 CR , 将伪随机整数序列的前 M ($M = CR \times N$) 个值作为索引,选择对应的行向量,并组合成一个大小为 $M \times N$ 的矩阵 $\mathbf{L}_2$, 此为最终构造生成的受控测量矩阵 $\text{PRBWM}(n, M, N)$.

2.3 加密与解密步骤

2.3.1 加密步骤:

(1) 将大小为 $N \times N$ 的明文图像在某一稀疏基下进行分解,得到同样尺寸的系数矩阵 $\mathbf{C}_1$;

(2) 利用 Lorenz 混沌系统产生长度为 $N \times N \times 2$ 的一维伪随机整数序列 S_1 , 分成两个长度均为 $N \times N$ 的伪随机序列 a 和 b 并应用在 Arnold 变换中,将 $\mathbf{C}_1$ 中的每个元素位置进行置乱,得到矩阵 $\mathbf{C}_2$;

(3) 利用 Lorenz 混沌系统产生长度为 N 的伪随机整数序列 S_2 , 按 2.2 节中所述方法构建大小为 $M \times N$ 的测量矩阵 Φ ;

(4) 用测量矩阵 Φ 对系数矩阵 $\mathbf{C}_2$ 进行压缩感知测量,得到大小为 $M \times N$ 的密文图像 $\mathbf{C}_3$;

(5) 对密文图像 $\mathbf{C}_3$ 进行量化,得到元素值在 $[0, 255]$ 灰度区间的整数矩阵 $\mathbf{C}_4$;

(6) 利用 Lorenz 混沌系统产生长度为 $M \times N \times 2$ 的一维伪随机整数序列 S_3 , 分成两个长度均为 $M \times N$ 的伪随机序列,分别应用在前向扩散和后向扩散过程中,得到最终的密文图像 $\mathbf{C}_5$.

2.3.2 解密步骤:

解密是加密的拟过程,其步骤简述如下:

(1) 将接收到的密文图像分别进行后向扩散和前向扩散的逆运算,得到明文图像 $\mathbf{P}_1$;

(2) 利用发送方传送的两个辅助参数 coeff1 和 coeff2 进行逆向量化,得到明文图像 $\mathbf{P}_2$;

(3) 将 $\mathbf{P}_2$ 的每个列向量进行重构,并组合得到明文图像 $\mathbf{P}_3$;

(4) 对 $\mathbf{P}_3$ 进行置乱还原,得到明文图像 $\mathbf{P}_4$;

(5) 对 $\mathbf{P}_4$ 进行稀疏逆变换,得到最终的明文图像 $\mathbf{P}_5$.

3 实验

3.1 实验环境设置

仿真所用的台式计算机硬件参数为:Core i7-6700+8G RAM, 仿真软件为 MATLAB 2016a, 操作系统为 window 7 专业版. 稀疏基采用的是 Daubechies 8 小波变换, 信号重构算法选择的是重建精度高且计算量低的 SL_0 (smoothed l_0 norm) 算法, Lorenz 混沌系统的初始值设置为: $\mathbf{x}_0 = 1.13$, $\mathbf{y}_0 = 2.52$, $\mathbf{z}_0 = 3.38$, $\omega_0 = 4.64$.

3.2 压缩性能分析

选取 3 幅大小为 256×256 的灰度图像 Lena、Cameraman 以及 Fingerprint, 压缩率设置为 0.5, 测量矩阵为 pRBWM(16,128,256), 加密及解密过程如前

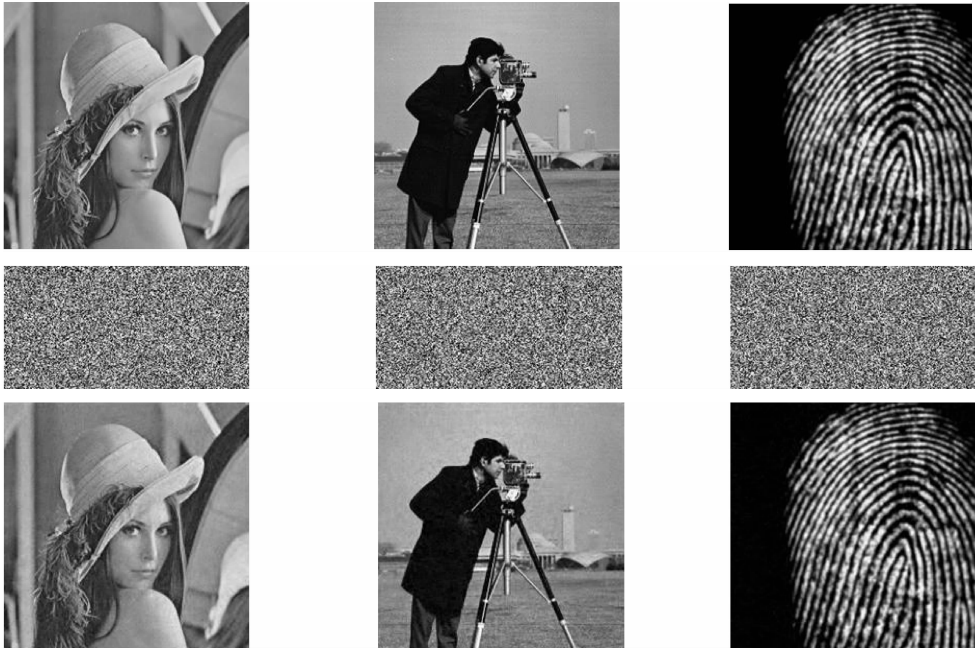


图 2 加密及解密图像效果

由图 2 可知,加密后的图像在视觉上均无法获得任何有用信息,证明了加密方案的有效性.同时,在压缩率为 0.5 时,解密图像虽然在质量上有一定的损失,但是在视觉上仍清晰可见,且 PSNR 值均超过 30 dB,表明该方案具有良好的压缩效果.

3.3 与其他方案压缩性能的比较

在压缩感知测量过程中,稀疏基的选择、测量矩阵的构造以及重构算法都会对恢复图像的质量产生影响.因此,很难在完全相同的条件下与其他算法进行比较.为做到尽可能公平,我们在相同的稀疏基(小波基)和重构算法条件下进行比较.表 1 列出了本方案以及文献[2]、[3]中得到的重构图像的 PSNR 值.由表中数据可知,当利用正交匹配追踪算法 OMP(orthogonal matching pursuit)时,在相同的压缩率下,本方案中重建图像的质量相较文献[2]提升了约 3~5 dB;当选择 SL_0 算法时,与文献[3]的结果相比,在低压缩率条件下本方案的重建图像质量略低约 1 dB,但是在中高压缩率条件下,重建图像的质量提升了约 0.5~7 dB.以上结果证明了利用置乱稀疏系数矩阵及 pRBWM 测量矩阵,可有效提升加密方案的压缩性能.

文所述,仿真结果如图 2 所示.为了衡量解密图像的质量,用解密图像与明文图像之间的峰值信噪比 PSNR(peak signal to noise ratio)值作为测试指标.

表 1 与其他方案的压缩性能比较

明文图像 (256×256)	重构 算法	压缩率	PSNR 值(dB)		
			本方案	文献[2]	文献[3]
Lena	OMP	0.3	23.32	20.02	/
		0.5	29.33	25.99	/
		0.75	34.27	29.39	/
		0.25	23.91	/	25.23
Cameraman	SL_0	0.5	30.02	/	29.43
		0.75	36.66	/	28.93

4 安全性能分析

4.1 密钥空间

为抵御暴力统计攻击,加密算法的密钥空间应大于 2^{100} . 根据 Lorenz 超混沌系统初值的取值范围, $x_0 \in (-40, 40)$, $y_0 \in (-40, 40)$, $z_0 \in (1, 81)$, $\omega_0 \in (-250, 250)$, 其中, x_0 、 y_0 和 z_0 的步长为 10^{-13} , ω_0 的步长为 10^{-12} , 所以本方案的密钥空间为:

$$S = 2.56 \times 1059 \approx 2197 \tag{11}$$

其值远远大于 2^{100} , 因此本方案的密钥空间足以抵御暴力统计攻击.

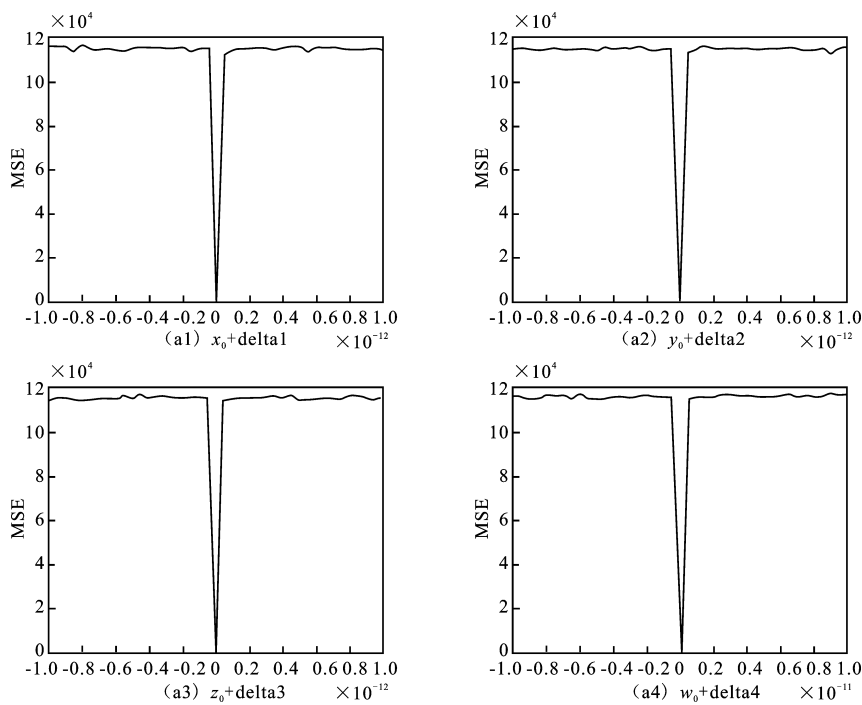


图 3 密钥偏差时对应的 MSE 曲线

4.2 密钥敏感性

密钥敏感性指的是当接收方使用的密钥有微小变化时,解密图像相对于明文图像有显著差异,无法得到任何有价值的信息.在仿真实验中,将 Lena 设置为明文图像,假设某一密钥出现微小偏差而其他密钥均正确,计算解密图像与明文图像之间的均方误差 MSE(Mean Square Error),图 3 给出了四个密钥变化时对应的 MSE 曲线.可见,只有当密钥完全正确时,MSE 的值很小;而当任何一个密钥出现微小偏差时,解密图像的 MSE 值都较大,因此本方案具有较好的密钥敏感性.

4.3 密文统计特性

4.3.1 直方图分析

为防止攻击者从密文直方图中获得有用的统计信息而增加破译的概率,密文图像的灰度直方图应呈现类似白噪声一样的分布.图 4 给出了明文图像和对应密文图像的灰度直方图,由图可见,明文图像的像素分布呈现特定规律,而加密图像的直方图很平坦,表明每一像素出现的次数近乎相等,攻击者从中无法获得任何有用信息.

4.3.2 相关系数

明文图像相邻像素之间往往具有较强的相关性,表现在水平、垂直和对角方向上的相关系数都接近 1.而经过性能良好的加密系统得到的密文图像,其相邻像素之间的相关系数在各个方向上应趋近于

0.在明文图像和对应的密文图像中,我们随机选取了 8000 对相邻像素,分别计算了其在水平、垂直、正对角、反对角方向的相关性,计算表达式如下:

$$r_{xy} = \frac{\sum_{i=1}^N (x_i - E(x))(y_i - E(y))}{\sqrt{(\sum_{i=1}^N (x_i - E(x))^2)(\sum_{i=1}^N (y_i - E(y))^2)}} \quad (12)$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad E(y) = \frac{1}{N} \sum_{i=1}^N y_i \quad (13)$$

式中, x_i 和 y_i 分别表示一对相邻像素的灰度值; N 为选取的像素数量.为消除随机性,重复计算 100 次后取平均值作为最终结果,如表 2 所示.

表 2 相邻像素之间的相关系数

图像	水平	垂直	正对角	反对角
Lena(明文)	0.959 4	0.929 8	0.899 3	0.919 6
Lena(密文)	-0.005 4	-0.003 0	0.003 4	-0.001 3
Camerman(明文)	0.960 7	0.931 1	0.898 7	0.918 0
Camerman(密文)	-0.008 5	-0.000 4	0.005 4	-0.001 4

由表中数据可知,明文图像相邻像素之间的相关性较强,而经过加密得到的密文图像的在四个方向上接近于 0,呈现出近似无相关性.

4.4 明文敏感性分析

选择明文攻击或已知明文攻击指的是攻击者对某一确定的明文图像做微小变化后,利用同一密钥

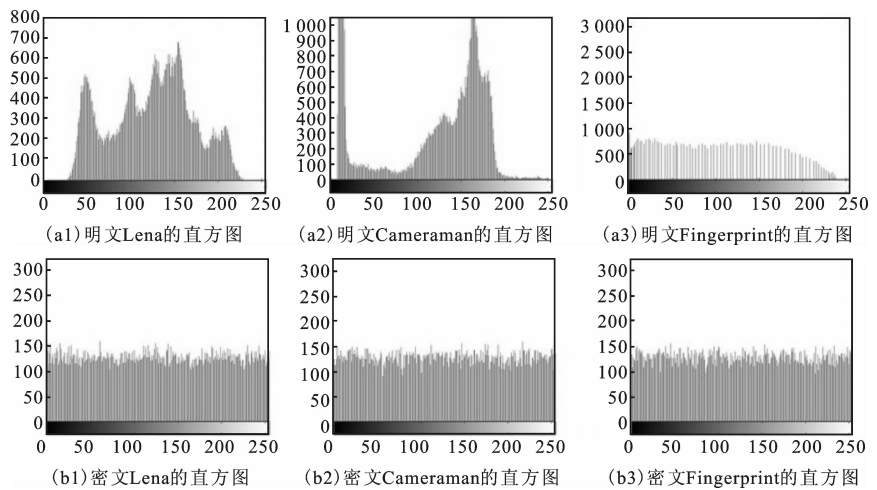


图 4 明文图像及密文图像的灰度直方图

分别进行加密,通过对两幅密文图像的对比,找出明文图像与加密图像之间的联系.为抵御此类攻击,加密算法应具有较强的明文敏感性,即差别微小的两个明文图像经过加密之后应具有显著差异.衡量两幅图像差别的指标主要包括像素改变率 NPCR (number of pixels change rate) 和一致平均改变强度 UACI(unified average changing intensity),前者反映了不同像素点的个数占全部像素点的比例,后者反映了相应位置像素点的差值与 255 比值的平均值.其表达式分别如下:

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N D(i,j) \times 100\% \quad (14)$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N \frac{|I_1(i,j) - I_2(i,j)|}{255} \times 100\% \quad (15)$$

$$D(i,j) = \begin{cases} 1, & I_1(i,j) \neq I_2(i,j) \\ 0, & I_1(i,j) = I_2(i,j) \end{cases} \quad (16)$$

式中, $I_1(i,j)$ 和 $I_2(i,j)$ 分别表示两幅图像中对应像素点的灰度值.两幅随机图像的 NPCR 和 UACI 理论期望值分别为 99.6094% 和 33.4635%.越接近理论值,表明加密方案的明文敏感性越强.

在实验中,随机选择明文图像 P_1 中的 1 个像素点,并将其像素值的变化量设为 1,记为 P_2 ,将 P_1 和 P_2 使用相同的密钥加密后,得到对应的密文图像 C_1 和 C_2 ,并计算其 NPCR 和 UACI 值.为消除随机性,以上步骤重复 100 次取平均值,结果如表 3 所示.由表中数据可知,三幅不同明文图像的测试结果均接近理论值,表明本文提出的加密方案具有良好的明文敏感性,可以有效抵御选择明文攻击和已知明文攻击.

表 3 明文敏感性分析结果

	Lena	Cameraman	Fingerprint	理论值
NPCR(%)	99.369 2	99.154 7	99.309 4	99.609 4
UACI(%)	33.195 2	33.389 5	33.156 2	33.436 5

4.5 鲁棒性分析

为定量评价加密算法在各种噪声环境下的抗干扰能力,我们对 Lena 的密文图像添加了三中不同类型的噪声,包括高斯噪声 GN(gaussian noise)、椒盐噪声 SPN(salt& pepper noise)以及斑点噪声 SN(speckle noise),归一化噪声强度依次设为 0.000001~0.000007,并计算解密图像的 PSNR 值,图 5 绘出了在不同噪声环境下 PSNR 值与噪声强度之间的关系曲线.

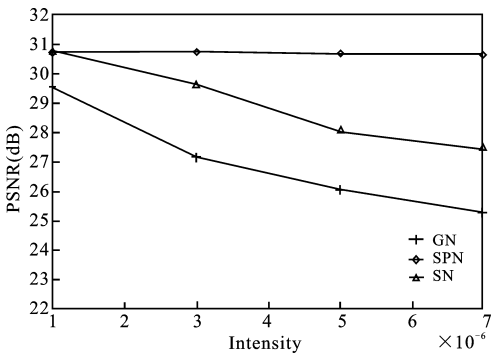


图 5 不同噪声环境及强度下的解密图像质量曲线

由图可知,高斯噪声对于加密系统的影响最大,表现在随着噪声强度的变大,其 PSNR 变化曲线下滑最为明显;椒盐噪声的影响最小,表现在 PSNR 值几乎没有变化,斑点噪声对于加密系统的影响介于二者之间.因此,该加密方案对椒盐噪声的抗干扰能力最强,同时也可以抵御一定的斑点噪声和高斯

噪声攻击.

5 结束语

本文提出了一种基于并行压缩感知和混沌映射的灰度图像加密方案,通过压缩感知与传统加密算法的结合,可实现灰度图像的同步加密和压缩.通过置乱稀疏系数和构造受控的测量矩阵,得到了质量较好的解密图像.同时,相关的安全性分析结果也证明了本方案的有效性和可靠性.

参考文献:

- [1] DonohoDavid L. Compressed sensing [J]. IEEE Transactions on Information Theory, 2006, 52(4): 1289-1306.
- [2] HU G P, XIAO D, WANG Y, et al. An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications [J]. Journal of Visual Communication and Image Representation, 2017, 44: 116-127.
- [3] CHAI X L, ZHENG X Y, GAN Z H, et al. An image encryption algorithm based on chaotic system and compressive sensing [J]. Signal Processing, 2018, 148: 124-144.
- [4] CHEN J X, ZHANG Y, QI L, et al. Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression [J]. Optics and Laser Technology, 2018, 99: 238-248.
- [5] RachlinYaron, BaronDror. The secrecy of compressed sensing measurements [C]// 46th Annual Allerton

Conference on Communication, Control, and Computing, Monticello:IEEE, 2008: 813-817.

- [6] ZHANG L Y, WONG K W, ZHANG Y S, et al. Bi-level protected compressive sampling [J]. IEEE Transactions on Multimedia, 2016, 18 (9): 1720-1732.
- [7] ZHANG Y S, ZHOU J T, CHEN F, et al. Embedding cryptographic features in compressive sensing [J]. Neurocomputing, 2016, 205: 472-480.
- [8] ZHANG Y. A chaotic system based image encryption scheme with identical encryption and decryption algorithm [J]. Chinese Journal of Electronics, 2017, 26(5): 1022-1031.
- [9] 张勇. 混沌数字图像加密 [M]. 北京: 清华大学出版社, 2016.
- [10] ZHAO H, YE H, WANG R Y. The construction of measurement matrices based on block weighing matrix in compressed sensing [J]. Signal Processing, 2016, 123: 64-74.

作者简介:

朱礼亚 男,(1980-),硕士,工程师.研究方向为图像处理与信息安全.

E-mail:lyzhu@chd.edu.cn.

张 曦 男,(1979-),博士,副教授.研究方向为信号处理与模式识别.

张 亮 男,(1983-),硕士,工程师.研究方向为网络空间安全.