文章编号：2096-1618(2022)05-0558-07

基于混沌压缩感知的多图像隐藏加密算法

杜鑫昌， 高瑜翔
(成都信息工程大学通信工程学院微电子学院，四川 成都 610225)

摘要：针对现有的图像加密算法大多只对单幅图像单次操作，加密后的密文图像在传递过程中占据较大的带宽，且密文图像特有的纹理特征容易被特定识别截取等问题，提出了一种基于混沌压缩感知的多图像压缩隐藏加密算法。该算法通过结合压缩感知技术将多幅图像同时隐藏加密于一幅明文载体图像中，并提出一种新的组合置乱算法。对压缩后的密文图像进行加权、置乱、扩散操作得到最终的密文图像，将密文图像隐藏嵌入明文覆盖图像中进行传递。仿真实验表明，合并压缩加密4幅图像的情况下，可节省超过81.5%的存储空间，且平均每幅复原图像的峰值信噪比达到27.71 dB。并且该算法有较好的抗差分攻击性能，密文图像像素改变率(UACI)与统一平均变化程度(NPCR)接近理论值。故提出的压缩加密隐藏算法具有较好的压缩性、安全性。

关 键 词：压缩感知；混沌；多图像；隐藏加密
中图分类号：TN911.73 **文献标志码**：A
doi：10.16836/j.cnki.jcuit.2022.05.012

0 引言

随着数字化时代的快速发展，人们无时无刻不在进行着信息的交流传递，如何保证网络信息传递的安全性是迫切需要解决的重要问题[1]。图像作为一种重要的信息载体在日常信息交流中扮演重要角色，而图像本身具有冗余度高、数据量大等属性[2]，在传递过程中占据了较大的带宽。因此研究在图像传递过程中如何保证信息传递的安全性，同时又减少带宽的占用率是非常重要的。

压缩感知[3-4]可以同时完成信号的采集和压缩。如果将压缩感知与加密算法相结合，就可以在数据的采样、压缩过程中对数据进行加密[5-7]。近年来利用混沌系统来构造密码算法已成为国内外的研究热点[8]。传统的加密算法大多只对单幅图像进行加密处理且直接将具有纹理特征的密文图像进行传递，传递过程中密文图像不但占据了较大的带宽且具有的纹理特征很容易被特定拦截并进行分析[9]。为此提出一种基于混沌压缩感知的多图像隐藏加密算法，将多幅需要加密的图像信息处理嵌入到一幅载体图像中，实现了一种视觉有意义加密算法[10-11]，在视觉上减少密文信息传递的过程中被发现的概率并提高带宽的利用率。

1 基于混沌压缩感知的多图像隐藏加密算法设计

总体加密方案如图1所示，首先将多幅加密图像经过稀疏基稀疏变换，得到各个密文图像的小波图像。截取每幅加密图像小波图的左上角部分拼接为一整幅小波图。为减少稀疏图像中非零元素点的相关性，使之分布更均匀，采用本文提出的组合置乱算法对稀疏图像进行置乱。利用超混沌Lorenz混沌方程生成的伪随机序列构建受控的测量矩阵进行压缩感知测量，得到加密压缩后的密文图像，然后将压缩后得到的密文图像进行二次置乱与扩散操作来增加密文的安全性。为了增加密文传递过程中视觉上的安全性，通过图像嵌入隐藏算法将密文图像嵌入隐藏在明文载体图像进行传递，从而达到视觉有意义的加密算法的整体设计。

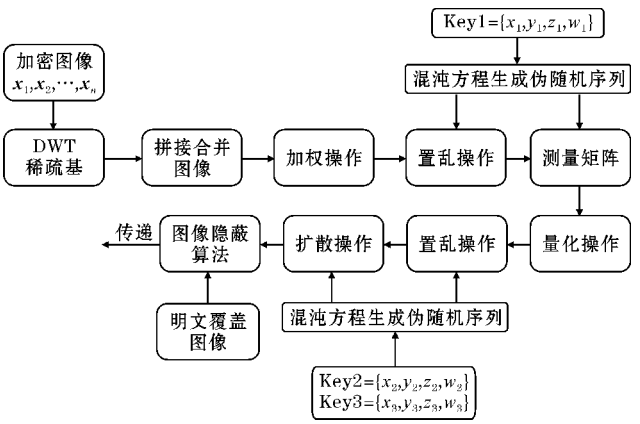


图1 加密总体方案设计

2 加密算法的关键技术

2.1 压缩感知

2.1.1 信号的稀疏表示

一般而言，信号都是在时域或空域中来表示，也可

收稿日期：2021-12-01
基金项目：四川省教育厅资助项目(15TD0022)

以在其他变换域中通过少量元素的线性组合来很好地近似该信号。稀疏信号模型提供了一个可捕获大多数高维信号中包含少量信号的数学框架。信号的稀疏表示是压缩感知的先验条件,即信号必须在某种变换下可以稀疏表示。常见的信号稀疏基包括:正(余)弦基、小波基、chirplet 基以及 curvelet 基等。

本方案采用离散小波基对图像做稀疏处理,加密测试图像 X"Lena"大小为 256×256,离散小波基 $\boldsymbol{W}$ 的大小设置为 256×256($\boldsymbol{WW}^{\mathrm{T}}=\boldsymbol{I}$,$\boldsymbol{W}^{\mathrm{T}}\boldsymbol{W}=\boldsymbol{I}$),稀疏处理可以得到

$$\boldsymbol{R}=\boldsymbol{WXW}^{\mathrm{T}}$$

$\boldsymbol{R}$ 为图像在 DWT 域的表示,原始图像经过小波稀疏变换处理后被分解为高频和低频两部分信息。图 2 显示了"Lena"在不同剪切率下离散小波基 DWT 变换的结果,其中图 2(a)~(c)分别为不同剪切率下裁剪的稀疏图像;图 2(d)与图 2(e)显示了在剪切率为0.5、0.75下合并压缩 2 幅图像与 4 幅图像的图像压缩模型。经过稀疏变换后的矩阵能量主要集中在左上角的低频部分,其余黑色部分的高频信息能量接近于零,因此图像信号在 DWT 域中的表示是稀疏的。因为图像的绝大数信息都分布在稀疏图像的左上角部分,其余部分的像素值灰度值几乎为零。通过不同剪切率下的稀疏图像的重建图像质量实验研究分析可得,选择性地舍去黑色部分的区域对于信号重构的质量影响不大(表 1)。

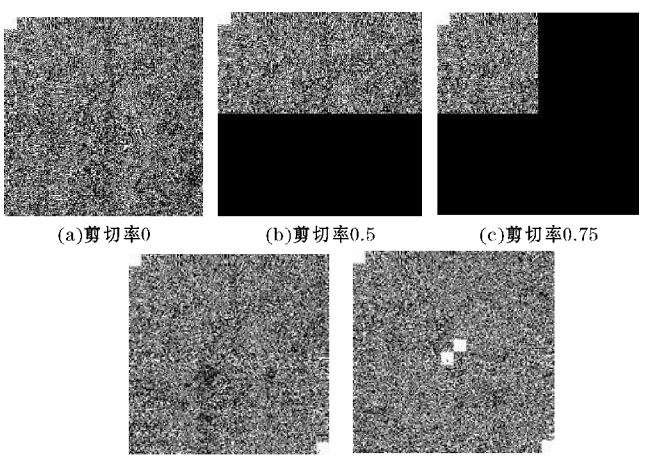


图 2　小波变换图像

表 1　不同剪切率下重构图像质量分析

明文图像	重构算法	压缩率	剪切率	PSNR 值/dB
Lena	CS_CoSaMP	0.75	0	32.0549
			0.5	33.9585
			0.75	29.9636
Camera			0	29.3.53
			0.5	30.3569
			0.75	26.9068

2.1.2　编码测量(采样过程)

与传统采样数据不同,压缩感知采集的不是像素点,而是一组线性组合的测量值。下面公式表示每一个测量值的计算过程,$\boldsymbol{f}$ 表示稀疏信号,$\boldsymbol{\Phi}$ 表示测量矩阵,大小为 $M\times N$ 维,两者的内积之和为 $\boldsymbol{y}_i$。经过 M 次的测量之后,即得到所需要的 M 个测量数据 $\boldsymbol{y}$。

$$\boldsymbol{y}_1=\langle\boldsymbol{f},\boldsymbol{\varphi}_1\rangle,\boldsymbol{y}_2=\langle\boldsymbol{f},\boldsymbol{\varphi}_2\rangle,\cdots,\boldsymbol{y}_M=\langle\boldsymbol{f},\boldsymbol{\varphi}_M\rangle$$

$$\boldsymbol{y}=\boldsymbol{\varphi}\bullet\boldsymbol{f}$$

为了重构信号,测量矩阵 $\boldsymbol{\Phi}$ 的选择尤其重要,矩阵需要满足与信号的稀疏基不相关。测量矩阵分为确定性测量矩阵和随机测量矩阵。由于随机测量矩阵具有随机性、在传输过程中占据较大带宽以及不宜在硬件中实现等缺点,因此采用混沌系统产生的伪随机序列来构造确定性测量矩阵以便在传输过程中节省带宽和保证图像的重建效果。

2.1.3　恢复算法(非线性)

压缩感知的重构问题的求解是一个非凸优化问题,属于 NP 难问题。由低维 M 维的矢量求解高维 N 维的矢量,是一个欠定问题的求解。Candes 等[4]和 Donoho 等[3]提出,可以将其转化维凸优化问题,求解 l_1 最小范数。

$$\min_{f}\|\boldsymbol{f}\|_{l_1}\text{ subjectto }\quad\boldsymbol{\Phi f}=\boldsymbol{y}$$

常见的压缩感知恢复算法包括:匹配追踪算法、正交匹配追踪算法、分段正交匹配追踪算法、压缩采样匹配追踪算法等来重构原始信号[12]。

2.2　图像隐藏算法

图像隐藏算法的的核心思想是通过将加密图像的图像块进行酉相似变换处理得到对角化形式的特征向量嵌入到明文图像中完成图像的隐藏加密,而特征向量作为密钥传递给对方[13-14]。加密图像嵌入操作:

首先将加密图像 $\boldsymbol{X}$,明文图像 $\boldsymbol{Y}$(大小为 $M\times N$)划分为特定大小的块 $\boldsymbol{X}_i$,$\boldsymbol{Y}_i$(大小为 $m\times n$),

$$\boldsymbol{X}=\{\boldsymbol{X}_i;0\leqslant i\leqslant\frac{M\cdot N}{m\cdot n}\}$$

求出加密图像的每个分块的特征值与特征向量。特征向量可作为提取密文的密钥。特征值的求取:

$$|\boldsymbol{X}_i-\lambda\boldsymbol{I}|$$

特征值可以写为 $\lambda_i,\lambda_2,\lambda_3\cdots,\lambda_n$。

特征向量的求取:

$$\boldsymbol{X}_i\boldsymbol{q}_i=\lambda\boldsymbol{q}_i$$

定义矩阵 $\boldsymbol{Q}$

$$\boldsymbol{Q}_i=[q_1,q_2,q_3,\cdots,q_n]$$

酉相似变换:利用酉相似变换将每个分块所表示的矩阵变换为对角矩阵。

$$\boldsymbol{A}_i=\boldsymbol{Q}_i^{-1}\boldsymbol{S}_i\boldsymbol{Q}_i$$

$$\boldsymbol{A}_i=\begin{bmatrix}\lambda_1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & \lambda_n\end{bmatrix}$$

嵌入操作：

$$\boldsymbol{W}_i=\boldsymbol{Y}_i+\boldsymbol{A}_i$$

（$\boldsymbol{W}$ 为嵌入密文图像之后的明文图像）

提取图像：

从接收到的嵌入密文的明文图片减去明文图像，就可以得到对角矩阵，通过求取特征向量的逆矩阵得到加密图像。

$$\boldsymbol{X}=\boldsymbol{Q}_i\boldsymbol{A}_i\boldsymbol{Q}_i^{-1}$$

2.3 混沌理论

超混沌 Lorenz 系统是 Lorenz 混沌系统的一种演变，主要定义如下：

$$\begin{cases}\dfrac{\mathrm{d}x}{\mathrm{d}t}=a(y-x)+w\\ \dfrac{\mathrm{d}y}{\mathrm{d}t}=cx-y-xz\\ \dfrac{\mathrm{d}z}{\mathrm{d}t}=xy-bz\\ \dfrac{\mathrm{d}w}{\mathrm{d}t}=-yz+rw\end{cases}$$

当 $a=-10,b=8/3,c=28$ 且 $-1.52\leqslant r\leqslant -0.06$ 时，系统处于超混沌状态。

2.4 组合置乱算法

为了使稀疏图像中非零像素点的分布更加均匀减少之间的相关性，提高信号的重构质量。本文提出了一种新的组合置乱算法。

（1）借助于混沌系统产生伪随机向量，去除掉向量中重复出现的数值并将范围内没有出现的数值排列在向量的尾部，即产生了无重复的随机数向量。

（2）产生无重复随机数向量 $\boldsymbol{X}_i\in\{1,2,\cdots,M\}$，对图像进行行置乱。将图像的第 $\boldsymbol{X}_i$ 行与第 $\boldsymbol{X}_{M+1-i}$ 行进行交换。$i=1,2,\cdots,M/2$。

（3）产生无重复随机数向量 $\boldsymbol{X}_j\in\{1,2,\cdots,N\}$，对图像进行列置乱。将图像的第 $\boldsymbol{X}_j$ 行与第 $\boldsymbol{X}_{N+1-j}$ 行进行交换。$j=1,2,\cdots,N/2$。

（4）将进行完行置乱与列置乱的二维图像展开为一维向量 $\boldsymbol{Z}$，借助产生无重复随机数向量 $\boldsymbol{X}_l\in\{1,2,\cdots,M\times N\}$。$l=1,2,\cdots,M\times N$。将 $\boldsymbol{Z}(\boldsymbol{X}_l)$ 与 $\boldsymbol{Z}(\boldsymbol{X}_{M\times N-l+1})$ 进行交换。

3 加密与解密步骤

3.1 加密过程

（1）将需要加密的多幅图像稀疏变换之后，截取各自小波图像的左上角非零信息部分将其拼接为一幅稀疏图像。

（2）对稀疏图像进行置乱操作，通过降低相邻非零元素之间的相关性，使之分布更加均匀。

（3）对置乱后的稀疏图像进行加权处理，通过提高稀疏信号系数的差异性，从而提升后续信号的重构性能。

（4）利用超混沌 Lorenz 混沌方程产生的无重复伪随机混沌序列构建受控的测量矩阵，确保重构信号的质量稳定性。

（5）利用测量矩阵对稀疏信号进行压缩感知测量得到观测矩阵。

（6）对观测矩阵进行量化操作得到元素值在[0.255]的整数矩阵。

（7）利用超混沌 Lorenz 混沌方程生成无重复的伪随机序列，用于对整数密文矩阵的二次置乱和扩散操作。

（8）将密文图像通过嵌入算法处理生成密文特征值矩阵与密钥特征向量矩阵，并将密文特征值矩阵嵌入明文载体图像中，特征向量矩阵作为密钥单独传递给对方。

3.2 解密过程

解密过程是加密过程的逆过程

（1）通过特征值矩阵与特征向量生成密文矩阵 $\boldsymbol{W}1$。

（2）将生成的密文图像 $\boldsymbol{W}1$ 分别进行扩散、置乱和量化操作的逆过程，得到观测矩阵 $\boldsymbol{W}2$。

（3）通过重建算法对观测矩阵 $\boldsymbol{W}2$ 进行信号重构获得明文图像 $\boldsymbol{W}3$。

（4）对明文图像 $\boldsymbol{W}3$ 执行反加权的操作得到小波图像 $\boldsymbol{W}4$。

（5）对小波图像 $\boldsymbol{W}4$ 进行分割，获得各个加密图像的小波图像，并进行小波逆变换得到加密图像。

4 仿真实验

4.1 压缩性能分析

为验证提出的压缩加密隐藏算法的性能，选取了多幅标准的灰度测试图像作为实验图像。在压缩率设置为0.75的情况下，通过比较 PSNR（峰值信噪比）来衡量重构图像的质量。

4.1.1 压缩隐藏加密 2 幅图像

（1）第一组测试（图 3）。选取测试图像“couple”与“camera”作为实验加密图像经过合并加密后隐藏嵌入到明文覆盖图像“Lena”中。

图 3　第一组测试图像

(2)第二组测试(图 4)。选取测试图像“peppers”与“plane”作为实验加密图像经过合并加密后隐藏嵌入到明文覆盖图像“Lena”中。

图 4　第二组测试图像

4.1.2　压缩隐藏加密 4 幅图像

(1)第三组测试(图 5)。选取测试图像“Lena”“camera”“peppers”以及“plane”作为实验加密图像经过合并加密后隐藏嵌入到明文覆盖图像“couple”中。

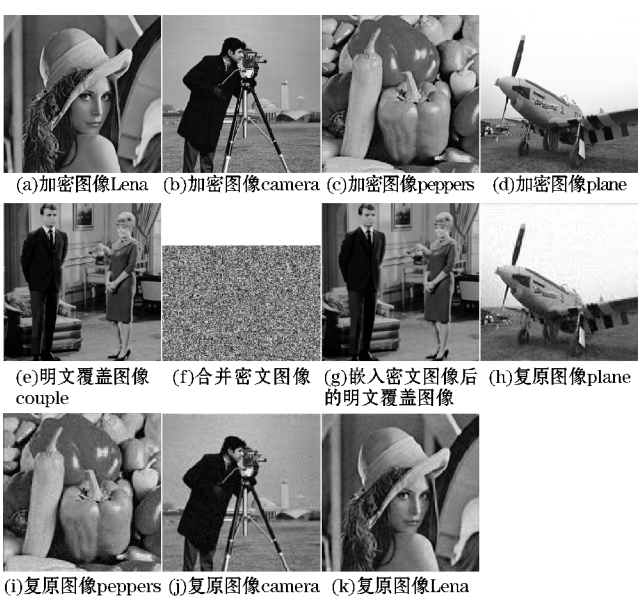


图 5　第三组测试图像

(2)第四组测试(图 6)。选取测试图像“Lena”“couple”“peppers”以及“boat”作为实验加密图像经过合并加密后隐藏嵌入到明文覆盖图像“couple”中。

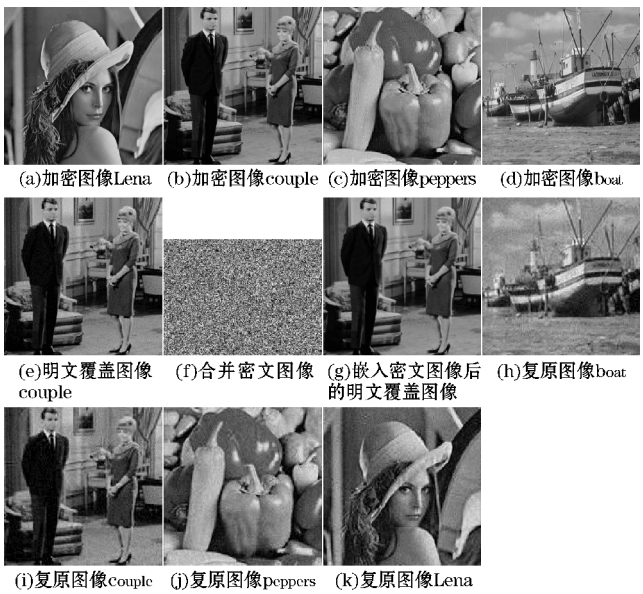


图 6　第四组测试图像

由表 2、表 3、表 4 可知,经过多次多组实验仿真分析,本文提出的压缩加密隐藏算法具有良好的性能,在合并压缩 2 张图像时,复原图像与原图像相比,图像的质量基本不受影响,存储空间节省率达到62.5%。在合并压缩 4 张图像时,复原图像与原图像相比,复原图像虽然在重构质量上有一定影响,但是在视觉上影响不大,还是可以清晰地观察到图像的细节,存储空间节省率达到81.3%。

表 2　合并压缩 2 张图像下重构图像质量分析

加密图像		重构算法	压缩率	PSNR 值
测试组 1	couple	CS_CoSaMP	0.75	30.4327
	camera			29.2778
测试组 2	peppers			31.8224
	plane			30.8464

表 3　合并压缩 4 张图像下重构图像质量分析

加密图像		重构算法	压缩率	PSNR 值
测试组 3	Lena	CS_CoSaMP	0.75	28.5815
	camera			26.2380
	peppers			29.4409
	plane			27.9092
测试组 4	Lena			27.5315
	Peppers			28.4855
	couple			27.2404
	boat			26.2433

表 4 与其他加密压缩算法性能对比

	压缩率	空间节省率	恢复图像平均 PSNR 值
本文方案（压缩加密 2 张图片）	0.75	62.5%	30.59
文献[12]（压缩加密 3 张图片）		42.8%	28.04
本文方案（压缩加密 4 张图片）		81.3%	28.64

与其他加密压缩算法进行性能对比(表 4),可见本文提出的图像隐藏算法在在性能上要优于文献[12],由于本文在算法中引入了图像隐藏算法,在减小了密文在传递过程中被发现的概率,同时增大了密文的嵌入量,节省了带宽的占用率。故本文提出的压缩加密隐藏算法,在隐藏加密的前提下,极大地节省了压缩空间,具有良好的压缩性能。

4.2 密钥安全空间

对于本文提出的压缩加密隐藏系统而言,密钥为超混沌 Lorenz 系统的初始值,即 $K1=\{x_1,y_1,z_1,w_1\}$,$K2=\{x_2,y_2,z_2,w_2\}$ 和 $K3=\{x_3,y_3,z_3,w_3\}$,以及充当密钥的特征向量矩阵。其中混沌方程中,$x\in(-40,40)$,$y\in(-40,40)$,$z\in(1,81)$,$w\in(-250,250)$,x、y 和 z 的步长为 10^{-13},w 的步长为 10^{-12},因此混沌方程的密钥空间大小约为 7.68×10^{59}。图像加密算法的密钥空间大于 2^{100} 就能抵御蛮力攻击,本文提出的压缩加密隐藏算法只是混沌方程的密钥空间就远远大于 2^{100}[15-16]。所以该方案的密钥空间足够抵御蛮力攻击。

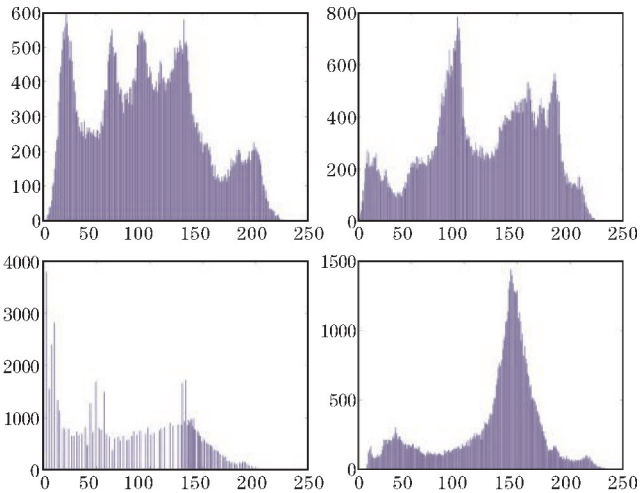
4.3 直方图分析

直方图反映了图像中每一个像素灰度值的统计特性。明文图像的像素灰度值的直方图具有明显的统计特性,为避免针对于统计特性的统计分析攻击,加密图像的像素分布的直方图需要是均匀的。以联合合并隐藏加密 4 幅图像为例。

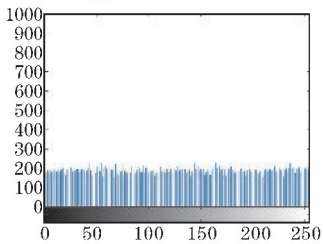
如图 7 所示,直方图的横轴表示图像的像素值,纵轴表示像素值的分布情况。由此可看出,密文图像的直方图较为均匀,从密文中很难提取任一明文图像的像素统计特征,因此可以抵御统计攻击。

4.4 相关性分析

在一般图像中,每个像素点都与相邻像素点呈很高的相关性。一个理想的图像加密系统加密后图像的相邻像素点越趋近于零说明性能越好,因此相邻像素点的相关系数作为评价一个图像加密系统优劣的重要指标[17]。



(a)明文图像直方图



(b)合并密文图像直方图

图 7 实验图像直方图

相关性的计算表达式如下:

$$r_{xy}=\frac{\mathrm{cov}(u,v)}{\sqrt{D(u)}\sqrt{D(v)}}$$

$$\mathrm{cov}(u,v)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(u))(y_i-E(v))$$

$$D(u)=\frac{1}{N}\sum_{i=1}^{N}(u_i-E(u))^2$$

$$E(u)=\frac{1}{N}\sum_{i=1}^{N}u_i$$

从水平、垂直、对角线方向进行相关性分析,结果如表 5 所示。

表 5 相关性分析

图像	垂直方向	对角线方向	水平方向
Lena	0.9786	0.9328	0.9519
camera	0.9744	0.9404	0.9630
peppers	0.9728	0.9458	0.9612
plane	0.9504	0.8911	0.9235
密文图像	0.0025	0.0018	0.0060
文献[12]	0.0055	0.0010	0.0028

由表 5 可以看出,经过压缩加密处理得到的密文图像,像素间的相关性显著下降,密文图像各个方向的相关性接近于零,因此可以抵抗基于相关性的统计攻击能力。密文图像的加密效果较好。

4.5 信息熵分析

信息熵反映了图像信息的不确定性,信息熵的值越大说明信息的不可预测性越好。就以 256 级灰度图像而

言,信息熵理论最大值为8[18-19]。因此对加密前后的密文与各个明文图像的信息熵进行计算,具体结果见表6。

信息熵的计算公式如下:

$$H=-\sum_{i=0}^{L}p(i)\log_2 p(i)$$

表6　信息熵分析

图像	信息熵
Lena	7.5683
camera	7.5797
peppers	6.1689
plane	7.1612
密文图像	7.9967

由表6知,原图像的信息熵值均要小于加密图像的信息熵值。而加密后的图像信息熵的值接近于理论最大值8,由此可见该加密算法对图像处理的有效性。

4.6　敏感性分析

NPCR(像素变化率)指2幅图像中不同的像素点的个数占全部像素点的比例,UACI(像素的统一变化强度)指计算全部相应位置的像素点的差值与最大差值的比值的平均值[20]。如果2幅图像的所有相应位置的像素值均不相同,则NPCR为100%,两个随机图像的UACI理论期望值约为33.4635%。

计算公式如下:

$$\mathrm{NPCR}=\frac{1}{N\cdot M}\sum_{i=1}^{M}\sum_{j=1}^{N}E(i,j)\times 100\%$$

$$\mathrm{UACI}=\frac{1}{N\cdot M}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{I(i,j)-R(i,j)\mid}{255}\times 100\%$$

表7　敏感性分析　　单位:%

图像	NPCR	UACI
Lena	99.1086	31.6339
camera	99.7162	34.1311
peppers	99.6979	32.5016
plane	99.6887	39.8378

由表7可知,本文方法在NPCR与UACI上表现较好,接近于理论值,可有效抵抗差分攻击。

4.7　鲁棒性分析

鲁棒性分析是检验算法在非理想状态下抗干扰能力的重要分析方法,为检验所提出算法的抗干扰能力,以隐藏加密4幅图像为例,密文图像压缩率设置为0.75,对嵌入密文图像的明文覆盖图像进行不同强度高斯随机噪声的干扰,通过检验噪声环境下图像的重构质量来验证算法的抗噪声干扰能力。图8、表8分别给出了在3种不同噪声强度干扰下4幅隐藏加密图像的复原情况以及复原图像的峰值信噪比。由实验数据可得,当噪声强度 $\sigma=0.00001$ 时,图像的重构质量接近于无噪声干扰下图像的重构质量,图像信息基本不受噪声干扰影响。在噪声强度 $\sigma=0.001$ 时,虽然复原图像受噪声干扰影响较大,但仍能提取主要信息。

(a)噪声强度为0.001情况下的压缩复原图像　(b)噪声强度为0.0001情况下的压缩复原图像　(c)噪声强度为0.00001情况下的压缩复原图像

图8　不同噪声强度下的鲁棒性分析

表8　不同噪声强度干扰下的重构图像PSNR　　单位:dB

测试图像	PSNR			
	$\sigma=0.001$	$\sigma=0.0001$	$\sigma=0.00001$	$\sigma=0$
Lena	16.2214	24.6265	27.7264	28.5815
camera	16.1403	23.6938	25.6612	26.2380
peppers	16.2910	25.1624	28.4571	29.4409
plane	16.2520	24.5561	27.1463	27.9092

5　结束语

提出的基于混沌压缩感知的多图像加密方法,利用压缩感知技术与加密算法相结合,在保证密文图像传递安全性的同时实现了多图像的压缩,极大地减少了传递过程中的带宽占用率以及节省了存储空间。为降低传递过程中密文图像被特定识别拦截,在算法模型内引入了图像隐藏算法,将密文图像隐藏嵌入到明

文载体图像中,实现了视觉有意义的多图像压缩加密算法。由于为提高图像的重构质量在压缩感知框架内加入了加权操作,在提高信号重构质量的同时也影响了噪声情况下的信号重构质量,因此下一步将对这方面进行优化。

参考文献:

[1] 杨岿.基于压缩感知与实时动态置乱的图像加密算法[J].计算机工程与设计,2018,39(9):2879-2886.

[2] 刘为超.数字图像加密技术及其安全性分析[J].科学技术创新,2020(17):86-87.

[3] Donoho, D L. Compressed sensing [J]. IEEE Transaction on Information Theory, 2006, 52(4): 1289-1306.

[4] CANDES E J, TAO T. Ner-optimal signal recovery from random projections; universal encoding strategies[J]. IEEE Transactions on Information Theory, 2006, 52(12): 5406-5425.

[5] Brahim A. Image encryption based on compressive sensing and chaos systems[J]. Optics and laser technology technology, 2020, 132.

[6] 石航,王丽丹.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[J].物理学报,2019,68(20):39-52.

[7] 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.

[8] 黄林荃,刘会,王志颖,等.结合混沌映射与 DNA 计算的自适应图像加密算法[J].小型微型计算机系统,2020,41(9):1959-1965.

[9] 曹圣楠,杨宇光.基于压缩感知的视觉有意义图像加密算法[J].信息安全研究,2018,4(6):539-547.

[10] Zhou Yuanyuan. Method of multiple-image hiding in QR code based on compressed sensing and orthogonal modulation[J]. Optik, 2018, 159: 265-274.

[11] Muhammad, Nazeer. Reversible integer wavelet transform for blind image hiding method [J]. PLoS ONE, 2017, 12(5).

[12] 王紫琪.基于混沌压缩感知的多图像信息隐藏与加密算法[D].北京:北京邮电大学,2020.

[13] Hamzeh hajizaadeh. A new high capacity and EMD- based image steganography scheme in spatial domain[C]. IEEE transactions on information forensics and security, 2013: 634-673.

[14] Sure, Srikanth. compression efficiency for combining different embedded image compression techniques with Huffman encoding[C]. international conference on communication and signal processing, 2013.

[15] CHU Chunyang, GAO Yuxiang, XIE Jianfeng, et al. Improved chaotic equation and its new multichaotic image encryption method[J]. Telecommunication Engineering, 2020, 60(8): 955-960.

[16] 谢国波,丁煜明.基于 Logistic 映射的可变置乱参数的图像加密算法[J].微电子学与计算机,2015,32(4):111-115.

[17] 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[J].杭州师范大学学报(自然科学版),2020,19(2):208-214.

[18] Pak C, Huang L. A new color image encryption using combination of the 1d chaotic map[J]. Signal Process, 2017, 138: 129-137.

[19] Hoang TM, Thanh HX. Ceyptanalysis and security improvenment for a symmetric color image encryption algorithm[J]. Optik, 2018, 155: 366-383.

[20] 郭媛,周艳艳,敬世伟.基于图像重组和比特置乱的多图像加密[J].光子学报,2020,49(4):174-186.

Multi-image Hiding Encryption Algorithm based on Chaotic Compressed Sensing

DU Xinchang, GAO Yuxiang

(College of Communication Engineering(College of Microelectronics), Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: Most of the existing image encryption algorithms only operate on a single image once, the encrypted ciphertext image still occupies a large bandwidth in the process of transmission, and the unique texture features of the ciphertext image are easy to be intercepted by specific recognition, etc. This paper proposes a multi-image compression and concealment encryption algorithm based on chaotic compressed sensing. In this algorithm, multiple images are simultaneously hidden and encrypted in a plaintext carrier image by combining compressed sensing technology. A new combinatorial scrambling algorithm is proposed. The compressed ciphertext image is weighted, scrambled and diffused to get the final ciphertext image, and the ciphertext image is hidden and embedded in the plaintext overlay image for transmission. Simulation results show that the combined compression and encryption of four images can save more than 81.5% of the storage space, and the average peak signal-to-noise ratio of each restored image reaches 27.71 dB. Moreover, the algorithm has a good anti-differential attack performance, and the pixel change rate (UACI) and uniform mean change degree (NPCR) of ciphertext images are close to the theoretical values. Therefore, the compression encryption and hiding algorithm proposed in this paper has good compressibility and security.

Keywords: compression perception; chaos; more images; hide the encryption