doi:10.3788/gzxb20144309.0910002

基于压缩感知及光学理论的图像信息加密

卢佩[1],刘效勇[2],卢熙[3],田敏[1],曹海宾[2]

(1 石河子大学 信息科学与技术学院,新疆 石河子 832000)

(2 石河子大学 理学院 物理系生态物理重点实验室,新疆 石河子 832000)

(3 中国电子科技集团公司第 34 研究所,广西 桂林 541004)

摘 要:针对信息加密系统中信息安全性不理想的问题,提出一种基于压缩感知的光学图像信息加密方法.在发送端,自然图像经稀疏表示、随机投影实现图像信息加密;然后将降维后的观测值通过 4F 双随机相位编码光学系统进行二次加密并将其融入宿主图像,实现信息加密及隐藏.在接收端,图像信息经双随机相位编码技术解码,通过正交匹配追踪算法实现原始图像信息重构.该系统能有效降低数据传输量、减小随机相位板大小.且收发方只需按照规则生成密钥而不需传输密钥,保证了密钥的安全性.仿真结果表明:解密恢复图像质量理想,峰值信噪比为 30.899 1 dB,且系统能较好地抵抗裁剪、噪音污染、高通滤波、旋转等攻击,鲁棒性强,安全性高.

关键词:压缩感知;双随机相位编码;正交匹配追踪;约束等距性

中图分类号:TP309.7; O438.2 **文献标识码**:A **文章编号**:1004-4213(2014)09-0910002-8

Image Information Encryption by Compressed Sensing and Optical Theory

LU Pei[1], LIU Xiao-yong[2], LU Xi[3], TIAN Min[1], CAO Hai-bin[2]

(1 *College of Information Science and Technology, Shihezi University, Shihezi, Xinjiang* 832000, *China*)

(2 *KeyLaboratory of Ecophysics and Department of Physics, College of Science, Shihezi University, Shihezi, Xinjiang* 832000, *China*)

(3 *No.* 34 *Research Institute of China Electronics Technology Group Corporation, Guilin, Guangxi* 541004, *China*)

Abstract: Due to the problem of security for information encryption system, an image information encryption scheme combined compressed sensing with optical theory was proposed. At the transmitted terminal, image information encryption based on compressive sensing was realized by sparse representation and random projection firstly. Then, the measured values with low data volume after dimensional reduction were re-encrypted by double random-phase encoding technique and then dispersed and embedded into the host image. At the received terminal, original image information was reconstructed approximately via Orthogonal Matching Pursuit algorithm after the inverse process of double random-phase encoding technique. Not only the security of information was ensured under the premise of decreasing the amount of data transmission and reducing the size of the random phase masks but also the privacy of keys were assured which were gained by rules rather than transmitted from transmitter to receiver. Numerical experiments showed that the quality of decryption image was ideal with the corresponding peak signal to noise ratio of 30.899 1 dB and this system had the advantages of good performance of anti-cropping, anti-noising, anti-rotating and anti-filtering, strong robustness and high security.

Key words: Compressive Sensing (CS); Double Random-Phase Encoding (DRPE); Orthogonal Matching Pursuit (OMP); Restricted Isometry Property (RIP)

OCIS Codes: 100.0100; 070.2025; 070.4560; 070.7345

基金项目:国家自然科学基金(No. 61065006)、中科院"西部之光"人才培养计划资助项目资助

第一作者:卢佩(1979—),女,讲师,博士,主要研究方向为信号与信息处理,光电图像目标识别与跟踪等. Email:lupei0@163.com

通讯作者:刘效勇(1976—),男,副教授,博士,主要研究方向为信息安全,光学三维测量,激光与光通信等. Email:llxxyy1017@shzu.edu.cn

收稿日期:2013-12-25;**录用日期**:2014-04-25

0 引言

随着计算机网络、通信技术的迅猛发展及信息交互量的与日俱增，信息的完整性、保密性、安全性等问题日显突出.信息安全及信息保护技术研究已不容忽视，并在众多领域[1-3]发挥着重要作用.为确保信息安全须采取一定方式来隐藏信息，而隐藏信息的最有效手段便是加密.

由于数字图像数据量庞大用传统信息加密方法[4,5]无法在处理速度上满足需求，而基于光学理论的信息安全系统以其数据的并行处理、加密方式多样等独特优势引起学者们的广泛关注，其中，基于双随机相位编码技术(Double Random-Phase Encoding, DRPE)的信息加密及隐藏技术[6,7]备受瞩目.然而，信息经上述方式处理后，由于其具有白噪音特性，使得宿主图像较低位平面像素值的随机性发生较大改变，因此对融合图像较低位平面进行统计分析可判断其是否含有加密信息[8]，故可对隐藏信息的安全性带来威胁.

压缩感知理论[9]可以用尽量少的数据去提取尽量多的信息[10-12]，并利用信号稀疏分解重构方法从不完整原始信号.另外，从数学角度分析，每个观测值是传统理论下每个原始样本信号的组合函数，即每个观测值均包含着所有样本的少量信息，丢失某些值仍能够近似精确重构原始信号，在信息加密领域且在减少传输数据量的前提下有效抵抗裁剪攻击.结合压缩感知理论，2009 年 Venkatraman D 等实现了图像有损压缩加密，并给出联合解压缩和解密的方法[13]；刘丹华和石光明等解决了无线传输中不可避免的丢包现象对图像加密系统的影响问题[14]；Orsdemir A 等提出了鲁棒加密概念以及对国土安全的作用[15].2010 年梁敬赛等对压缩感知应用于数字图像加密进行探索，提出了基于压缩感知的秘密图像分存等加密方法[16]；杨震等提出基于压缩感知和信息隐藏的语音保密通信系统设计方法[17].2011 年 Rong Huang 等将压缩感知理论与 Aronold 变换相结合提出了鲁棒的数字图像加密方法[18].2012 年周南润等实现了测量矩阵受控的图像压缩感知与图像加密方法[19].2013 年 Athira V 等提出一种结合压缩感知的数据加密新方法[20]；张艾迪则实现了对彩色图像的加密[21].尽管 Rachlin 等[22]提出基于压缩感知的加密系统并不能保证信息的绝对安全，但在破译过程中由于其计算复杂度极高仍不失为一种高效方案.

本文结合压缩感知及光学理论实现了图像信息的加密及隐藏.该系统在有效降低数据传输量及降低随机相位板大小的条件下，保证了信息的安全性，且只需收、发方按照密钥产生规则生成密钥而无需传输密钥，保证了密钥的安全性.仿真实验表明：该系统能较好地抵抗裁剪、噪音污染、高通滤波、旋转等攻击，鲁棒性强，安全性高.

1 理论分析

1.1 双随机相位编码

设(x,y)、(u,v)分别表示空、频域坐标，$h(x,y)$表示待加密图像信息，$g(x,y)$表示加密后图像，$\theta(x,y)$、$\omega(u,v)$分别表示服从 $u(0-1)$均匀分布的空、频域随机相位函数，且可对输入光产生 $0\sim2\pi$ 的随机相位延迟.以 $4f$(f 为焦距)光学系统为例[23]，双随机相位编码实现信息加密原理如图 1.

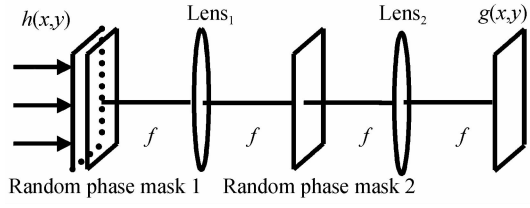

图 1 基于 $4f$ 光学系统的双随机相位编码

Fig. 1 Double random-phase encoding with $4f$ optics system

在该系统中，随机相位板是一种全透明的塑料薄片，分辨率高达数百万像素/mm^2，像素的相位满足白噪音分布，且各像素的折射率不同，能对入射光产生 $0\sim2\pi$的随机相位延迟.将两块统计无关的随机相位板分别置于光学系统的输入平面和傅里叶平面，且待加密图像 $h(x,y)$与随机相位板 1 紧贴，当平行光照射该系统时，$h(x,y)$首先经随机相位板 1 在空域接受随机相位函数 $\exp(\mathrm{j}2\pi\theta(x,y))$的调制并经透镜做一次傅氏变换，然后在频域经随机相位板 2 受随机相位函数 $\exp(\mathrm{j}2\pi\omega(u,v))$调制并经透镜再做一次傅氏变换，即分别对 $h(x,y)$的空间信息和频谱信息进行随机扰乱，在输出平面使之成为具有平稳白噪音特性的加密信息 $g(x,y)$.在此，两随机相位板均为其密钥，且加密过程数学表达式为

$$g(x,y)=F\{F[h(x,y)\exp(\mathrm{j}2\pi\theta(x,y))]\cdot \exp(\mathrm{j}2\pi\omega(u,v))\} \tag{1}$$

由于光路具有可逆性，其解密过程为

$$h(x,y)=\{F^{-1}[F^{-1}(g(x,y))]\cdot \exp(-\mathrm{j}2\pi\omega(u,v))\}\exp(-\mathrm{j}2\pi\theta(x,y)) \tag{2}$$

该 $4f$ 光学系统能把输入平面的像素信息扩散到整个输出平面上，因而对加密信息数据丢失具有较高的容忍度[24].只有当解密密钥及其空间位置均与加密过程准确匹配时才能得到清晰的解密信息，故对元件的空间排列准确度要求高，且需用对光强敏感的器件来接收信息.

1.2 压缩感知

以一维信号为例，设 $\boldsymbol{x}\in\boldsymbol{R}^{N\times1}$ 是长度为 N 的一维

实离散信号，可用 $N\times N$ 维正交基矩阵 $\boldsymbol{\Psi}=[\boldsymbol{\psi}_1,\boldsymbol{\psi}_2,\cdots\boldsymbol{\psi}_N]$ 的线性组合表示为

$$\boldsymbol{x}=\sum_{i=1}^{N}\boldsymbol{\alpha}_i\boldsymbol{\psi}_i=\boldsymbol{\Psi}\boldsymbol{\alpha} \tag{3}$$

式中，$\{\boldsymbol{\psi}_i\}_{i=1}^{N}$ 为 $\boldsymbol{\Psi}$ 的列向量，α_i 为加权系数. 如果 α 有 K 个（$K\ll N$）非零值，则 $\boldsymbol{x}$ 称为 K 稀疏信号. 信号的稀疏性是实现压缩感知的前提条件.

考虑自然信号一般在某变换域具有稀疏性，若用一个与变换基 $\boldsymbol{\Psi}$ 不相关的 $M\times N(M<N)$ 维测量矩阵 $\boldsymbol{\Phi}$ 对信号 $\boldsymbol{x}$ 进行线性投影，可得

$$y=\boldsymbol{\Phi}\boldsymbol{x}=\boldsymbol{\Phi}\boldsymbol{\Psi}\alpha \tag{4}$$

该过程为降维过程，对其求解属不适定数学反问题

$$\min_{\alpha}\|\alpha\|_{l_0}\quad s.t.\quad y=\boldsymbol{\Phi}\boldsymbol{\Psi}\alpha \tag{5}$$

由于 $\boldsymbol{x}$ 是 K 稀疏信号，若式(5)中 $\boldsymbol{\Phi}\boldsymbol{\Psi}$ 的满足有限等距性质[25]（其等价条件为 $\boldsymbol{\Phi}$ 与 $\boldsymbol{\Psi}$ 不相关），则 K 个稀疏系数能够从 M 个测量值中在 l_1[26] 最小范数下通过求解最优化问题进行精确重构，即

$$\hat{\alpha}=\operatorname{argmin}\|\alpha'\|_1\quad s.t.\quad y=\boldsymbol{\Phi}\boldsymbol{\Psi}\alpha' \tag{6}$$

l_1 最小范数下最优化问题可以通过贪婪迭代算法解决，如正交匹配追踪（Orthogonal Matching Pursuit，OMP）[27] 算法.

最后，当稀疏系数被精确重构后，即可通过式(3)最终恢复原始信号 $\boldsymbol{x}$. 压缩感知理论实现框图如图 2.

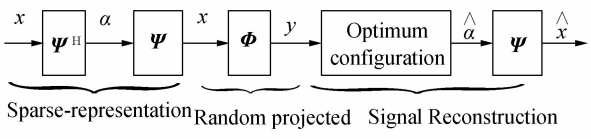

图 2　压缩感知理论框图

Fig. 2　The scheme of compressive sensing theory

2　基于压缩感知及光学理论图像信息加密

2.1　系统设计

系统设计流程如图 3.

首先，待加密信息经压缩感知降维采样后得到加密信息. 然后，利用双随机相位编码技术对其进行二次加密. 该设计方案优点有：1）利用压缩感知随机投影、降维操作实现了用较少数据量表征原始信息，在二次加密过程中降低了随机相位板的大小，节约了系统设计成本. 2）压缩感知随机投影、降维过程中的随机观测矩阵（密钥 1）和二次加密中的随机相位板（密钥 2 和 3）均按密钥生成规则产生而无需传输，从而提高了密钥的保密性及安全性.

另外，加密信息在传输时，为确保其安全，通常将加密信息 $g(x,y)$ 隐藏到宿主图像 $o(x,y)$ 中形成组合图像 $c(x,y)$

$$c(x,y)=o(x,y)+\lambda*h(x,y) \tag{7}$$

同时，为使加密信息尽可能小的影响宿主图像，需在组合前乘以小数常量 λ.

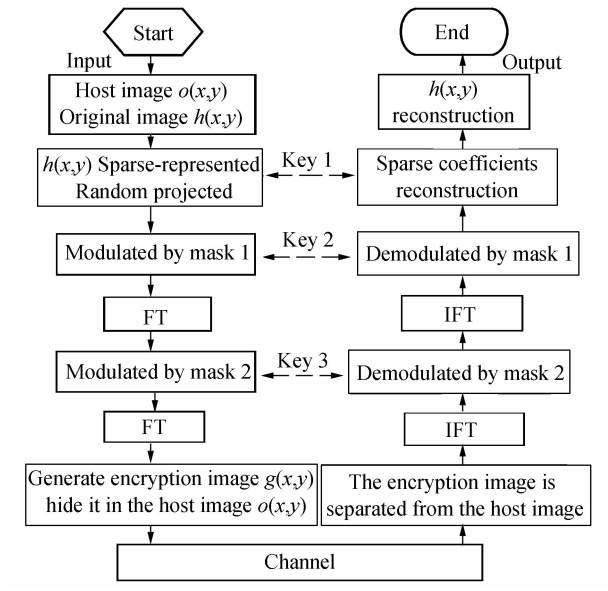

图 3　信息加密系统设计流程

Fig. 3　The flow diagram of the system for information encryption and decryption

2.2　基于无理数的密钥生成规则

在序列密码领域，通常采用序列构建函数生成随机序列作为密钥，但序列构建函数存在周期性，从而对信息的安全造成威胁[28]. 由于无理数是无限不循环小数，具有周期无限长的特点，对无理数序列进行分析可知：若序列足够长，则 0 到 9 十个数字出现概率几近相同，且具有很好的似混沌特点[29]. 故本文用无理数展开式构造随机序列作为加密密钥.

1）随机相位板设计

以无理数 $\pi=3.14159265358979323\cdots$ 为例，设 $P_I^d(L,o)=[p(1),p(2),\cdots p(L)]$ 为无理数序列，其中 I 为无理数，o 为无理数展开式初始位置，d 为小数位数，$L=m\times n$ 为序列长度（$m\times n$ 为随机相位板的大小）. 若 $d=4$，$o=2$，则序列为

$$P_{\pi}^{4}(L,2)=[0.4159,0.1592,0.5926,\cdots] \tag{8}$$

由序列可生成满足 $u(0-1)$ 均匀分布的随机相位板，图 4 为随机相位板生成方式.

p_1	p_2	$\cdots$	p_n
p_{n+1}	p_{n+2}	$\cdots$	$p_{2\times n}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
$p_{(m-1)\times n+1}$	$\cdots$	$\cdots$	$p_{m\times n}$

图 4　随机相位板设计

Fig. 4　The design of random phase mask

2）随机观测矩阵设计

要将高维信号从其低维投影中恢复出来，通常选用具有高斯分布特性的随机矩阵作观测矩阵来解决稀疏重构问题.

随机观测矩阵设计为：先按照上述方式构造基于无理数的服从 $u(0-1)$ 分布的两个随机序列，然后由 Box-muller 法得到服从 $N(0,1)$ 分布的随机序列，最后按照图 4 生成规则得到随机观测矩阵.

3 实验结果及分析

3.1 实验结果

实验中，$h(x,y)$ 选取大小为 $N\times N$(N=256)的 peppers 图像，变换矩阵 $\boldsymbol{\Psi}$ 为与 $h(x,y)$ 大小一致的二维小波变换矩阵，随机观测矩阵 $\boldsymbol{\Phi}$ 的大小为 $M\times N$(M 的取值由图像稀疏度决定. 该待加密图像经变换矩阵后，具有稀疏性，其稀疏度 K 大约为 48，一般地，当满足 $M\approx 4K$ 或 $M\geqslant K\log_2^{(N/K)}$ 条件时，信号才能被近乎完美重构，故在此取 $M=192$)，密钥由 2.2 节中的生成规则产生，稀疏系数重构选择正交匹配追踪算法. 系统实验结果如图 5. 其中，图 5(a)至图 5(f)依次为：待加密图像、宿主图像、基于压缩感知的加密图像、基于双随机相位编码二次加密图像、宿主与加密信息融合图像以及解密恢复图像.

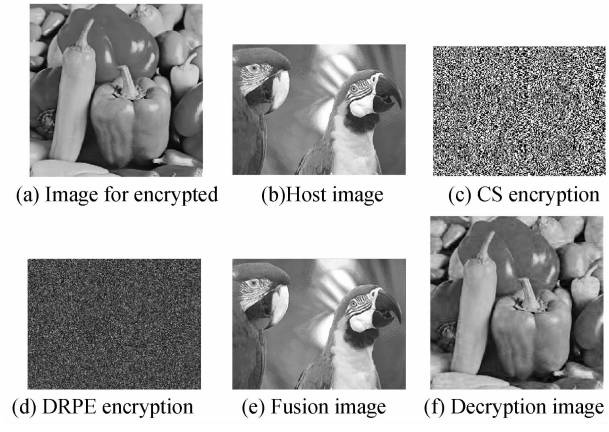

图 5 图像信息加密、解密实验结果

Fig. 5 The experimental results of image information encryption and decryption

为定量分析评判重建图像质量，引入峰值信噪(Peak Signal to Noise Ratio，PSNR)

$$\mathrm{PSNR}=10\log\{255^2/\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[R(i,j)-I(i,j)]^2\} \quad (9)$$

式中，$R(i,j)$、$I(i,j)$ 分别表示重建图像及原始图像像素值. 由图可知，系统重建图像质量理想，对应 PSNR 值为 30.899 1 dB.

图 6 为 M 取不同值时对解密重构结果影响的定量分析. 由实验结果知，当 $M<100$ 时，重构图像质量急剧下降，这是因为 M 不满足与稀疏度 K 的关系条件，故图像不能被高概率重构. 随着 M 值的增加，重构图像质量总体呈上升趋势，当 $M=256$ 时，重构图像 PSNR 为 34.425 3 dB，虽然恢复图像的质量较高，但这与压缩感知对信号的采样转变成对“信息”采样的初衷不符. 故，通过分析信息在信号中的结构与内容，在满足约束关系的条件下，选取 $M=192$，这也使二次加密过程中减小随机相位板大小成为可能，从而节约了系统设计成本.

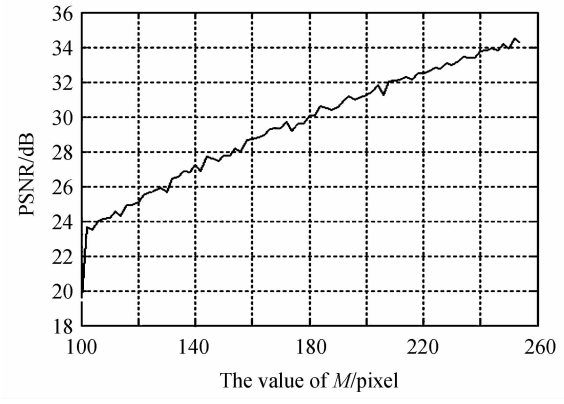

图 6 M 取不同值时对应 PSNR

Fig. 6 The PSNR corresponding with different value of M

3.2 系统性能分析

3.2.1 抗裁剪分析

图 7 为对加密后图像分别进行 12.5%(图 7(a)与图 7(b))、25%(图 7(c)与图 7(d))、50%(图 7(e)与图 7(f))裁剪时对应重构结果. 显然，重构图像质量随着加密图像剪切面积增加而降低，当图像被裁剪至 50% 时，图像基本还能辨识，故该系统能够抵御一定程度的裁剪攻击. 另外，当剪切面积相同而位置不同时，重构图像质量基本无差异，说明重构图像质量与剪切位置无关，从而验证了压缩感知随机观测思想的可行性及在信息加密应用中的有效性.

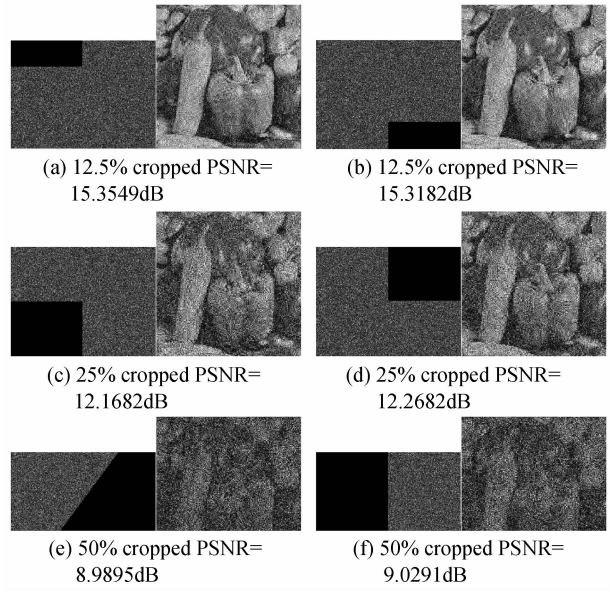

图 7 加密图像抗裁剪鲁棒性

Fig. 7 The analysis of robustness to the pixels cropped for the encrypted image

3.2.2 抗噪音分析

图 8 为加密图像在各种噪音污染下图像重建结

果.其中，左图为融合了加密信息的组合图像 $c(x,y)$ 的含噪图，依次分别含有均值为 0 方差为 0.01、均值为 0 方差为 0.1 的高斯白噪音，密度为 0.01 以及密度为 0.1 的椒盐噪音.右图为与左图对应的解密重构图；其 PSNR 值依次为 29.516 7 dB、24.977 7 dB、27.832 9 dB 及 20.301 8 dB.实验结果表明：基于压缩感知的光学图像信息加密系统抗噪音能力较强.

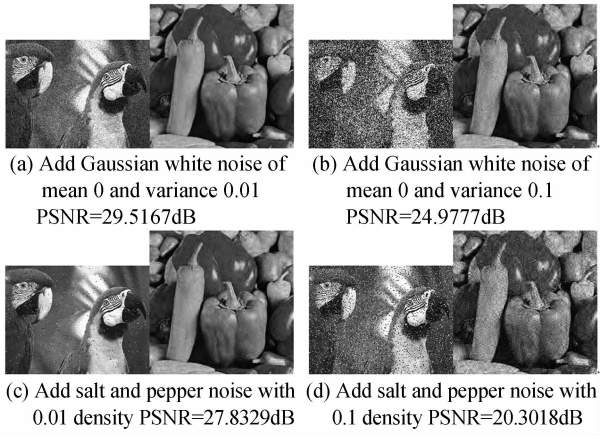

图 8　加密图像抗噪音鲁棒性

Fig. 8　The analysis of robustness to encrypted image with noise

3.2.3　抗滤波分析

图 9 为加密图像经高通滤波和低通滤波后信息重构结果.

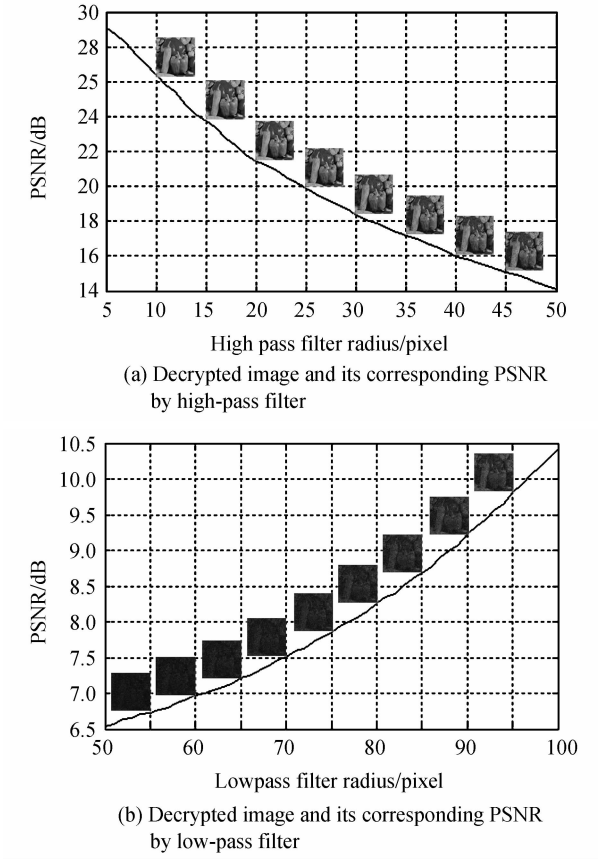

图 9　加密图像抗滤波分析

Fig. 9　The analysis of robustness to encrypted image by filters

由实验知：该方案经高通滤波后信息重建效果理想、系统鲁棒性强，重构图像质量随高通滤波器半径增大而降低，这是因为高通滤波器半径越大，源信号会减弱，当半径分别为 10、45 个像素时对应重构图的 PSNR 分别为 26.393 6 dB 及 15.069 8 dB，仍然可获得比较好的恢复效果.由此可证明该加密方案在抗高通滤波攻击方面是健壮的.而系统经低通滤波后性能较差，重构图像质量随低通滤波半径增大而提高，这与低通滤波器固有特性有关，当半径分别为 55 和 95 时对应重构图的 PSNR 分别为 6.722 8 dB 和 9.810 8 dB.

3.2.4　抗旋转变换分析

图 10 为对加密图像进行旋转操作及对应重构结果.其中，图 10(a)、10(b)和 10(c)分别为逆时针旋转 10°、45°及 60°时对应的加密图像及解密重构图，对应 PSNR 分别为 11.721 3 dB、10.106 2 dB 及 10.120 8 dB.由实验结果知，该加密方法具有一定的抗旋转变换能力.

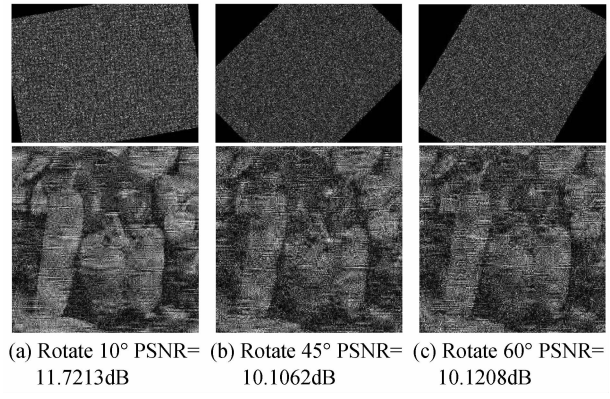

图 10　加密图像抗旋转变换分析

Fig. 10　The analysis of robustness to encrypted image by rotation transformation

3.2.5　信息安全性分析

系统属于双加密系统，共有三个密钥，且密钥无需传输，只需依据规则生成.图 11 为任一密钥错误情况下的信号重构图.key 1 为随机观测过程中密钥、key 2 为双随机相位编码过程中随机相位板 1、key 3 为随机相位板 2 错误时的重构图，对应 PSNR 分别为 3.177 7 dB、3.248 5 dB 和 3.102 5 dB.由结果知，任一密钥错误时，重构信息均完全不能表征原始信息，

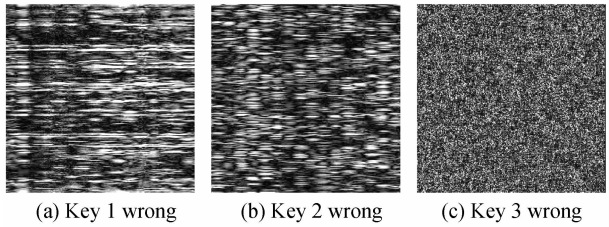

图 11　密钥错误时信息重构图

Fig. 11　The reconstruction images with wrong keys

只有在所有密钥均无误情况下，加密信息才能被精确重构.

另外，即使按传统检测方法能判断出隐藏了信息的事实，但密钥由生成规则产生而不需传输，破译过程计算量大、随机性强，密钥保密性高，故系统安全性理想.

3.3 仿真实验对比分析

为进一步检验基于压缩感知的图像信息加密效果，将本文加密方案与典型的 Arnold 置乱图像加密[30]方法进行对比实验.

对于大小为 $N\times N$ 的二维图像，Arnold 变换定义为

$$\begin{bmatrix}x'\\y'\end{bmatrix}=\begin{bmatrix}1&1\\1&2\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}(\mathrm{mod}\ N),\quad x,y\in\{0,1,2,\cdots,N-1\}\tag{10}$$

式中，(x,y) 为原始图像像素坐标，(x',y') 为置乱后的像素坐标. 此处 Arnold 置乱周期为 192，实验中进行了 100 次置乱.

3.3.1 灰度直方图对比

对原始图像使用 Arnold 置乱加密和本文方案加密，产生的加密图像及其对应直方图如图 12.

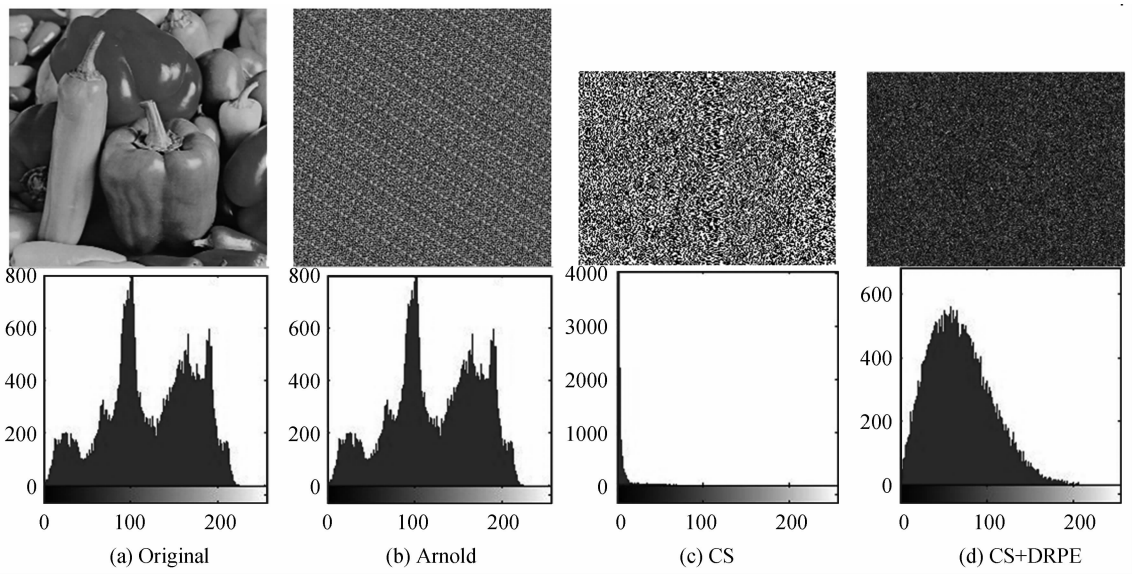

图 12 原始图像直方图与加密图像直方图对比

Fig. 12 Gray histgrams of original image and encrypted images

对比分析可知，Arnold 置乱加密(图 12(b))得到的密文图像的直方图在加密前后基本没有改变，这是因为 Arnold 置乱算法虽然改变了像素位置，但没有改变像素值大小. 而图像经压缩感知变换后(图 12(c))其直方图与原始图像直方图已完全不同且具有稀疏性，因为压缩感知加密过程所感知到的信息是在变换域具有稀疏性的信号. 将经压缩感知加密后图像再进行双随机相位编码(图 12(d))，图像直方图呈高斯分布，这是因为图像经本文方案加密后加密信息具有平稳白噪音特性. 综上，本加密系统充分实现了明文信息的混淆和扩散，没有简单的关系可循，因而能够掩盖明文的统计特性，可以较好的抵抗针对密文统计特性的破解攻击.

3.3.2 特性优势对比统计

通过实验测试，Arnold 置乱和压缩感知两种加密方法特性统计如表 1.

对比中，选取了两种加密情况下加密图像的灰度直方图、信息熵的变化，加密解密运算速度，抗噪及裁剪攻击能力以及密钥空间. 可以看出，压缩感知加密在抵御攻击方面具有更高的安全性. 原始图像的信息熵为 7.5895，Arnold 置乱加密后加密图像和原始图像的信息熵相同，说明这种加密方法像素统计特性没有改变. 压缩感知加密后信息熵减小，这是因为在该加密过程中需要数据抽样，故难免丢失部分信息. 在加解密速度方面，Arnold 置乱加密速度快，可以迅速处理大量的图像信息，但是由于 Arnold 置乱加密存在周期性，当变换次数为 192 的整数倍时，图像又恢复到原始图像，因而保密性不强. 基于压缩感知的加密方法由于使用多重加密，较 Arnold 置乱加密有更大的密钥空间，大大增加了计算量，因而使加、解密速度明显变慢，同时

表 1 Arnold 置乱加密和压缩感知加密特性优势对比统计

Table 1 The comparison to encrypted image by Arnold and CS

Encryption properties	Arnold encryption	CS encryption
Gray histogram	Unchanged	Changed utterly
Information entropy of encryption image	7.589 5	7.016 4
Encryption time/s	0.374 1	0.628 4
Decryption time/s	0.731 9	10.543 6
Anti noise ability	weak	strong
Anti cropping attack ability	worse	better
Key space	$\leqslant 10^{16}$	$\leqslant 10^{18}$

也表明如果破解这种加密方法需要很大的计算量.

4 结论

针对基于光学理论的信息加密系统虽具有数据并行处理、加密方式多样等特点但信息安全性不理想的问题，提出将压缩感知应用于基于光学系统的图像信息加密领域. 首先，对待加密信息进行随机观测、投影；然后，对经降维得到的投影值进行双随机相位编码得到加密信息；最后，将其隐藏在宿主图像中传输. 为防止密钥被截获，保障其安全，收发端不需传输密钥，只需按约定规则产生密钥，从而提高了加密系统安全性. 另外，由于随机观测过程中原始信号被降维，在二次加密过程中降低了随机相位板的大小，降低了光学系统设计成本. 仿真实验结果表明：该系统具有较理想的信号重构能力，能有效抵抗裁剪、噪音污染、高通滤波、旋转等攻击，系统鲁棒性强，安全性、保密性高.

参考文献

[1] WEI Zhi-qiang, YANG Guang, CONG Yan-ping. Security of underwater sensor networks [J]. *Chinese Journal of Computer*, 2012, **35**(8): 1594-1606.
魏志强，杨光，丛艳平. 水下传感器网络安全研究[J]. 计算机学报，2012，**35**(8)：1594-1606.

[2] CHEN Lai-jun, MEI Sheng-wei, CHEN Ying. Smart grid information security and its influence on power system survivability[J]. *Control Theory & Applications*, 2012, **29**(2):240-244.
陈来军，梅生伟，陈颖. 智能电网信息安全及其对电力系统生存性的影响[J]. 控制理论与应用，2012，**29**(2)：240-244.

[3] PAN Jing, QI Na, XUE Bing-bing, *et al*. Field programmable gate array-based chaotic encryption system design and hardware realization of cell phone short message[J]. *Acta Physica Sinica*, 2012, **61**(18): 72-83.
潘晶，齐娜，薛兵兵，等. 基于现场可编程门阵列的手机短信息混沌加密系统设计方案及硬件实现[J]. 物理学报，2012，**61**(18)：72-83.

[4] DIFFIE W, HELLMAN M F. New directions in cryptography [J]. *IEEE Transaction on Information Theory*, 1976, **22**(6): 644-654.

[5] SHANNON C E. Communication theory of secrecy systems[J]. *Bell System Technology Journal*, 1949, **28**(4): 656-715.

[6] QIN Yi, ZHENG Chang-bo. Color image encryption based on double random phase encoding[J]. *Acta Photonica Sinica*, 2012, **41**(3): 326-239.
秦怡，郑长波. 基于双随机相位编码的彩色图像加密技术[J]. 光子学报，2012，**41**(3)：326-239.

[7] YUAN S, ZHOU X, ALAM M S, *et al*. Information hiding based on double random-phase encoding technology and public-key cryptography[J]. *Optics Express*, 2009, **17**(5): 3270-3284.

[8] LU X, ZHOU X, LU P, *et al*. Determination of optimal parameters for detecting the existence of secret information hidden by the double random-phase encoding technique[J]. *Optics & Laser Technology*, 2009, **41**(6): 751-754.

[9] CAND′ES E J, ROMBERG J, TAO T, Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information[J]. *IEEE Transactions on Information Theory*, 2006, **52**(2): 489-509.

[10] JIAO Li-cheng, YANG Shu-yuan, LIU Fang, *et al*. Development and prospect of compressive sensing[J]. *Acta Electronica Sinica*, 2011, **39**(7): 1651-1662.
焦李成，杨淑媛，刘芳，等. 压缩感知回顾与展望[J]. 电子学报，2011，**39**(7)：1651-1662.

[11] XU Zhi-qiang. Compressed sensing [J]. *Scientia Sinica Mathematica*, 2012, **42**(9): 865-877.
许志强. 压缩感知[J]. 中国科学：数学，2012，**42**(9)：865-877.

[12] SHI Guang-ming, LIU Dan-hua, GAO Da-hua, *et al*. Advances in theory and applicaiton of compressed sensing[J]. *Acta Electronica Sinica*, 2009, **37**(5): 1071-1081.
石光明，刘丹华，高大化，等. 压缩感知理论及其研究进展[J]. 电子学报，2009，**37**(5)：1071-1081.

[13] VENKATRAMAN D, MAKUR A. A compressive sensing approach to object-based surveillance video coding[J]. *IEEE Acoustics, Speech and Signal Processing*, 2009: 3513-3516.

[14] SHI Guang-ming, LIU Dan-hua, ZHOU Jia-she, *et al*. New method of multiple description coding for image based on compressed sensing [J]. *Journal of Infrared Millimeter Waves*, 2009, **28**(4): 298-302.
石光明，刘丹华，周佳社，等. 基于 Compressed Sensing 框架的图像多描述方法[J]. 红外与毫米波学报，2009，**28**(4)：298-302.

[15] ORSDEMIR A, ALTUN H O, SHARMA G, *et al*. On the security and robustness of encryption via compressed sensing [C]. *IEEE Military Communications Conference*, 2008: 1-7.

[16] LIANG Jing-sai. Image secret sharing based on compressed sensing[C]. Advances in Mathematics and Its Applications, 2011:149-162.
梁敬赛. 基于压缩感知的秘密图像分存[C]. 数学及其应用新进展，2011:149-162.

[17] 杨震，叶蕾，徐挺挺. 基于压缩感知和信息隐藏的语音保密通信系统设计方法：中国，102034478B[P]. 2013-10-30.

[18] HUANG R, SAKURAI K. A robust and compression-combined digital image encryption method based on compressive sensing[C]. Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011 Seventh International Conference on. IEEE, 2011: 105-108.

[19] 周南润，张艾华，吴建华，等. 测量矩阵受控的图像压缩感知与图像加密方法：中国，102833514A[P]. 2012-12-19.

[20] ATHIRA V, GEORGE S N, DEEPTHI P P. A novel encryption method based on compressive sensing [C]. Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on. IEEE, 2013: 271-275.

[21] ZHANG A, ZHOU N, GONG L. Color image encryption algorithm combining compressive sensing with arnold transform [J]. *Journal of Computers*, 2013, **8**(11): 2857-2863.

[22] RACHLIN Y, BARON D. The secrecy of compressed sensing measurements[C]. 46th Annual Allerton Conference on Communication, Control and Computing, 2008, 813-817.

[23] REFREGIER P, JAVIDI B. Optical image encryption based on input plane and Fourier plane random encoding[J]. *Optics Letters*, 1995, **20**(7): 767-769.

[24] JAVIDI B, SERGENT A, AHOUZI E. Performance of double phase encoding encryption technique using binarized encrypted images[J]. *Optical Engineering*, 1998, **37**(2): 565-569.

[25] CANDÉS E J, WAKIN M, An introduction to compressive sampling[J]. *IEEE Signal Processing Magazine*, 2008, **25**(2): 21-30.

[26] DONOHO D L, Compressive sensing[J]. *IEEE Transaction on Information Theory*, 2006, **52**(4): 1289-1306.

[27] BARANIUK R G. Compressive sensing[J]. *IEEE Signal Processing Magazine*, 2007, **24**(4): 118-120, 124.

[28] BAILEY D H, CRANDALL R E. On the random character of fundamental constant expansions [J]. *Experimental Mathematics*, 2001, **10**(2): 175-190.

[29] PRASAD M, SUDHA K L. Chaos image encryption using pixel shuffling [J]. *Computer Science & Information Technology*, 2011, **4**(1): 169-179.

[30] YE G. Image scrambling encryption algorithm of pixel bit based on chaos map[J]. *Pattern Recognition Letters*, 2010, **31**(5): 347-354.