计算机科学
COMPUTER SCIENCE

基于压缩感知和超混沌系统的图像压缩加密方法

潘涛，佟晓筠，张淼，王翥

引用本文

潘涛，佟晓筠，张淼，王翥.基于压缩感知和超混沌系统的图像压缩加密方法[J]．计算机科学, 2023, 50(6A): 220200121-6.

PAN Tao, TONG Xiaojun, ZHANG Miao, WANG Zhu. Image Compression and Encryption Based on Compressive Sensing and Hyperchaotic System [J]. Computer Science, 2023, 50(6A): 220200121-6.

相似文章推荐（请使用火狐或 IE 浏览器查看文章）

Similar articles recommended (Please use Firefox or IE to view the article)

基于残差特征聚合的图像压缩感知注意力神经网络

Image Compressed Sensing Attention Neural Network Based on Residual Feature Aggregation

计算机科学, 2023, 50(4): 117-124. https://doi.org/10.11896/jsjkx.211200215

传感器唤醒机制下的智能干扰源定位方法

Intelligent Jammers Localization Scheme Under Sensor Sleep-Wakeup Mechanism

计算机科学, 2022, 49(11A): 211000165-6. https://doi.org/10.11896/jsjkx.211000165

基于深度神经网络的块压缩感知图像重构

Block-based Compressed Sensing of Image Reconstruction Based on Deep Neural Network

计算机科学, 2022, 49(11A): 210900118-9. https://doi.org/10.11896/jsjkx.210900118

基于离散动力学反控制的混沌序列密码算法

Chaotic Sequence Cipher Algorithm Based on Discrete Anti-control

计算机科学, 2022, 49(4): 376-384. https://doi.org/10.11896/jsjkx.210300116

面向分块压缩感知的交叉子集导引自适应观测

Cross Subset-guided Adaptive Measurement for Block Compressive Sensing

计算机科学, 2020, 47(12): 190-196. https://doi.org/10.11896/jsjkx.200800197

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220200121

基于压缩感知和超混沌系统的图像压缩加密方法

潘　涛[1]　佟晓筠[1]　张　淼[1]　王　轰[2]
1 哈尔滨工业大学(威海)计算机科学与技术学院　山东 威海 264209
2 哈尔滨工业大学(威海)信息科学与工程学院　山东 威海 264209
(pantaocolor@163.com)

摘　要　在医疗、军事、金融系统等需要传输重要图像的场景下,为了安全高效地传输图像,将图像进行压缩加密是一种行之有效的办法,图像经过压缩后传输可以减小传输开销,经过加密后也可以抵抗一些攻击者的攻击手段,保证了信息的安全性。基于压缩感知理论可以完成稀疏采样,超混沌系统能够为系统安全性提供保障。同时,文中还分析了超混沌系统的混沌特性,证明了该系统是混沌的且足够安全,超混沌系统生成的混沌序列还被用于构造测量矩阵,从而不必在传输过程中传输文本较大的矩阵,而只需要传输密钥即可。在压缩理论基础上还使用了置乱扩散操作,扩散采用了与明文相关的扩散操作,使图像安全性得到了很大提升,保障了数据安全。经过实验测试,图像的压缩加密效果较好,密钥空间大、对密钥足够敏感,说明所提方法能够抵抗暴力攻击、统计攻击等多种常用的攻击方法;在压缩比正常的情况下恢复得到的解密图像与原文图像在视觉上差距较小,甚至与原文图像相差无几,说明该算法重构质量较好,安全性较高。

关键词:混沌系统;压缩感知;压缩加密;视觉安全;图像安全
中图法分类号　TP309.7

Image Compression and Encryption Based on Compressive Sensing and Hyperchaotic System

PAN Tao[1],TONG Xiaojun[1],ZHANG Miao[1] and WANG Zhu[2]
1 School of Computer Science and Technology,Harbin Institute of Technology,Weihai,Shandong 264209,China
2 School of information science and Engineering,Harbin Institute of Technology,Weihai,Shandong 264209,China

Abstract　In medical,military,financial systems and other scenarios where important images need to be transmitted,image compression and encryption is a feasible and effective way to transmit images safely and efficiently. Image compression and transmission can reduce the transmission overhead. Compressed images can be encrypted to make images more secure,and ordinary people can not get key information from them. After encryption,it can also resist some attacks means to ensure the security of information. Based on the compression perception theory,sparse sampling can be completed,and images can be compressed to any scale. Hyperchaotic system can guarantee the security of the system. Chaotic characteristics such as Lyapunov exponents of hyperchaotic system are also analyzed. It is proved that the system is chaotic and safe enough. Chaotic sequences generated by hyperchaotic system are also used to construct measurement matrix. This eliminates the need to transfer a matrix with large text during transmission,but only the key. On the basis of compression theory,scrambling diffusion operation is also used,and diffusion operation related to plain text is used,which greatly improves image security and ensures data security. Experiments show that the image is compressed and encrypted well,the key space is large,the key is sensitive enough,the cipher histogram is distributed evenly,the cipher information entropy is close to the theoretical value,and the correlation between cipher images is low,which shows that it can resist many common attacks such as violent attacks and statistical attacks. At the same time,the decrypted image restored under normal compression ratio has a small visual gap with the original image,even if the compression ratio is small,most of the information content of the image can be seen,which indicates that the algorithm has a good reconstruction quality and high security.

Keywords　Chaotic system,Compressed sensing,Compression encryption,Visual safety,Image security

基金项目:国家自然科学基金(61902091);山东省自然科学基金(ZR2019MF054)
This work was supported by the National Natural Science Foundation of China(61902091) and Natural Science Foundation of Shandong Province,China(ZR2019MF054).
通信作者:佟晓筠(tong_xiaojun@163.com)

1 引言

随着信息技术的不断发展，许多领域对信息安全的重视程度不断加强，如何研究出一个图像领域加密后快速传输的方法是一个亟需解决的问题。通过压缩图像可以在传输大规模图片时节省带宽、提高传输速率，通过使用加密操作可以保证信息传输时的安全，从而应用在更多对保密性要求高的领域，将压缩与加密相结合是值得研究的重要方向，有着较强的现实意义。

压缩感知由于可以在不丢失重要信息的情况下实现亚尼奎斯特采样率，所以被广泛用于图像信号处理领域。除了一维压缩感知，一些学者通过使用二维压缩感知并加入新的压缩方案来实现更好的压缩效果，避免了图像信息广泛丢失，例如 Zhang 等[1]提出了一种新的基于 2DCS 的 ETC(2DCS-ETC)压缩方案，利用两种非线性操作全局随机排列(GRP)和负正变换(NPT)，该压缩方案的特点是并不直接对图像进行采样，而是将图像灰度值映射到[−128,128]区间内后进行采样。该算法进行图像重构时效率也快于一般的方法，这种压缩方案与一般的压缩方案相比，从视觉质量上看，效果最好。Chai 等[2]提出了一种基于压缩感知和双随机加密策略的彩色图像压缩与加密方案，该算法使用了双随机位置排列，由两次索引序列来置乱图像像素位置，降低了像素间的相关性。该算法可以同时实现图像数据安全和图像外观安全，且密文图像和原始图像的大小相等，缺点是解密运行时间较长。Wang 等[3]提出了基于像素值调整策略的绝对矩块截断编码(AMBTC)压缩图像的自适应可逆数据隐藏方案，AMBTC 压缩图像域中，将原始图像分割成大小相等的块，每个块被 AMBTC 压缩，得到量化值 L、H 和比特位图 B，根据这些值来进行相应的嵌入操作，因为这些值与明文图像有相关性，所以该方案能够根据不同的图像自适应嵌入，同时恢复图像的 PSNR 值更好。Liu 等[4]提出了一种基于压缩感知和分数傅里叶域混沌的图像加密算法。明文图像经过压缩感知降维后在分数傅里叶变换域中使用基于混沌的双随机相位编码技术对测量值进行加密。加密过程中使用的测量矩阵和随机相位掩模是由混沌映射生成的伪随机序列组成。该算法结合了光学域变换来对信号进行处理，提高了压缩加密速度，同时也保证了安全性。Lu 等[5]提出了一种基于压缩感知和双随机相位编码的图像信息加密方法。该方法采用基于无理数序列的具有较小随机相位掩码的双随机相位编码技术，对低数据量的测量值进行重新加密，然后将双加密的信息分散并嵌入到主机映像中。在接收的终端上，通过正交匹配追踪算法近似地重建原始图像信息。数值实验表明，该加密方案具有加密数据量低、信息安全性高等特点。Huang 等[6]设计了一种由置扰、混合、S-box 和混沌晶格 XOR 组成的块密码结构，对量化的测量数据进行进一步加密。特别是，该方法在并行计算环境下工作非常有效。此外，通信单元在多个处理器之间交换数据而不发生冲突。这种无碰撞的特性等价于最优扩散。实验结果表明，该加密方法不仅具有显著的混淆、扩散和灵敏度，而且在可压缩性和加密速度方面都优于现有的并行图像加密方法。

本文基于超混沌 Chen 系统设计了一套压缩加密算法，置乱操作为二维猫映射，扩散操作采用了与明文相关联的操作，同时使用了正交匹配追踪法(OMP)来完成图像重构操作，该算法保证了图像压缩后再重建的视觉质量，同时运行效率较高，安全性较好。

2 超混沌 Chen 系统

混沌是确定的非线性系统表现出的一种貌似无规则、类随机的现象，混沌意味着杂乱无序，是一种无序状态。混沌系统是一个非线性动力系统，它能产生具有良好随机性、非相关性和复杂性的混沌序列，且具有初始值和参数的敏感性，非常适用于加密。式(1)为超混沌 Chen 系统的数学表达公式[7]：

$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=-xz+dx+cy-w\\ \dot{z}=xy-bz\\ \dot{w}=x+k\end{cases} \tag{1}$$

2.1 Lynapunov 指数

描述混沌系统性能的重要指标之一是 Lyapunov 指数(LE 指数)，它表达了混沌运动轨道的分离速度。经典的一维混沌系统一般有一个正的 Lyapunov 指数，且正的 Lyapunov 指数越高，混沌行为越复杂，更适合用于加密。本文使用的超混沌 Chen 系统是一个四维混沌系统，我们仿真测试了该系统的 LE 指数，如图 1 所示。当参数 $a=36$，$b=3$，$c=28$，$d=16$ 且 $-0.7\leqslant k\leqslant 0.7$ 时，该系统处于混沌状态，本文 k 取 0.2，仿真结果为 $LE1=1.748\,006$，$LE2=0.008\,908$，$LE3=-0.094\,690$，$LE4=-12.662\,224$，其中有两个正的 LE 指数，说明该系统是混沌的。LE 指数越高，说明系统有更复杂的混沌行为，用于加密时安全性能更好。

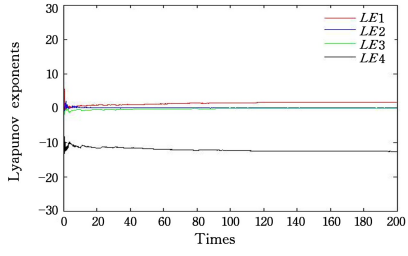


图 1 Lyapunov 指数

Fig. 1 Lyapunov exponents

2.2 奇怪吸引子

奇怪吸引子是耗散系统混沌现象的另一个重要的特征。奇怪吸引子就是相空间的一个有限的区域内，由无穷多个不稳定点集组成的一个集合体，它们稳定地收敛于一个稳定的轨道。虽然从整体来看是稳定的，但是从局部来看有部分是不稳定的。如果一个吸引子具有初值敏感性，那么它就是奇怪吸引子。经过测试，超混沌 Chen 系统的相点轨迹图如图 2—图 5 所示。

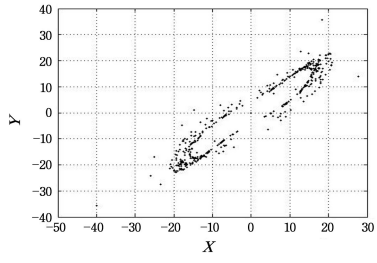


图 2 x-y 相点轨迹图

Fig. 2 x-y phase point trajectory diagram

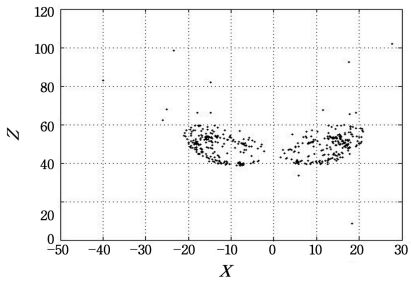


图 3　x-z 相点轨迹图

Fig. 3　x-z phase point trajectory diagram

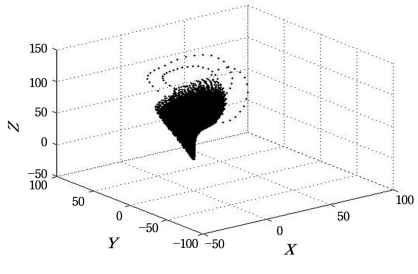


图 4　x-y-z 相点轨迹图

Fig. 4　x-y-z phase point trajectory diagram

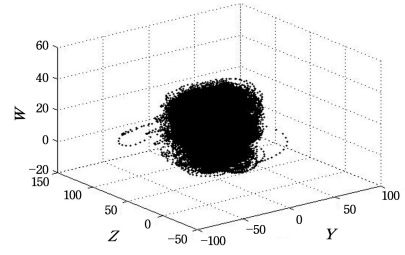


图 5　y-z-w 相点轨迹图

Fig. 5　y-z-w phase point trajectory diagram

3　基于超混沌系统和压缩感知的图像加密算法

3.1　压缩感知

压缩感知是一种新的采样理论，通过这种技术可以在不丢失重要信息的情况下实现亚尼奎斯特采样率[8]。当一个信号是稀疏的或者被稀疏表示后，即便该信号远低于奈奎斯特采样率，仍然可以保证信号被无失真地重构。压缩感知过程如式(2)所示：

$$Y=\boldsymbol{\Phi}X=\boldsymbol{\Phi}\psi S=\boldsymbol{\Theta}S \tag{2}$$

其中，稀疏基 $\boldsymbol{\Phi}$ 为大小 $M\times N$ 的测量矩阵，$\boldsymbol{\Theta}$ 为传感矩阵。在重构阶段，需要对式(2)进行求解，由于未知数 N 大于测量方程 M，所以一般方法无法求得信号 X，我们通过增加约束条件来进行求解，对于 Ψ 域上的信号 X，求解 Ψ 域上最系数的向量，即 l_0 范数最小，如式(3)所示[8-10]：

$$\begin{aligned}&(l_0)\theta^{(0)}=\arg\min_{\theta\in R^N}\|\theta\|_0\\&\text{s. t. } y=\boldsymbol{\Phi}X=\boldsymbol{\Theta}S\end{aligned} \tag{3}$$

这是一个 NP 难的非凸优化问题，一般通过松弛技术来逼近凸问题。求解凸问题的方法(即常用的恢复信号的方法)有基追踪法(BP)、正交匹配追踪法(Orthogonal Matching Pursuit，OMP)和平滑的 l_0 范数(SL_0)等，本文将采用正交匹配追踪法(OMP)来进行信号重构。

3.2　测量矩阵构造

迭代超混沌 Chen 系统 $M\times N+l_0$ 次，为了避免瞬时效应，舍弃前 l_0 次，得到长为 $M\times N$($M\times N$ 为原始图像的大小)的混沌序列$\{x_i,y_i,z_i,w_i\}$，通过式(4)得到一个新的混沌序列 t_i：

$$t_i=\mathrm{mod}\left(\frac{(x_i+y_i+z_i+w_i)}{4}*10^{14},256\right) \tag{4}$$

然后用式(5)来构造测量矩阵：

$$\boldsymbol{\Phi}=\sqrt{\frac{2}{M}}\begin{bmatrix}t_1 & t_{M+1} & \cdots & t_{(M-1)\times N+1}\\ t_2 & t_{M+2} & \cdots & t_{(M-1)\times N+2}\\ \cdots & \cdots & \cdots & \cdots\\ t_M & t_{2M} & \cdots & t_{M\times N}\end{bmatrix} \tag{5}$$

3.3　图像压缩加密方法

步骤 1　读取大小为 $M\times N$ 的原始图像，利用多维离散小波变换进行信号稀疏，得到稀疏系数 c_1，设置阈值 Threshold，对 c_1 进行稀疏化。

步骤 2　对稀疏化后的 c_1 进行 Arnold 置乱操作，具体步骤如式(6)所示，得到置乱后的系数 c_2：

$$\begin{pmatrix}x_{n+1}\\y_{n+1}\end{pmatrix}=\begin{pmatrix}1 & b\\ a & 1+a\times b\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}\bmod\begin{pmatrix}M\\N\end{pmatrix} \tag{6}$$

其中，x，y 为 c_1 的矩阵坐标位置，x_{n+1}，y_{n+1} 为变换后的矩阵坐标位置。

步骤 3　对 c_2 进行压缩感知操作，具体步骤如式(7)所示：

$$c_3=\boldsymbol{\Phi}c_2 \tag{7}$$

其中，$\boldsymbol{\Phi}$ 为 3.2 节构造出的测量矩阵，大小为 $M\times N$。

步骤 4　对压缩感知后的结果 c_3 进行一次量化操作，具体步骤如式(8)所示：

$$D_i=floor\left(\frac{255*(c_3-\min)}{\max-\min}\right) \tag{8}$$

步骤 5　对 c_4 进行异或操作得到最终的加密图像 P，具体步骤如下：

$$P_1=D_1\oplus t_1 \tag{9}$$

$$E_i=D_{i-1}\lll \bmod(x_i*10^{14},4) \tag{10}$$

$$P_i=(E_i+c_3(i))\oplus t_i \tag{11}$$

其中，x_i，t_i 为 3.1 节中的混沌序列，式(10)对异或结果进行了循环左移，$i=2,3,\cdots,M\times N$。

3.4　基于正交匹配追踪法的解密方法

步骤 1　获得初始密钥，迭代超混沌 Chen 系统得到混沌序列$\{x_i,y_i,z_i,w_i\}$，通过式(4)计算得到序列 t_i，并生成测量矩阵。

步骤 2　对密文图像进行异或逆运算。

步骤 3　采用 OMP 方法对信号进行重构得到重构后的信号。

步骤 4　对重构信号进行 Arnold 逆变换得到小波系数。

步骤 5　对小波系数进行多维离散小波变换逆变换，得到最终的解密图像。

4　实验仿真与结果分析

实验对密钥空间、密钥灵敏度、统计性能、抗攻击性能和时间复杂度分析等性能进行了安全评估。本次实验选取美国南加州大学信号与图像处理研究所(SIPI)图像数据库的杂项数据集作为测试数据集。

4.1　实验结果

本次实验对 Lena，Female，Tree，House，Cameraman 这 5

张经典图像(大小均为 256 * 256)分别进行了压缩加密实验，如图 6 所示。初始密钥$\{x_0, y_0, z_0, w_0, k\}$分别为{36, 3, 28, 16, 0.2}，压缩比为 0.5，解密后图像与原文图像在视觉上差距较小，说明本文方法的压缩性能、恢复性能较好。

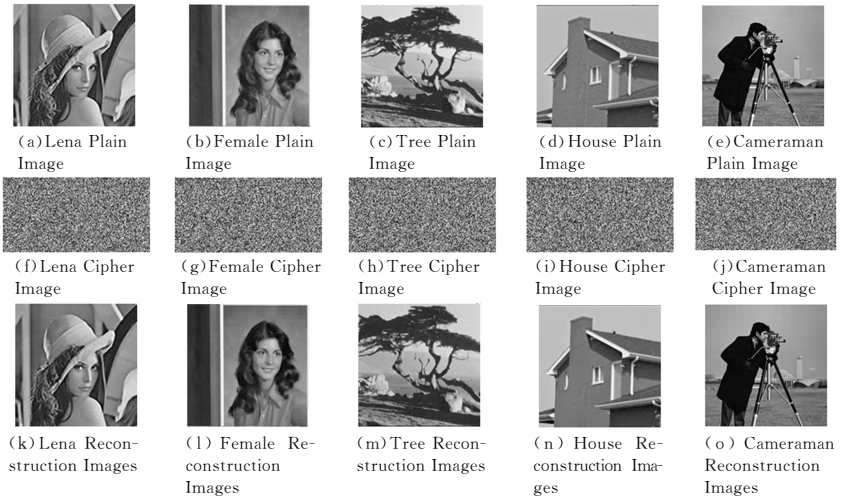


图 6 压缩加密结果及重构结果

Fig. 6 Compression & encryption results and reconstruction results

4.2 压缩性能分析

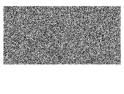
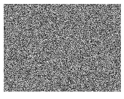
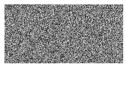
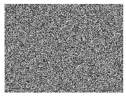
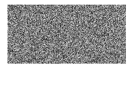
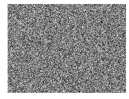
本次实验是有损压缩，图像在不同的压缩比下有着不同的压缩性能，同时恢复的图像的视觉质量也是衡量压缩性能的一项指标，通常用峰值信噪比(PSNR)来计算原始图像与重构图像对应像素点的差异，从而衡量图像质量，PSNR 的计算式如式(12)所示：

$$MSE=\frac{1}{N\times N}\sum_{i=1}^{N}\sum_{j=1}^{N}(X(i,j)-Y(i,j))^2$$
$$PSNR=10\times\log_{10}\left(\frac{255\times 255}{MSE}\right) \tag{12}$$

我们分别设置压缩比为 0.25，0.5 和 0.75，对压缩加密结果和重构质量进行分析，结果如表 1 所列。

表 1 不同图像重建的 PSNR 值

Table 1 PSNR values of different image reconstruction

Items	Compressive Ratio		
	0.25	0.5	0.75
Images			
Encrypted Images	  	  	  
Reconstruction Images	  	  	  
PSNR/dB	20.4237	32.1584	29.4786	20.9657	30.6362	28.2741	13.3599	21.3101	22.6998

当压缩比为 0.25 时，重构图像视觉损失较大，但仍然可以获取图像的大部分信息；当压缩比为 0.5 时，图像的视觉质量和原始图像差距较小，说明本文算法可以较好地完成压缩加密和重构加密后的图像，并保证视觉质量。

同时本文以 Lena(256 * 256)灰度图像作为样本与其他文献进行了对比测试，结果如表 2 所列。从对比结果可以看到，在不同压缩比下，本文方法重构效果明显好于其他算法。

表 2 不同方法重建图像的 PSNR 比较

Table 2 PSNR comparison of different methods for image reconstruction

(单位：dB)

Methods	CR(0.25)	CR(0.5)	CR(0.75)
Ours	20.42	32.16	29.48
[11]	26.56	29.83	31.62
[12]	26.06	29.82	29.56
[13]	26.52	29.23	29.22
[14]	17.41	25.99	30.68

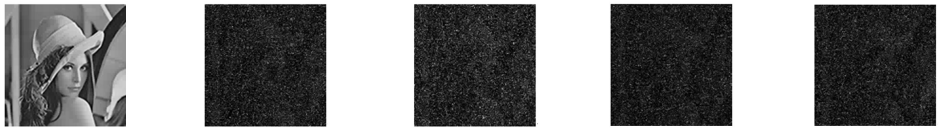
4.3 密钥空间分析

密钥空间决定了该算法抵抗暴力攻击的能力，通常密钥空间越大，抵抗暴力攻击能力越强，该算法共有$\{x_0, y_0, z_0, w_0, k\}$ 5 个密钥，当计算机浮点精度达到10^{-14}时，密钥空间为

$(10^{14})^5 \approx 2^{333}$，足以抵抗暴力攻击。

4.4　密钥敏感性分析

一个加密算法足够安全时，即便密钥发生了极其微小的改变，都会使解密失败，这也是评估算法是否安全的一项指标之一，通过对$\{x_0, y_0, z_0, w_0\}$加减10^{-14}来解密图像，得到的结果如图 7 所示。结果显示，即便改变微小值，也无法正确解密出明文图像，说明该算法对密钥足够敏感。



(a) Correct key decryption result　(b) Decryption result with x_0+10^{-14}　(c) Decryption result with y_0+10^{-14}　(d) Decryption result with z_0+10^{-14}　(e) Decryption result with w_0+10^{-14}

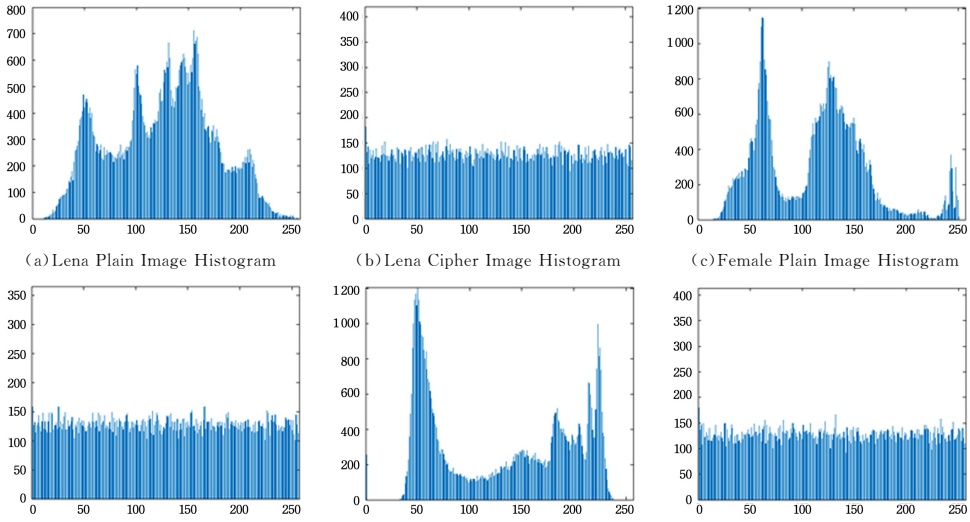
图 7　Lena 图像密钥敏感性测试结果(压缩比为 0.5)

Fig. 7　Key sensitivity test results with Lena image(compression ratio is 0.5)

4.5　统计攻击分析

4.5.1　直方图分析

直方图反映了图像的灰度分布，当一个加密算法的加密效果越好，它的分布就越均匀，攻击者就无法从直方图中得到相关信息。我们测试了 Lena，Female，Tree(256 * 256)在压缩比为 0.5 下的加密结果图的直方图，如图 8 所示。图 8(a)、图 8(c)、图 8(e)为明文图像直方图，图 8(b)、图 8(d)、图 8(f)为密文图像直方图，可以看到经过算法加密，密文图像直方图变得十分均匀，攻击者无法从统计特性去攻击该算法。



(a) Lena Plain Image Histogram　(b) Lena Cipher Image Histogram　(c) Female Plain Image Histogram

(d) Female Cipher Image Histogram　(e) Tree Plain Image Histogram　(f) Tree Cipher Image Histogram

图 8　明文与压缩比为 0.5 密文的直方图

Fig. 8　Histogram of plain image and cipher image(compression ratio is 0.5)

4.5.2　相邻像素相关性分析

相邻像素相关性反映图像相邻位置像素值的相关程度。好的图像加密算法能够降低相邻像素的相关性，尽量达到零相关。一般要分析图像的水平、垂直、对角像素 3 个方面。相邻像素 x 与 y 之间的相关系数定义如式(13)所示：

$$\rho_{x,y}=\frac{cov(x,y)}{\sqrt{D(x)D(y)}} \tag{13}$$

我们测试了 Lena，Female，Tree(256 * 256)在压缩比为 0.5 下的加密结果图的相邻像素相关性，结果如表 3 所列，同时与其他文献方法进行了对比，结果如表 4 所列。结果显示，加密后 3 个方向向量的相关系数明显下降，十分趋近于 0，说明该算法显著降低了相邻像素的相关性。

表 3　不同图像的相关性分析

Table 3　Correlation analysis of different images

Images	Plain image			Cipher image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9636	0.9814	0.9374	0.0246	−0.0367	0.0111
Female	0.9729	0.9850	0.9591	0.0175	0.0059	0.0185
Tree	0.9692	0.9480	0.9263	−0.0235	0.0345	0.0081

表 4　不同算法 Lena 图像相关性对比

Table 4　Correlation coefficients of Lena image for different algorithms

Methods	Horizontal	Vertical	Diagonal
Plain image	0.9636	0.9814	0.9374
Ours	0.0246	−0.0367	0.0111
[14]	0.0042	−0.0043	0.0163
[15]	0.0198	0.0141	0.0026
[16]	0.0024	0.0580	0.0270

4.5.3　信息熵

信息熵的计算式如式(14)所示：

$$H(x)=\sum_{i=0}^{T-1}p(x_i)\log\frac{1}{p(x_i)} \tag{14}$$

信息熵的理想值为 8，密文图像越接近于 8，其随机性越好。我们测试了 Lena，Female，Tree，House，Cameraman (256 * 256)在压缩比为 0.5 下的加密结果图的信息熵，结果如表 5 所列。结果显示，密文图像的信息熵均接近于 8，说明随机性较好。

表 5 图像的信息熵

Table 5 Information entropy of images

Images	Plain Image Information Entropy	Cipher Image Information Entropy
Lena	7.5446	7.9936
Cameraman	3.2523	7.9946
Female	7.2575	7.9948
House	6.4961	7.9949
Tree	7.3103	7.9937

结束语 本文使用了超混沌 Chen 系统来生成混沌序列并应用到加密算法中，其密钥空间大、随机性好，能够抵抗不同类型的攻击。此外，使用了多维离散小波变换和压缩感知理论来对图像信号进行稀疏变换和压缩。为了让密文图像更加安全，我们不仅进行了置乱，同时还应用了与明文相关联的扩散操作，经过实验仿真，该算法有着较好的加密效果，同时，其在低压缩比的情况下也可以恢复出图像，并且能够保证视觉质量。测量矩阵的性能还存在一些不足，以后可以设计一个优化测量矩阵的算法，从而改进图像的重构性能。

参 考 文 献

[1] ZHANG B, XIAO D, XIANG Y. Robust Coding of Encrypted Images via 2D Compressed Sensing[J]. IEEE Transactions on Multimedia, 2020, 23: 2656-2671.

[2] CHAI X, BI J, GAN Z, et al. Color image compression and encryption scheme based on compressive sensing and double random encryption strategy[J]. Signal Processing, 2020, 176: 107684.

[3] WANG X, CHANG C, LIN C. Adaptive reversible data hiding scheme for AMBTC compressed images[J]. Multimedia Tools and Applications, 2020, 79: 6547-6568.

[4] LIU X, MEI W, DU H. Optical image encryption based on compressive sensing and chaos in the fractional Fourier domain[J]. Journal of Modern Optics, 2014, 61: 1570-1577.

[5] LU P, XU Z, LU X, et al. Digital image information encryption based on Compressive Sensing and double random-phase encoding technique[J]. Optik, 2013, 124(16): 2514-2518.

[6] HUANG R, RHEE K H, UCHIDA S. A parallel image encryption method based on compressive sensing[J]. Multimed Tools Application, 2014, 72: 71-93.

[7] CHEN G, UETA T. Yet Another Chaotic Attractor[J]. International Journal of Bifurcation and Chaos, 1999, 9(7): 1465-1466.

[8] DONOHO D L. Compressive sensing[J]. IEEE Trans. Inform. Theory, 2006, 52(4): 1289-1306.

[9] CANDÈS E J, TAO T. Near optimal signal recovery from random projections: universal encoding strategies[J]. IEEE Trans. Inform. Theory, 2006(52): 5406-5425.

[10] CANDÈS E J. Compressive sampling[C]// Proceedings of the International Congress of Mathematicians Madrid. Spain, 2006: 1433-1452.

[11] CHAI X, WU H, GAN Z, et al. Nixon. An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding[J]. Optics and Lasers in Engineering, 2020, 124: 105837.

[12] CHAI X, ZHENG X, GAN Z, et al. An image encryption algorithm based on chaotic system and compressive sensing[J]. Signal Processing, 2020, 124: 105837.

[13] XU Q, SUN K, CAO C, et al. A fast image encryption algorithm based on compressive sensing and hyperchaotic map[J]. Optics and Lasers in Engineering, 2019, 121: 203-214.

[14] CHAI X, ZHENG X, GAN Z, et al. An image encryption algorithm based on chaotic system and compressive sensing[J]. Signal Processing, 2018, 148: 124-144.

[15] ZHOU N, ZHANG A, WU J, et al. Novel hybrid image compression-encryption algorithm based on compressive sensing[J]. Optik, 2014, 125(18): 5075-5080.

[16] LIU H, WANG X, KADIR A, et al. Color image encryption using Choquet fuzzy integral and hyper chaotic system[J]. Optik, 2013, 124(18): 3527-3533.

PAN Tao, born in 2000, postgraduate. His main research interests include information security and so on.

TONG Xiaojun, born in 1963, professor, Ph.D supervisor. Her main research interests include information security and so on.