

基于压缩感知的光学图像加密技术研究

刘效勇^{1,2} 曹益平¹ 卢佩^{3,4}

¹ 四川大学光电系, 四川 成都 610064; ² 石河子大学理学院物理系生态物理实验室, 新疆 石河子 832000
³ 石河子大学信息科学与技术学院, 新疆 石河子 832000
⁴ 中国科学院光电技术研究所, 四川 成都 610209

摘要 提出了一种基于压缩感知的光学数字图像加密方案, 利用压缩感知理论及特点, 借助双随机相位编码技术, 实现了对数字图像的多重加密。通过压缩感知使用随机测量矩阵作为密钥对原始图像加密, 然后对加密图像利用 Arnold 变换置乱二次加密, 并通过 $4f$ 光学系统进行双随机相位编码再次对图像加密, 从而实现了对图像的多次加密。考虑实际应用中传输过程的安全性, 将加密图像融合于载体图像。在接收端, 对加密图像进行解密重构。实验结果表明, 该加密方案能够有效降低采样数据量, 具有高稳健性, 对密钥响应敏感并可以抵御较强的攻击。

关键词 信号处理; 压缩感知; Arnold 变换; 双随机相位编码技术; 密钥

中图分类号 TP309 **文献标识码** A **doi**: 10.3788/AOS201434.0307002

Research on Optical Image Encryption Technique with Compressed Sensing

Liu Xiaoyong^{1,2} Cao Yiping¹ Lu Pei^{3,4}

¹ Opto-Electronics Department, Sichuan University, Chengdu, Sichuan 610064, China

² Key Laboratory of Ecophysics and Department of Physics, Shihezi University, Shihezi, Xinjiang 832000, China

³ College of Information Science and Technology, Shihezi University, Shihezi, Xinjiang 832000, China

⁴ Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu, Sichuan 610209, China

Abstract A new digital image optical encryption method based on compressed sensing is proposed. With the advantage of the characteristics of compressed sensing as well as double random phase encoding technique, multi-encryption of digital image is realized. Compressed sensing is utilized to compress and encrypt a digital image with the random measurement matrix as secret key. Arnold transformation is used to scramble the encryption image with low data volume. The encryption image is encrypted again by double random phase encoding technique to realize the multiple encryption of image. Security overall process is taken into account in the scheme. The multi-encrypted information is embedded into the host image and transmitted. At the receiver, original image information is reconstructed. The experimental results show that the encryption scheme has such features as low data volume, strong robustness, high key sensitivity, and can resistance brute force attack.

Key words signal processing; compressed sensing; Arnold transformation; double random phase encoding technique; key

OCIS codes 060.4785; 070.4560; 070.7345; 070.2025

1 引言

信息安全已经成为一个非常重要的研究课题,

而大部分的安全验证系统是基于图像的。现在已提出了多种数字图像加密方法, 按加密与压缩过程关

收稿日期: 2013-07-30; **收到修改稿日期**: 2013-11-07

基金项目: 国家 863 计划(2007AA01Z333)、国家科技重大专项(2009ZX02204-008)

作者简介: 刘效勇(1976—), 男, 博士研究生, 讲师, 主要从事激光、信息安全和光信息处理等方面的研究。

E-mail: llxxyy1017@shzu.edu.cn

导师简介: 曹益平(1962—), 男, 教授, 博士生导师, 主要从事光学三维传感、光信息处理及光机电一体化等方面的研究。

E-mail: ypcao@scu.edu.cn(通信联系人, 中国光学学会会员号: 6100106)

系可分为直接加密、选择加密、具有压缩功能的加密。按加密手段主要分为基于秘密分割和秘密共享的图像加密技术、基于矩阵变换/像素置换的图像加密技术、基于现代密码体制的图像加密技术、基于混沌动力学系统的图像加密技术、基于频域的图像加密技术、基于脱氧核糖核酸(DNA)计算的图像加密技术和基于 SCAN 语言的图像加密技术 7 大类^[1-8]。按加密对象可分为对空间域像素的加密和对变换域(频域)系数的加密^[9]。另外还有对多图像加密及彩色图像的单通道加密等^[10-11]。但是,随着计算机技术和密码分析学的进步,总会有新的破解方法出现,使任何加密机制或算法变得不再安全,传统的图像加密方法正面临着严重的挑战。

光的波长短、信息容量大,具有相位、振幅、偏振等多种属性,是多维的信息载体,同时能够快速实现卷积和相关运算,光学信息处理技术在完成数据加密等任务方面与使用电子手段相比具有天然的优势。自双随机相位编码方法被提出后,研究人员先后提出了基于分数傅里叶变换(即梅林变换)的光学图像加密方法、基于菲涅耳变换的加密方法,基于联合变换相关器的加密系统,利用数字全息加密和利用相移干涉技术加密等大量新的或改进的加密技术^[12-15]。这些技术具有高速度、高并行数据处理、高设计自由度、光路精密不易被仿造、高稳健性等优点,光学加密手段越来越受到研究者的青睐。

近来,压缩感知(CS)理论在图像和信号处理领域吸引了众多研究者的注意^[16-18],这一理论最初由 Donoho 等^[19-21]提出。压缩感知使用低采样率进行信号采集,在恢复过程中信息不可避免地出现丢失,但是这种程度的破坏并不会引起感官察觉。一些研究者也提出了基于压缩感知的图像加密方案^[22-23],尽管这种加密方案安全性不能达到十分完美,但由于它在抵御攻击方面具有很高的计算复杂性而具有重要应用意义。

本文将压缩感知和光学加密技术相结合,提出一种新的基于压缩感知的光学图像信息加密方案,应用压缩感知进行采样能够有效节省存储空间,减小传输负荷。加密过程使用了 Arnold 变换对图像进行置乱和基于 $4f$ 光学系统的双随机相位编码技术(DRPE)^[24-26]。通过使用上述技术,实现了对图像信息的多重加密。实验结果显示该加密方案具有能够减少采样数据、稳健性好、对密钥响应敏感和可以抵御很强的攻击等特性。

2 理论基础

2.1 压缩感知

随着信息时代的到来,人们对信息需求量越来越大,使得信号采样率、传输和存储实现的压力越来越大。Nyquist 采样定理指出,采样率达到信号带宽的两倍以上时,才能够由采样信号精确重建原始信号,但是采样率太高使很多采样结果必须在存储和传输之前进行压缩^[27-28]。

为了更加有效存储和传输信息,压缩感知作为一个新的信号采样技术以低于 Nyquist 采样率取代了传统的采样和恢复方法。简单地说,压缩感知理论指只要信号是可压缩的或在某个变换域是稀疏的,那么就可以用一个与变换基不相关的观测矩阵将变换所得高维信号投影到一个低维空间上,然后通过求解一个优化问题就能从这些少量的投影中以高概率重构出原信号。可以证明,这样的投影包含了重构信号的足够信息^[29-30]。

考虑一个长度为 N 的一维实值离散时间信号 x ,可以看作一个 \mathbb{R}^N 空间 $N \times 1$ 维的列向量,元素为 $x[n], n = 1, 2, \dots$,如果是图像或高维数据矢量,则转化成一个长的一维向量。 \mathbb{R}^N 空间的任何信号都能用 $N \times 1$ 维的正交基 $\{\psi_i\}_{i=1}^N$ 的线性组合表示。把向量 $\{\psi_i\}$ 作为列向量形成 $N \times N$ 的基矩阵 $\Psi = [\psi_1, \psi_2, \dots, \psi_N]$,任意信号 x 都可以表示为

$$x = \sum_{i=1}^N \alpha_i \psi_i, \text{ or } x = \Psi \alpha, \quad (1)$$

式中 α 为 $N \times 1$ 列向量的加权系数, $\alpha_i = \langle x, \psi_i \rangle = \psi_i^T x$, x 和 α 是同一个信号的等价表示, x 是信号在时域的表示, α 则是信号在 Ψ 域的表示。如果(1)式中 α 只有 K ($K \ll N$) 个非零(或绝对值较大)的系数, x 称为 K 稀疏信号。信号的可稀疏性表示是压缩感知的先验条件,在已知信号是可压缩的前提下,压缩感知过程可分为两步:

1) 设计一个与变换基不相关的 $M \times N$ ($M \ll N$) 维测量矩阵对信号进行观测,得到 M 维的测量向量;

2) 由 M 维的测量向量重构信号。

用一个与变换矩阵不相关的测量矩阵 Φ 对信号进行线性投影,得到线性测量值 y 为

$$y = \Phi x = \Phi \Psi \alpha = \Theta \alpha, \quad (2)$$

式中 Φ 是个 $M \times N$ 的随机测量矩阵, $\Theta = \Phi \Psi$ 。构造合理有效的测量矩阵是压缩感知研究的核心问题。Candès 指出,高斯随机变量形成测量矩阵可以作为普适的 CS 观测矩阵。

因为 y 的维数小于 x 的维数，所以(2)式有无穷解，重构原始信号比较困难。既然 x 为 K 稀疏，可以利用优化问题求解 x ，

$$\hat{a} = \arg\{\min \|\alpha\|_0\}, \quad y = \Phi x. \quad (3)$$

当 $M \geq cK \lg N$ 时， Φ 具有有限等距性(RIP)， $x[n]$ 能被重构，其中 c 是个小常数。

上面的问题可以通过贪婪迭代算法解决，其中最常用的是正交匹配追踪算法(OMP)。

2.2 基于 $4f$ 光学系统的双随机相位编码技术

双随机相位编码技术是 1995 年由美国康涅狄格大学的 Refregier 和 Javidi 教授提出的，自其诞生

以来就受到研究重视，该技术采用 $4f$ 光学信息处理系统实现^[31-32]，如图 1 所示。各种基于双随机相位编码技术的加密方式相继被发明出来^[33-34]，在图像的加密过程中，起到加密密钥作用的是两个随机相位板 RPM1 和 RPM2，分别表示为

$$\theta(x, y) = \exp[i2\pi\theta_0(x, y)], \quad (4)$$

$$\varphi(u, v) = \exp[i2\pi\varphi_0(u, v)], \quad (5)$$

式中 (x, y) 和 (u, v) 分别表示空间域和频域的坐标， $\theta_0(x, y)$ 和 $\varphi_0(u, v)$ 分别表示空间域和频域的随机相位函数，它们以均匀概率分布在 $[0, 1]$ 区间上，可以对输入的光产生 $0 \sim 2\pi$ 的随机相位延迟。

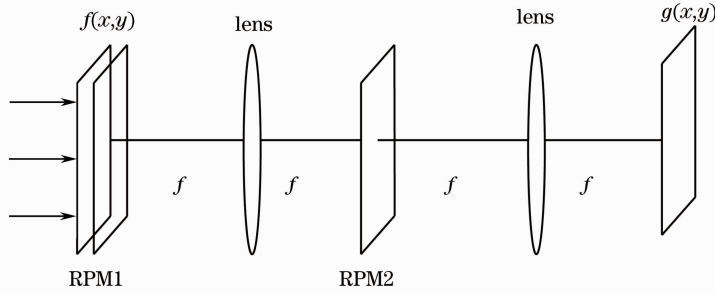


图 1 $4f$ 双随机相位编码光学系统

Fig. 1 $4f$ architecture of the optical system for double random phase encoding

双随机相位编码的加密和解密过程用数学表达式可以分别表示为

$$g(x, y) = \mathcal{F}\{\mathcal{F}[f(x, y) \cdot \theta(x, y)] \cdot \varphi(u, v)\}, \quad (6)$$

$$f(x, y) = \mathcal{F}^{-1}\{\mathcal{F}^{-1}[g(x, y)] \cdot \varphi^*(u, v)\} \cdot \theta^*(x, y), \quad (7)$$

式中 $f(x, y)$ 为输入图像， $g(x, y)$ 为加密图像， \mathcal{F} 、 \mathcal{F}^{-1} 分别表示傅里叶变换和逆傅里叶变换。“*”表示共轭。

2.3 加密和解密方案

现在的图像加密技术由于采用线性变换而存在安全隐患，直接采用非线性变换虽然可以取得很好的结果，但会使图像增大，不利于图像传输和存储，将压缩感知和图像加密结合，可以有效克服这方面的缺陷。

加密和解密过程如图 2 所示。研究中，原始图像通过压缩感知进行加密，在压缩感知模块中，选择合适的随机测量矩阵，随机测量矩阵被用来作为密钥 1；将加密图像分为多个小块，每一小块图像都进行 Arnold 变换得到置乱图像，此处，将 Arnold 变换次数作为密钥 2，对图像再次加密；将置乱图像通过 $4f$ 双随机相位编码光学系统，得到多重加密图像，在编码过程中两个随机相位板使用无理数序列生

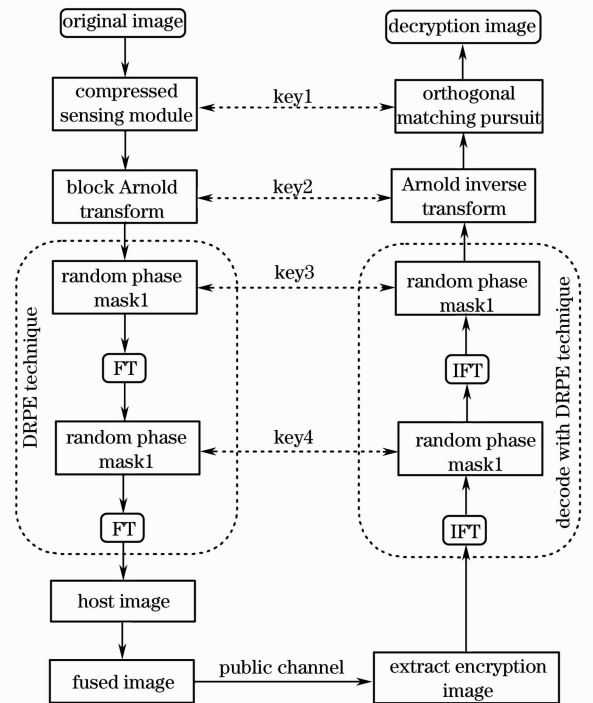


图 2 所提方案流程图

成^[35]，作为密钥 3 和密钥 4；将多重加密图像嵌入宿主图像中，最后得到融合图像图。这样，实现了原始

图像的多重加密,所得到的融合图像通过公共通道可以安全传输。

解密编码过程和加密编码过程相反。在接收端,从融合图像中提取出表现为白噪声的多重加密图像;使其通过 $4f$ 双随机相位编码光学系统,使用密钥 4 和密钥 3 进行初次解密,其间进行了两次逆傅里叶变换;应用密钥 2 通过 Arnold 逆变换解密,最后通过正交匹配编码技术使原始图像信息近似重构,得到解密图像。加密首要目的是使攻击者无法

将密文结果还原成明文,而保证密文安全性最重要的特征是密钥序列的随机性。密钥序列的随机性越强,攻击者攻击密文序列的难度就越大。此处使用的随机测量矩阵具有很强的随机性,因而以其作为密钥使攻击者更不易破译,这保证系统具有足够的抵御攻击能力。

使用原始图像和解密图像间的峰值信噪比 (PSNR, R_{PSN}) 和归一化互相关系数 (NC, C_N) 验证研究效果。分别定义为

$$R_{\text{PSN}}(f, f') = 10 \lg \frac{255^2}{\frac{1}{MN} \sum_{n=1}^N \sum_{m=1}^M [f(m, n) - f'(m, n)]^2}, \quad (8)$$

$$C_N(f, f') = \frac{\sum_{n=1}^N \sum_{m=1}^M [f(m, n) - \overline{f(m, n)}][f'(m, n) - \overline{f'(m, n)}]}{\sqrt{\sum_{n=1}^N \sum_{m=1}^M [f(m, n) - \overline{f(m, n)}]^2} \sqrt{\sum_{n=1}^N \sum_{m=1}^M [f'(m, n) - \overline{f'(m, n)}]^2}}, \quad (9)$$

式中 $f(m, n)$ 和 $f'(m, n)$ 分别表示原始图像和加密图像的像素值, M, N 为图像的宽和高, $\overline{f(m, n)} = \frac{1}{MN} \sum_{n=1}^N \sum_{m=1}^M f(m, n)$, $\overline{f'(m, n)} = \frac{1}{MN} \sum_{n=1}^N \sum_{m=1}^M f'(m, n)$ 。

3 实验与分析

3.1 实验验证

研究中,选择 $256 \text{ pixel} \times 256 \text{ pixel}$ 的灰度图像“lena”[图 3(a)]作为原始图像, $256 \text{ pixel} \times 192 \text{ pixel}$ 的灰度图像“Barbara”[图 3(b)]作为宿主图像。根据宿主图像大小选择合适的随机测量矩阵,将原始图像通过压缩感知进行加密,图像压缩感知后

[图 3(c)]由于被压缩抽样而变小,在压缩感知模块中,随机测量矩阵被用来作为密钥 1。然后加密图像被分为 16×12 块 $16 \text{ pixel} \times 16 \text{ pixel}$ 的小图,对每一小图都进行 Arnold 变换,以 Arnold 变换次数作为密钥 2,得到置乱后图像[图 3(d)],这样进行了二次加密。使用 $4f$ 双随机相位编码光学系统得到多重加密图像[图 3(e)],为保证加密信息在传输过程中的安全性,将其嵌入宿主图像“Barbara”中,得到融合图像[图 3(f)]。编码过程中,通过两个随机相位板可同步得到密钥 3 和密钥 4,此处密钥 3 和密钥 4 采用无理数序列生成。这样,实现了对原始图像的多重加密。

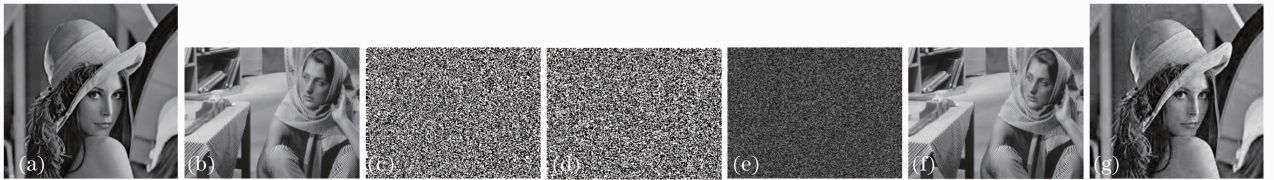


图 3 使用压缩感知的加密解密效果。(a)原始图像;(b)宿主图像;(c)CS 图像;(d)置乱图像;(e)多重加密图像;(f)融合图像;(g)解密图像

Fig. 3 Encryption and decryption results with CS. (a) Original image; (b) host image; (c) CS image; (d) scrambling image; (e) multiple encryption image; (f) fused image; (g) decryption image

在接收端,通过正确密钥对图像进行解密重构,得到解密图像[图 3(g)],原始图像和重构的解密图像间的峰值信噪比为 30.8170 dB ,归一化互相关系

数为 0.9901 。结果表明,该方案是可行和有效的。

如果原始图像不经过压缩感知,只对原始图像分块进行 Arnold 变换,然后通过 $4f$ 双随机相位编

码光学系统进行加密,则得到置乱后的图像,如图 4(b)所示,通过 $4f$ 双随机相位编码光学系统加密后的加密图像如图 4(c)所示,最后解密图像如图 4(d)。此时原始图像和解密图像间的峰值信噪

比为 7.2403 dB,说明尽管能够重构原始图像,但效果不好,归一化互相关系数为-0.0052,解密图像和原始图像负相关。比较图 3 和图 4 可知,没有经压缩感知的图像大小没有发生变化。

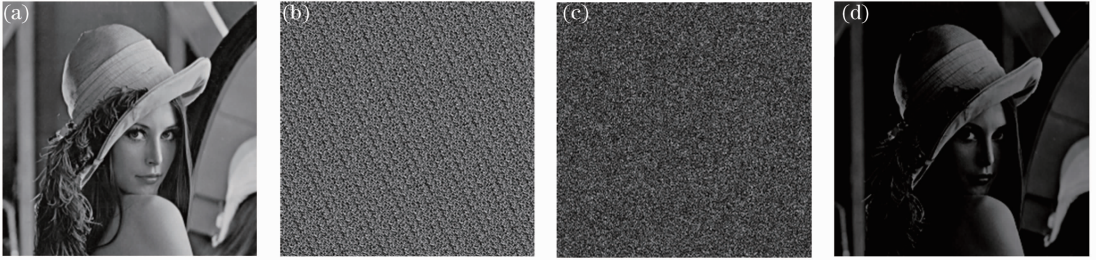


图 4 没有经过压缩感知加密的加密和解密效果。(a)原始图像;(b)置乱图像;(c)加密图像;(d)解密图像

Fig. 4 Encryption and decryption results without CS. (a) Original image; (b) scrambling image; (c) encryption image; (d) decryption image

3.2 安全性和稳健性分析

3.2.1 加密图像对剪切和噪声的稳健性

通过实验对融合图像剪切效果进行了研究,加密图像能够抵御一定强度的剪切攻击。剪切融合图像后的解密图像如图 5 所示,可知,剪切面积越大,原始图像和重构的解密图像间的峰值信噪比及归一化互相关

系数越小,说明重构图像的质量越低。比较图 5(b)和(c)可知,当剪切面积大小相同时,重构图像的质量对剪切位置并不敏感,这是因为原始信号的每个测量值经过测量矩阵时其携带的原始图像的信息部分同等地被认为重要或不重要,所以损失一些仍然可以重建原始信号,重构解密图像质量与裁剪位置无关。

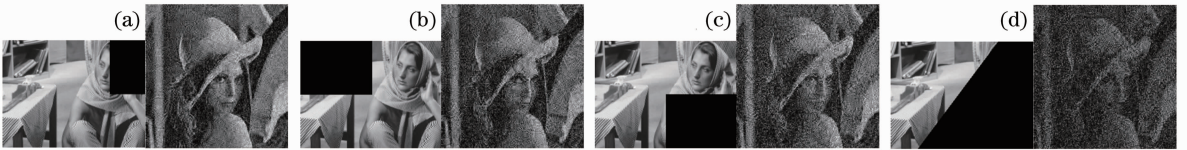


图 5 剪切融合图像后的解密图像。(a) 1/8 像素点被剪切 $R_{PSN} = 17.505$ dB, $C_N = 0.8211$; (b) 1/4 像素点被剪切 $R_{PSN} = 14.5759$ dB, $C_N = 0.7031$; (c) 1/4 像素点被剪切 $R_{PSN} = 14.1586$ dB, $C_N = 0.6752$; (d) 1/2 像素点被剪切 $R_{PSN} = 10.6999$ dB, $C_N = 0.4603$

Fig. 5 Decryption images with pixels occluded of the fused image. (a) 1/8 pixels occluded, $R_{PSN} = 17.505$ dB, $C_N = 0.8211$; (b) 1/4 pixels occluded, $R_{PSN} = 14.5759$ dB, $C_N = 0.7031$; (c) 1/4 pixels occluded, $R_{PSN} = 14.1586$ dB, $C_N = 0.6752$; (d) 1/2 pixels occluded, $R_{PSN} = 10.6999$ dB, $C_N = 0.4603$

图 6 为加密图像在各种噪声情况下重构的解密图像。当保密图像加入了随机噪声和均值为 0,方差为 0.1 的高斯白噪声时,原始图像和重构的解密图像间的峰值信噪比分别为 30.8156 dB 和 30.7432 dB,

归一化互相关系数分别为 0.9901 和 0.9900,如图 6 (a)和(b)所示。图 6(c)和(d)分别为加入噪声密度为 0.05 和 0.10 的椒盐噪声后得到的相应解密图像,原始图像和重构的解密图像间的峰值信噪比分别为



图 6 加密图像加入各种噪声后的解密图像。(a)随机噪声;(b)高斯白噪声;(c)噪声密度为 0.05 的椒盐噪声;(d)噪声密度为 0.10 的椒盐噪声

Fig. 6 Decryption images of encryption images under various noise conditions. (a) Random noise; (b) Gaussian white noise; (c) salt and pepper with 0.05 density; (d) salt and pepper with 0.10 density






30.8063 dB 和 30.7262 dB, 归一化互相关系数分别为 0.9883 和 0.9859, 此时强度对重构的解密图像影响不大, 保密图像能够很容易的被重构, 由此看出该算法具有良好的抗噪能力。

3.2.2 对滤波器的稳健性

加密图像通过高通滤波器后, 实验结果如表 1 所示, 分析可知: 随着滤波器半径增大, 重构图像的质量逐渐降低。这是因为高通滤波器半径越大, 源信号会减弱, 不过仍然可以获得比较好的恢复效果, 由此可证实该加密方案在抵御高通滤波攻击方面是稳健的。

表 1 经高通滤波后重构图像的质量随滤波器半径变换情况

Table 1 Relationship between quality of the reconstruction image after high pass filtering and the filter radius

Filter radius /pixel	High pass filter	Decryption image	R_{PSN}/dB	C_N
4	.		27.3274	0.9745
8	.		26.6364	0.9706
16	•		24.4783	0.9535
32	●		19.4174	0.9201
64	●		13.7100	0.6825

3.2.3 对密钥的安全性检测

这种多重加密的方案具有很高的安全和稳健

性, 密钥错误时的解密图像如图 7 所示, 解密图像对密钥非常敏感。密钥 1 错误时, R_{PSN} 为 3.5109 dB, C_N 为 0.0009.3454; 密钥 2 错误时, R_{PSN} 为 1.6134 dB, C_N 为 0.00064089; 密钥 3 错误时, R_{PSN} 为 3.0882 dB, C_N 为 0.0045。可见只有当所有的密钥正确时, 才能够获得正确的解密图像。保密方案具有很强的抵御攻击的能力, 能够保证信息的安全性和有效性, 攻击者在不知道所有密钥情况下打算破译加密信息几乎不可能。

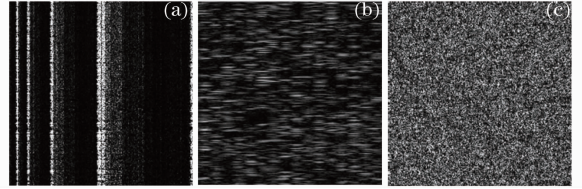


图 7 密钥错误时的解密图像。(a) 密钥 1 错误; (b) 密钥 2 错误; (c) 密钥 3 错误

Fig. 7 Decryption images using wrong keys. (a) Wrong key1; (b) wrong key2; (c) wrong key3

3.3 压缩感知与混沌置乱加密方法对比

为了进一步对本文提出的压缩感知图像加密效果进行综合评价, 选取典型的混沌置乱图像加密^[36-37]进行实验对比。混沌序列使用 Logistic 系统产生, 其动力学方程为

$$x_{n+1} = \mu x_n(1 - x_n). \quad (10)$$

利用(10)式生成混沌置乱序列, 实验中取 $\mu = 4$, $x_1 = 0.3966$ 为密钥信息, 然后对图像像素点进行置乱, 最后回复密文为二维矩阵形式。

3.3.1 直方图对比分析

图 8 为对原始图像“Lena”使用两种加密方法

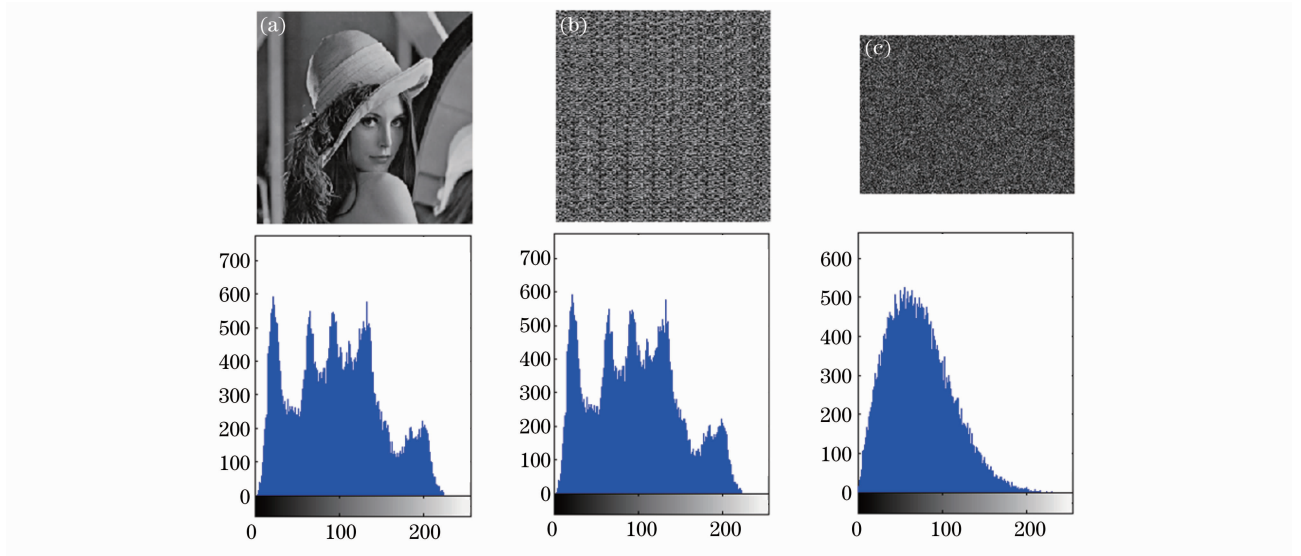


图 8 灰度直方图比较。(a) 原始图像; (b) 混沌置乱加密; (c) 压缩感知加密

Fig. 8 Comparison of gray histograms. (a) Original image; (b) encryption with chaos; (c) encryption with CS

产生的加密图像及其对应的灰度直方图。对比可知,经过混沌置乱图像加密得到的密文图像的灰度直方图在加密前后没有改变,这是因为置乱算法虽改变了像素位置,但并没有改变像素值大小。而基于压缩感知图像加密的灰度直方图分布发生了改变,这是因为加密过程中将图像灰度映射到变换域,灰度值改变为了变换系数,因此这种加密掩盖了明文的统计特性,可以较好的抵抗针对密文统计特性的破解攻击。

3.3.2 剪切与噪声攻击对比实验

对两种加密方法得到的保密图像进行剪切和噪

声攻击实验,分析两种方法的安全性。图9为各剪切密文图像的1/8后得到的解密图像,混沌置乱加密和压缩感知加密的解密图像和原始图像间归一化互相关系数分别为0.6385和0.8236。图10为在密文图像加入均值为0,方差为0.1的高斯白噪声时两种加密方法下的解密图像,其和原始图像间归一化互相关系数分别为0.7836和0.9859,可知,压缩感知加密比混沌置乱加密具有更强的抗剪切和抗噪能力。

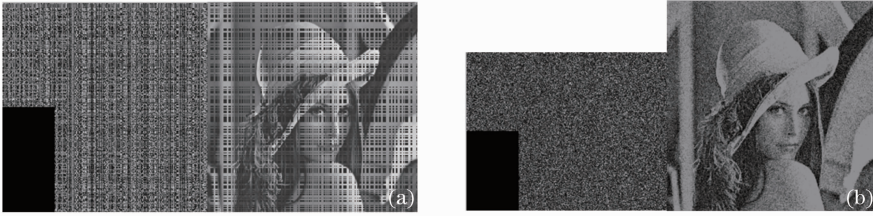


图9 剪切攻击实验。(a)混沌置乱加密;(b)压缩感知加密

Fig. 9 Cropping attack experiments. (a) Encryption with chaos; (b) encryption with CS

3.3.3 优势统计对比

通过用统计特性和稳健性测试,对两种加密算法对比分析如表2所示。可知,压缩感知加密在抗攻击方面具有更高的安全性,然而由于在加密过程时需要数据抽样,难免丢失部分信息,因此加密图像信息熵比原始图像减小。在加解密速度方面,由于本方案使用多重加密,大大增加了计算量,因而使解密速度明显变慢,同时说明这种加密解密时需要很大的计算工作量。



图10 噪声攻击实验。(a)混沌置乱加密;(b)压缩感知加密

Fig. 10 Noise attack experiments. (a) Encryption with chaos; (b) encryption with CS

表2 混沌置乱加密和压缩感知加密方法优势对比

Table 2 Comparison of image encryption with chaos and CS

Encryption property	Encryption with chaos	Encryption with CS
Gray histogram	unchanged	scrambled utterly
Anti noise ability	weak	stronger
Anti cropping attack ability	worse	better
Key space	$\leq 10^{15}$	$\leq 10^{18}$
Information entropy of encryption image	7.5683 (unchanged)	7.2297 (decrease)
Encryption time /s	0.4531	0.6875
Decryption time /s	0.7502	12.6563

4 结 论

提出了一种基于压缩感知和Arnold变换的图像加密方案。在加密过程中加密图像的空间大小被减小,正交匹配矩阵和双随机相位板以及Arnold变换变换次数作为加解密图像的多重密钥。实验分析

结果表明该方案具有较好的保密效果,多重加密方式能有效增强信息的可靠性和机密性,在密文信息受到剪切、加噪声和通过高通滤波器等攻击条件下对解密信息质量分析,证明了使用该方案密文信息具有很高的稳健性。攻击者如果没有正确的密钥即

使使用大量的攻击,也几乎不可能恢复出正确的密文图像信息。对压缩感知加密和混沌置乱加密优势也进行了统计比较和实验分析。

参 考 文 献

- 1 Zhang Xiaoqiang, Wang Mengmeng, Zhu Guiliang. Research on the new development of image encryption algorithms [J]. Computer Engineering & Science, 2012, 34(5): 1-6.
张晓强,王蒙蒙,朱贵良. 图像加密算法研究新进展[J]. 计算机工程与科学, 2012, 34(5): 1-6.
- 2 Yong-Ri Piao, Dong-Hak Shin, Eun-Soo Kim, *et al.*. Robust image encryption by combined use of integral imaging and pixel scrambling techniques [J]. Opt Laser Eng, 2009, 47(11): 1273-1281.
- 3 J Zhao, H Lu, X Song, *et al.*. Optical image encryption based on multistage fractional Fourier transforms and pixel scrambling technique [J]. Opt Comm, 2005, 249(4-6): 493-499.
- 4 Oleg Izmerly, Tal Mor. Chosen ciphertext attacks on lattice-based public key encryption and modern (non-quantum) cryptography in a quantum environment [J]. Theoretical Computer Science, 2006, 367(3): 308-323.
- 5 J Fridrich. Image encryption based on chaotic maps [C]. IEEE International Conference on Systems, Man, and Cybernetics, 1997, 2: 1105-1110.
- 6 Li Juan, Feng Yong, Yang Xuqiang. 3D chaotic encryption scheme for compressed image [J]. Acta Optica Sinica, 2010, 30(2): 399-404.
李娟,冯勇,杨旭强. 压缩图像的三维混沌加密算法[J]. 光学学报, 2010, 30(2): 399-404.
- 7 H T Panduranga, S K Naveen Kumar. Hybrid approach for image encryption using SCAN patterns and carrier images [J]. International Journal on Computer Science and Engineering, 2010, 2(2): 297-300.
- 8 Q Zhang, L Guo, X Wei. Image encryption using DNA addition combining with chaotic maps [J]. Mathematical and Computer Modelling, 2010, 52(11-12): 2028-2035.
- 9 Shang Yanhong. Research on Digital Image Encryption Technology [D]. Beijing: North China University of Technology, 2005. 6-17.
商艳红. 数字图像加密技术的研究[D]. 北京: 北方工业大学, 2005. 6-17.
- 10 Nanrun Zhou, Yixian Wang, Lihua Gong, *et al.*. Novel single channel color image encryption algorithm based on chaos and fractional Fourier transform [J]. Opt Commun, 2011, 284(12): 2789-2796.
- 11 Shi Yishi, Zhang Jingjuan. Research on the phase retrieval algorithm used for multiple-image encryption with region multiplexing [J]. Acta Optica Sinica, 2009, 29(10): 2705-2708.
史祎诗,张静娟. 相位恢复算法用于分区复用多图像加密的研究[J]. 光学学报, 2009, 29(10): 2705-2708.
- 12 Wu Kenan, Hu Jiasheng, Wu Xu. Optical encryption for information security [J]. Laser & Optoelectronics Progress, 2008, 45(7): 30-38.
吴克难,胡家升,乌旭. 信息安全中的光学加密技术[J]. 激光与光电子学进展, 2008, 45(7): 30-38.
- 13 Di Hong. Multiple-image Compressive Encryption and Hiding Base on Optical Information Processing [D]. Beijing: Beijing University of Post, 2012. 1-19.
狄宏. 基于光学信息处理技术的多图像压缩加密与隐藏算法的研究[D]. 北京: 北京邮电大学, 2012. 1-19.
- 14 Zhou Nanrun, Wang Yixian, Wu Jianhua. Optical Image Encryption Method Based on Fractional Mellin Transform [P]. Chinese Patent, 201010616865.2 [P]. 2011-05-25.
周南润,王轶娴,吴建华. 基于分数梅林变换的光学图像加密方法: 中国, 201010616865.2 [P]. 2011-05-25.
- 15 Qin Yi, Gong Qiong, Li Genquan, *et al.*. A optical encryption method with silhouette removal [J]. Chinese J Lasers, 2012, 39(12): 1209002.
秦怡,巩琼,李根全,等. 一种无轮廓像干扰光学加密系统[J]. 中国激光, 2012, 39(12): 1209002.
- 16 R M Willett, R F Marcia, J M Nichols, *et al.*. Compressed sensing for practical optical imaging systems: a tutorial [J]. Opt Eng, 2011, 50(7): 072601.
- 17 Justin Romberg. Imaging via compressed sampling [J]. IEEE Signal Proce Mag, 2008, 25(2): 14-20.
- 18 Zhang Shuo, Wang Jie, Wang Jincheng, *et al.*. Simple calculation method for three dimensional image base on compressed sensing [J]. Acta Optica Sinica, 2013, 33(1): 0111004.
张硕,王杰,王金成,等. 基于压缩感知的三维物体成像的简单计算方法[J]. 光学学报, 2013, 33(1): 0111004.
- 19 David Donoho, Yaakov Tsaig. Extensions of compressed sensing [J]. Signal Processing, 2006, 86(3): 533-548.
- 20 D L Donoho. Compressed sensing [J]. IEEE Trans Info Theory, 2006, 52(4): 1289-1306.
- 21 E J Candès, J Romberg, T Tao. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information [J]. IEEE Trans Info Theory, 2006, 52(2): 489-509.
- 22 R Huang, K Sakurai. A robust and compression combined digital image encryption method based on compressive sensing [C]. 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2011, 53: 105-108.
- 23 P Lu, Zhiyong Xu, Xi Lu, *et al.*. Digital image information encryption based on compressive sensing and double random-phase encoding technique [J]. Optik-International Journal for Light and Electron Optics, 2013, 124(6): 2514-2518.
- 24 V I Arnold. Ergodic Problems of Classical Mechanics Mathematical Physics Monograph Series [M]. New York: WA Ben jans in Inc, 1968.
- 25 W Jin, C Yan. Optical image encryption based on multichannel fractional Fourier transform and double random phase encoding technique [J]. Optik, 2007, 118(1): 38-41.
- 26 Yao-Yao C, Xin Z, Yong-Liang X, *et al.*. An improved watermarking method based on double random phase encoding technique [J]. Opt Laser Technol, 2010, 42(4): 617-623.
- 27 Richard Baraniuk. Compressive sensing [J]. IEEE Signal Proce Mag, 2007, 24(4): 118-121.
- 28 Chen Jing, Wang Yongtian. Research of the compressive imaging technology [J]. Laser & Optoelectronics Progress, 2012, 49(3): 030002.
陈靖,王涌天. 压缩成像技术研究进展[J]. 激光与光电子学进展, 2012, 49(3): 030002.
- 29 E Candès, T Tao. Near-optimal signal recovery from random projections and universal encoding strategies [J]. IEEE Trans Info Theory, 2006, 52(12): 5406-5245.
- 30 Elad Michael. Optimized projections for compressed sensing [J]. IEEE Trans Sign Proc, 2007, 55(12): 5695-5702.
- 31 B Javidi. Optical and Digital Techniques for Information Security [M]. New York: Springer Business Media, 2005.
- 32 M Singh, A Kumar, K Singh, *et al.*. Optical security system using jigsaw transforms of the second random phase mask and the encrypted image in a double random phase encoding system [J]. Opt Laser Eng, 2008, 46(10): 763-768.
- 33 G Unnikrishnan, J Joseph, K Singh. Optical encryption by double random phase encoding in the fractional Fourier domain [J]. Opt Lett, 2000, 25(12): 887-889.

- 34 X Peng, H Z Wei, P Zhang. Asymmetric cryptography based on wavefront sensing [J]. Opt Lett, 2006, 31(24): 3579–3581.
- 35 X Lu, Y Cao. Digital information encryption using multiple Fourier transforms and decimal expansion of irrational numbers [J]. Optik-International Journal for Light and Electron Optics, 2013, 124(12): 1202–1206.
- 36 Guodong Ye. Image scrambling encryption algorithm of pixel bit based on chaos map [J]. Pattern Recognition Letters, 2010, 31(5): 347–354.
- 37 Manjunath Prasad, K L Sudha. Chaos image encryption using pixel shuffling [J]. Computer Science & Information Technology, 2011, 4(1): 169–179.

栏目编辑：李志兰