基于压缩感知的光学干涉双灰度图像加密系统

白音布和[1] 吕晓东[2] 李根全[2] 秦 怡[2*]

[1]通辽职业学院机电工程学院, 内蒙古 通辽 028000

[2]南阳师范学院物理与电子工程学院, 河南 南阳 473061

摘要 提出了一种基于压缩感知(CS)和干涉原理的双灰度图像加密方法。该方法分别从两幅灰度图像中随机提取50%的数据,并将这些数据通过融合形成一幅合成图像(SI)。再将该合成图像加密至三个纯相位板(POMs)中。其中一个随机相位板使用随机函数生成,另外两个通过解析的方法得到。解密时,利用分束片对3个POMs的衍射场进行叠加,在光学解密装置中利用CCD记录合成图像,再从合成图像中分别提取的两幅原始图像信息。尽管对于每一幅原始图像来说,只能准确提取其50%的数据,但是压缩感知重构算法可以高质量的重现这两幅原始图像。与先前提出的方法相比,该方法加密过程是一个完全采用解析算法的过程,并且非常省时,因为在解密过程中没有迭代算法。此外,该方法也消除了先前提出的光学干涉加密方法存在的轮廓像问题,具有较高的安全性。计算机模拟结果证实了该方法的有效性。

关键词 傅里叶光学; 图像加密; 压缩感知; 干涉原理; 轮廓像问题

中图分类号 TP751 **文献标识码** A

doi: 10.3788/LOP53.041002

Optical Interference Double Gray Image Encryption System Based on Compressive Sensing

Bai Yinbuhe[1] Lü Xiaodong[2] Li Genquan[2] Qin Yi[2]

[1]*School of Mechanical and Electric Engineering Technology, Tongliao Technical College, Tongliao, Inner Mongolia* 028000, *China*

[2]*College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang, Henan* 473061, *China*

Abstract A novel double gray image encryption method is proposed based on compressive sensing (CS) and interference principle. The 50% image data of two gray images are random extracted by the proposed method, these data are combined to form a synthetic image (SI), and then it is hidden into three phase only masks (POMs). One of the phase masks is produced by random function and the other two are obtained by analytic method. For decryption, the diffraction fields of the three POMs are superposed by employing the beam splitters. The intensity of the complex field, namely the SI, is captured by CCD camera, and then the information of two original images is extracted from the SI. Although only 50% fragmentary data are extracted, the subsequent CS reconstruction will retrieve a high quality image from the fragmentary information. Compared with the earlier interference-based method, the proposed approach is a process of employing resolution algorithm completely and time-saving since no iterative algorithm is involved in the encryption process. Moreover, the silhouette problem existing in the earlier method is resolved by the proposed method with higher security. Simulation results are presented to support the validity of the proposed approach.

Key words Fourier optics; image encryption; compressive sensing; principle of interference; silhouette problem

OCIS codes 070.2025; 070.4560; 070.7345

1 引 言

近年来,基于光学原理的信息安全技术引起了广泛的重视,成为了信息光学领域的重要研究方向[1-13]。

收稿日期: 2015-09-21; **收到修改稿日期**: 2015-11-03; **网络出版日期**: 2016-03-05

基金项目: 国家自然科学基金(61505091)、河南省科技厅基础与前沿计划项目(142300410454)、南阳师范学院青年基金(QN2015013)、河南省高等学校重点科研项目(16A416010)

作者简介: 白音布和(1963—),男,学士,副教授,主要从事光电信息处理方面的研究。E-mail: BYBH@163.com

*通信联系人。E-mail: 641858757@qq.com

其原因在于,光学加密方法不但能够在加密的过程中自然地融合各种物理参数,例如波长、偏振态、衍射距离等,而且能够对图像进行并行高速处理。这些特性是对传统信息安全技术的变革性突破。双随机相位编码系统(DRPE)是该领域最早的成果之一[14]。自从该系统被提出,针对其系统安全性的分析以及开发由其衍生出来的各种光学加密系统成为研究的热点[15-18]。然而,DRPE及其衍生系统的密文均为复数,需要采用干涉装置进行记录,非常不便。此外,现有的空间光调制器无法显示复数,这些系统也不便于使用光学方法进行解密。为了克服这些缺点,人们开始考虑将图像隐藏于纯相位板(POM)中[19-21],这是因为相位板可以用空间光调制器直接显示,而且,相位板非常难复制,安全性很高。其中,2008年,Zhang等[21]提出了基于干涉原理的加密方法(IBE),引起了广泛的兴趣和关注。该方法可以将原始图像解析地隐藏于两个随机相位板中,因此加密过程非常省时。此外,解密时,利用这两个相位板,解密者可以利用CCD等强度感应器件直接记录解密图像。由于这两个显著的特性,该系统引起了广泛的关注[22-25]。

目前,随着信息技术特别是互联网技术的高速发展,图像信息传输量与图像信息交换量与日俱增。为了提高信息加密效率,人们对加密系统中加密容量的要求越来越高。于是一些多图像加密技术相继出现[26-32],其中包含一些尝试在IBE系统中实现多图像加密的方法。例如,本课题组曾经提出一种利用距离复用技术在IBE系统中实现多图像加密的方法,然而由于串扰噪声的干扰,该方法仅适用于二值图像[30]。Wang等[31]和Chen等[32]也在IBE系统中实现了双灰度图像加密和多灰度图像加密,但是其加密过程均涉及迭代算法,加密十分耗时,整个加密过程不再便捷。为了解决这个问题,本文将压缩感知技术和空间复用技术相结合,提出了一种在IBE系统中实现双灰度图像加密的方法。该方法从两幅原始图像中分别提取50%的数据,然后将这些数据利用空间复用技术融合为一个目标图像,再利用解析方法将目标图像隐藏于三个POM中。由于加密过程无需迭代,该方法继承了IBE系统省时的特点,适应于对加密过程时效要求较高的应用。解密时,尽管只能从直接解密结果中提取到每一幅原始图像50%的数据,但是之后的压缩感知技术可以保证高质量的重建两幅原始图像,并给出了理论分析及计算机模拟结果。

2 原理分析

2.1 压缩感知

近年来,压缩感知理论(CS)成为国内外学者研究的热点问题,其在计算机断层成像、合成孔径成像等领域得到广泛应用[33]。压缩感知作为一种新的采样理论,由Candès等[34]和Donoho[35]在2006年提出。它颠覆了传统的采样理论观点,认为假定信号是稀疏的或在某变换域内可稀疏表示,则可在远小于Nyquist采样率的条件下,采样获取信号的少量离散样本,然后利用重建算法高精确重建信号。压缩感知主要依赖于两个基本原理,即稀疏性和非相干性[35]。假设 f 是一个 $N\times1$ 的输入信号,稀疏性是指可以在某一个基 $\boldsymbol{\Psi}$ 上稀疏地表示,即可表示为

$$\boldsymbol{f}=\boldsymbol{\Psi}\alpha\,, \tag{1}$$

式中 $\boldsymbol{\Psi}$ 是指稀疏变换,α 是一个 S 稀疏 ($S\ll N$) 信号。CS采样信号的基本模型可以表示为

$$z=\boldsymbol{\Phi}\boldsymbol{f}=\boldsymbol{\Phi}\boldsymbol{\Psi}\alpha\,, \tag{2}$$

式中 z 表示对信号 $\boldsymbol{f}$ 的观测值,$\boldsymbol{\Phi}$ 为观测矩阵,其大小为 $M\times N$ ($M<N$)。对信号 $\boldsymbol{f}$ 的观测为非自适应的,这表明 $\boldsymbol{\Phi}$ 不依赖于 $\boldsymbol{f}$。非相干性是指观测矩阵与变换矩阵 $\boldsymbol{\Psi}$ 不相干,二者的相干函数定义为

$$\mu(\boldsymbol{\Phi},\boldsymbol{\Psi})=\sqrt{N}\cdot\max_{1\leqslant p,q\leqslant N}\left|\left\langle\boldsymbol{\varphi}_p,\boldsymbol{\psi}_q\right\rangle\right|, \tag{3}$$

式中 $\boldsymbol{\varphi}_p$ 为 $\boldsymbol{\Phi}$ 的行向量,$\boldsymbol{\psi}_q$ 是 $\boldsymbol{\Psi}$ 的列向量。如果公式 $1/\sqrt{N}\leqslant\mu(\boldsymbol{\Phi},\boldsymbol{\Psi})\leqslant1$ 成立,那么认为观测矩阵与变换矩阵 $\boldsymbol{\Psi}$ 不相干。在满足稀疏性和非相干性的前提下,对原始信号f的重构过程可以简化为一个$\ell1$范数最小化的问题[34],即

$$\min_{\alpha}\left\|\alpha\right\|_1\ \text{ s.t. }\ z=\boldsymbol{\Phi}\boldsymbol{\Psi}\alpha\,, \tag{4}$$

需要指出的是,对一个自然图像而言,其梯度是稀疏的。换句话说,一个自然图像在梯度变换域内是稀疏的,而梯度函数的$\ell1$范数正是图像的全变差。因此,另外一种常用的最小化问题是全变差最小化法。如果此处将二维图像信号也定义为 $\boldsymbol{f}$,全变差最小化问题可表述为[36]

$$\min_{f} \mathrm{TV}(f) \ \text{s.t.} \ z = \boldsymbol{\Phi} f$$

$$\text{with} \ \mathrm{TV}(f) = \sqrt{\left(f_{i+1,j} - f_{i,j}\right)^2 + \left(f_{i,j+1} - f_{i,j}\right)^2}, \tag{5}$$

式中TV表示求函数的全变差。

2.2 基于干涉原理的光学加密系统

一种典型的基于干涉原理的光学加密系统如图1所示。该系统包含三个纯相位板，其中相位板 P_1、P_2 为密文，而相位板 P_3 为密钥，其解密过程可简述如下。假设波长为 λ 的单色平面光波照射相位板 P_1、P_2，之后二者的衍射场首先被分束镜(BS)所结合，经过距离为 l 的衍射之后，到达 S 平面。相位板 P_3 即位于 S 平面，因此，此干涉场将被随机相位板 P_3 进一步调制，再经过距离为 d 的衍射到达输出平面 H，此时平面 H 的复数场的强度即为原始图像，可以使用图像传感器(如CCD等)即可直接记录。

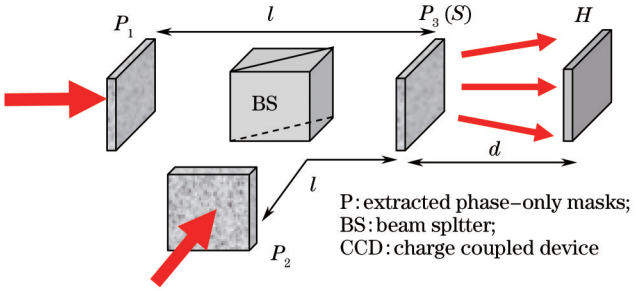

图1 基于干涉原理光学加密系统图

Fig.1 Schematic of optics encryption system based on principle of interference

加密算法为上述解密过程的逆过程，即把原始图像信息隐藏于 P_1、P_2 及 P_3 之中。其中 P_3 的相位值由计算机随机函数产生，其相位值记为 $P_3(x,y)$。假设 $\boldsymbol{o}(x_o,y_o)$ 是归一化的原始图像，通过其赋予一个随机的白噪声相位构造出一个新的函数

$$o'(x_o,y_o) = \sqrt{o(x_o,y_o)}\exp\left[\mathrm{j}2\pi \cdot \mathrm{rand}(x_o,y_o)\right], \tag{6}$$

这里 (x_o,y_o) 表示输出平面坐标，rand函数用于产生位于[0,1]区间的均匀分布的随机数。假设该复函数被一波长为 λ 的单色平面波所照射，并从输出平面 H 逆衍射至平面 S。平面 S 上位于 P_3 左侧所得到的衍射光场 $e(x,y)$ 可用数学公式描述为

$$e(x,y) = P_3^*(x,y)\mathrm{FrT}_{\lambda}\left[o'(x_o,y_o);-d\right], \tag{7}$$

式中 (x,y) 表示平面 S 上的坐标。FrT_{λ} 表示对于波长 λ 的菲涅耳变换[13]。根据如图1所示的解密过程可知，相位板 P_1、P_2 的相位值与复值函数 $e(x,y)$ 满足如下关系：

$$e(x,y) = \exp(\mathrm{j}p_1) * h(x,y,l) + \exp(\mathrm{j}p_2) * h(x,y,l), \tag{8}$$

式中 $\exp(\mathrm{j}p_1)$ 为 P_1 的相位值，$\exp(\mathrm{j}p_2)$ 为 P_2 的相位值，$*$ 表示卷积运算，$h(x,y,l)$、$h(x,y,d)$ 是自由空间衍射过程的脉冲响应函数，可表示为

$$h(x,y,l) = \frac{\exp(\mathrm{j}2\pi l/\lambda)}{\mathrm{j}\lambda l}\exp\left[\mathrm{j}\pi\left(x^2+y^2\right)/\lambda l\right], \tag{9}$$

由于 P_1、P_2 为纯相位板，除了满足(7)式之外，还满足条件

$$\left[\exp(\mathrm{j}p_1)\right]\left[\exp(\mathrm{j}p_1)\right]^* = \left[\exp(\mathrm{j}p_2)\right]\left[\exp(\mathrm{j}p_2)\right]^* = 1, \tag{10}$$

结合(7)式及(9)式，可以求得 $p_1(x,y)$ 和 $p_2(x,y)$ 的解析式分别为

$$p_1(x,y) = \arg(D) - \arccos\left[\mathrm{abs}(D)/2\right], \tag{11}$$

$$p_2(x,y) = \arg\left\{D - \exp\left[\mathrm{i}p_1(x,y)\right]\right\}, \tag{12}$$

式中 $\arg(\cdot)$ 和 $\mathrm{abs}(\cdot)$ 分别表示取复数的辐角与模。此外，有

$$D=\mathscr{F}^{-1}\left\{\frac{\mathscr{F}\left[e(x,y)\right]}{\mathscr{F}\left[h(x,y,l)\right]}\right\}, \tag{13}$$

式中 $\mathscr{F}$ 及 $\mathscr{F}^{-1}$ 表示傅里叶变换及逆变换。这样，原始图像 $o(x_o,y_o)$ 就成功地被隐藏在了这两个随机相位板之中，实现了加密的目的。为了方便起见，把得到 P_1、P_2 的加密过程表示为

$$P_1=\Gamma\left[o(x_o,y_o),\lambda;l;d\right], \tag{14}$$

$$P_2=\Omega\left[o(x_o,y_o),\lambda;l;d\right], \tag{15}$$

利用如图1所示解密装置或者使用数字方法均可对加密结果进行解密而得到原始图像。

2.3 本文方法

由2.2节可知，IBE系统的加密过程没有涉及迭代，所以加密过程的省时性是IBE系统最重要的特性之一。然而，为了能在IBE系统中加密两幅和两幅以上的灰度图像，Wang等[31]和Chen等[32]均提出采用迭代算法。这样IBE系统的加密过程的省时性就被加密容量所抵消，或者说，这些系统通过牺牲加密时间而换取加密容量的提升。在2.1节已经指出，压缩感知提供了利用图像稀疏数据完全恢复图像的可能，基于这种考虑，在IBE系统中提出一种新的双灰度图像加密方法。假设 $f(x_o,y_o)$ 和 $g(x_o,y_o)$ 为两幅原始图像，分别取它们50%的稀疏数据，然后将二者的稀疏数据合成一个新的图像，这个过程可以表示为

$$\overline{fg(x_o,y_o)}=f(x_o,y_o)\boldsymbol{RM}(x_o,y_o)+g(x_o,y_o)\left[1-\boldsymbol{RM}(x_o,y_o)\right], \tag{16}$$

式中 $\boldsymbol{RM}(x_o,y_o)$ 为一个随机二值振幅板(RBAM)。$\boldsymbol{RM}(x_o,y_o)$ 只包含0和1两种数值，且数值1在全部矩阵元素中所占的比例约为50%。而运算 $\left[1-\boldsymbol{RM}(x_o,y_o)\right]$ 用以产生 $\boldsymbol{RM}(x_o,y_o)$ 的互补矩阵。$\boldsymbol{RM}(x_o,y_o)$ 作为密钥保存。通过(15)式的处理，既能够将两幅原始图像的数据融合为一幅图像大小，同时能够使二者的数据互不重叠。在获取 $\overline{fg(x_o,y_o)}$ 之后，再利用2.2节的方法，将其隐藏与三个相位板之中，这个过程可表示为

$$P_1=\Gamma\left[\overline{fg(x_o,y_o)},\lambda;l;d\right], \tag{17}$$

$$P_2=\Omega\left[\overline{fg(x_o,y_o)},\lambda;l;d\right]. \tag{18}$$

解密过程是加密过程的逆过程，在图1装置中利用CCD记录下解密图像，即复合图像 $\overline{fg(x_o,y_o)}$。之后，将先前保存的 $\boldsymbol{RM}(x_o,y_o)$ 乘以 $\overline{fg(x_o,y_o)}$，即可提取出属于原始图像 $f(x_o,y_o)$ 的稀疏数据 $f^S(x_o,y_o)$，这样可以得到

$$f^S(x_o,y_o)=\boldsymbol{RM}(x_o,y_o)f(x_o,y_o), \tag{19}$$

即拟从(19)式中恢复 $f(x_o,y_o)$。需要指出的是，(19)式所描述的采样过程为(2)式采样过程的广义形式[37]。在这种情况下，$\boldsymbol{RM}(x_o,y_o)$ 作为采样矩阵直接从空域采样原始图像。尽管原始图像的部分信息在空域中直接丢失，但是 $\boldsymbol{RM}(x_o,y_o)$ 的随机性及自然图像在梯度域的稀疏性保证了原始图像可以被正确地重建，参考文献[38]。采用全变差最小化方法来复原 $f(x_o,y_o)$，将(19)式所述的欠定问题描述为

$$\min_{f}\ \mathrm{TV}\left[f(x_o,y_o)\right]\ \ \text{s.t.}\ \ f^S(x_o,y_o)=\boldsymbol{RM}(x_o,y_o)f(x_o,y_o), \tag{20}$$

文献[37]给出了求解(20)式广义压缩感知问题的详细算法，因此不再给出。类似地，同样可以准确地恢复 $g(x_o,y_o)$。

3 计算机模拟实验

为了证实本文方法的有效性及可行性，在计算机上使用Matlab R2011a进行了仿真实验。模拟中，两个距离参数分别为 $l=100$ mm，$d=200$ mm。照明所用单色平面波波长 $\lambda=632.8$ nm。图2给出了使用本文方法的加密结果。图2(a)、(b)分别为两幅待加密的原始图像Lena和Peppers，其大小均为256 pixel×256 pixel。图2(c)为随机二值矩阵(RBAM)。图2(d)、(e)分别为利用RBAM及其互补矩阵从Lena和Peppers中分别提取出来的稀疏数据(有效数据占总数据量的50%)。图2(f)是由图2(d)、(e)根据(15)式计算出来的合成图像。图2(g)~(i)分别为三个纯相位板 P_1~P_3，其中 P_3 是由Matlab软件rand函数生成。

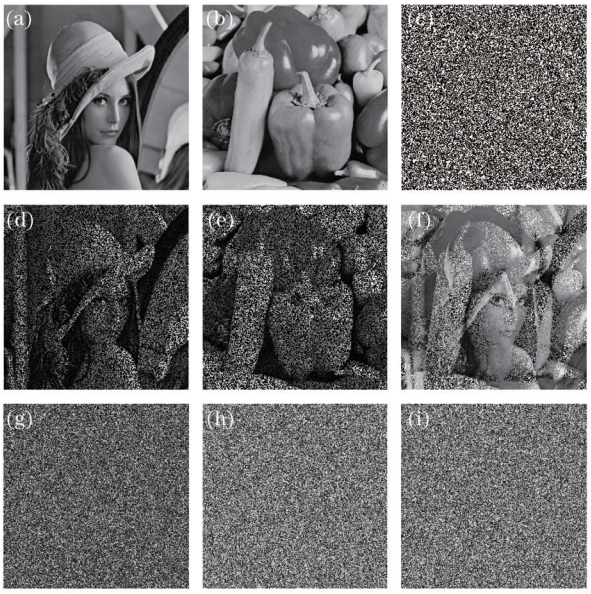

图2 使用本文算法加密结果。(a) Lena; (b) Peppers; (c) 随机二值矩阵; (d)、(e) 从两幅原始图像中提取出来的部分数据; (f) 由(d)和(e)合成的图像; (g) P_1; (h) P_2; (i) P_3

Fig.2 Encryption results with proposed method. (a) Lena; (b) Peppers; (c) RBAM; (d), (e) sparse data extracted from the two primary images; (f) synthetic image composed by (d) and (e); (g) P_1; (h) P_2; (i) P_3

图3(a)、(b)给出了在所有参数正确情况下的解密图像。为了客观的评价解密图像的质量,此处引入相关系数作为标准来表达恢复图像 f_{rec} 与原始图像 f 的符合程度。相关系数(CC)被定义为

$$X_{\mathrm{CC}}=\frac{E\left\{\left[f-E(f)\right]\left[\left|f_{\mathrm{rec}}\right|-E\left(\left|f_{\mathrm{rec}}\right|\right)\right]\right\}}{\left\{E\left\{\left[f-E(f)\right]^2\right\}E\left\{\left[\left|f_{\mathrm{rec}}\right|-E\left(\left|f_{\mathrm{rec}}\right|\right)\right]^2\right\}\right\}^{\frac{1}{2}}},\tag{21}$$

式中 E 表示求数学期望运算,简明起见这里省略了函数坐标。对应于图3(a)、(b)的相关系数分别为 X_{CC} = 0.9915, X_{CC} =0.9889,这说明两幅原始图像被高质量地恢复出来。图3(c)、(d)给出了当密钥 P_3 错误时的解密结果,其对应的相关系数为 X_{CC} =−0.0022, X_{CC} =0.0076。由此可知,当密钥错误时,攻击者无法获取原始明文的任何信息。

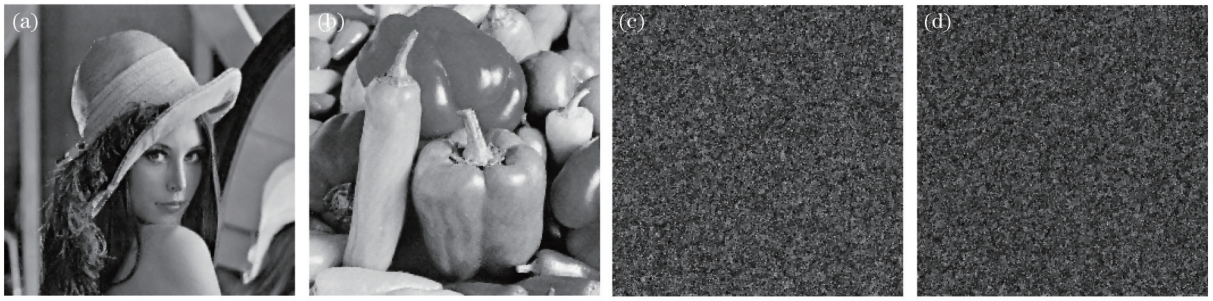

图3 使用正确密钥解密出来的(a) Lena和(b) Peppers; 使用错误的 P_3 解密出来的(c) Lena和(d) Peppers

Fig.3 Retrieved (a) Lena and (b) Peppers with correct keys; retrieved (c) Lena and (d) Peppers with incorrect P_3

除了相位板 P_3 之外,衍射距离 d 和 l,以及照明波长 λ 均可作为附加密钥使用。$\Delta\lambda$ 和 Δl 分别表示恢复图像所使用波长和距离与真实值之间的偏差,计算了相关系数与二者之间的依赖关系,结果如图4所示。可以看出,在波长和距离存在较小偏差时,相关系数即迅速下降至零附近,说明本文算法对附加参数相当敏感。换句话说,在解密参数与原始数值存在较小误差的情况下,都无法准确还原原始图像。相关系数与距离偏差 Δd 的关系与 Δl 类似,因此不再给出。此外,由于这些附加参数互相独立,所以攻击者除非精确掌握波长与距离参数,否则很难依靠穷举法来破解该系统。因而该系统拥有巨大的密钥空间和安全性。

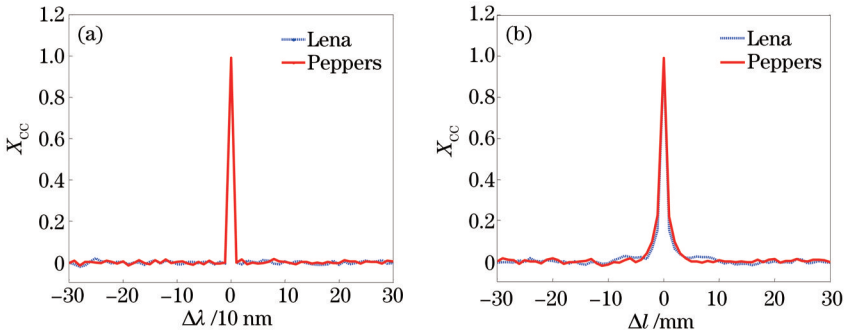

图4 解密时重建波长偏差及距离偏差与相关系数之间的关系

Fig.4 Relationship between correlation coefficient and wavelength deviation and distance deviation while decryption

之前的研究已经指出，由Zhang等[21]提出的IBE系统存在一个非常严重的安全问题，如果攻击者获取了两个随机相位板中的一个，则利用如图1所示的解密系统，就可观测到原始图像的轮廓，也就是IBE系统的轮廓像问题。针对于这个问题，Zhang等[24]提出对两个随机相位板的相位值进行随机地交换，从而打乱相位值的位置信息，即可消除轮廓像问题。但是此方法导致加密过程异常耗时，降低了IBE系统的实用性。正如文献[24]所指出，轮廓像问题的根源在于原始图像和与之对应的两个相位板之间的直接解析关系。因此通过两个技术来消除轮廓像问题：1) 在产生相位板P_1和P_2的过程中，引入了随机相位板P_3对光场进行扰乱，避免了原始图像与P_1和P_2的直接解析关系；2) 本文方法中原始图像本质上为两幅图像的像素的随机组合，因此与加密单幅图像相比，该原始图像本身类似于噪声图样[图2(f)]，破坏了轮廓像存在的基础。作为比较，图5(a)与(b)给出了在其他参数正确情况下，利用本文方法，单独使用P_1、P_2进行解密时图像的恢复结果，此时所得的解密结果为噪声图样，直观上已经获取不到任何有效信息。图5(a)与(b)对应的相关系数分别为0.0003，−0.0018，其绝对值远小于1。说明该系统中单独获取密文P_1或者P_2完全无法获取原始图像的轮廓，因而轮廓像问题在该系统得到了彻底地抑制。

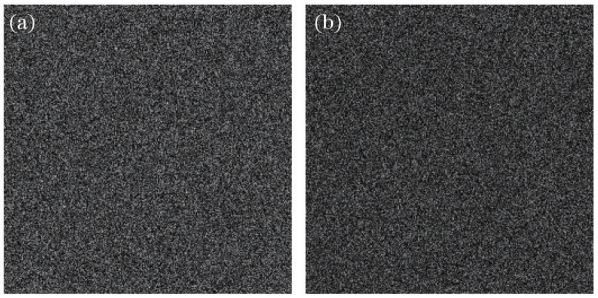

图5 (a) P_1和(b) P_2得到的解密结果

Fig.5 Decryption results from (a) P_1 and (b) P_2

由于需要利用压缩感知恢复算法准确地恢复出原始图像，所以对两幅原始图像的取样方式必须是随机取样，如(16)式所示，才能保证采样矩阵与变换矩阵的非相干性，这是压缩感知理论成立的前提。如果按照图6(a)所示的方法来组成一幅合成图像，尽管仍然从两幅图像各取50%数据，但却不能正确恢复出原始图像。为了证实这一点，在图6(b)、(c)中给出了这种情况下恢复出的两幅原始图像，可见重建效果很低。其原因在于当每幅图像各取50%的情况下，此时的采样矩阵为规则的取样矩阵。以Peppers为例，其采样矩阵为左半部分取值全部为1，右半部分取值全部为0，这种规则的取样矩阵与变换矩阵相关程度达不到足够低，破坏了压缩感知重建的条件。

此外，利用(16)式的空间复用技术，可以将更多的图像融合到一幅合成图像中，从而提高系统的加密容量。为了研究本文方法的加密容量，假设将N幅原始图像融合到一个合成图像之中，那么将对每幅原始图像取出$(100/N)\%$的数据。可以推断，随着N的增大，从每幅图像所采样的数据量也就越少。相应地，由这些数据恢复出来的原始图像的质量也就越低。这里以Peppers为例，给出了N=10、8、5、3时对其重建的结果，如图7(a)~(d)所示。与之对应的相关系数分别为0.9304、0.9438、0.9650、0.9824。这证实了上述推断。如果将相关系数取为0.9300作为图像重建质量标准，那么本文方法的加密容量即为N=10。

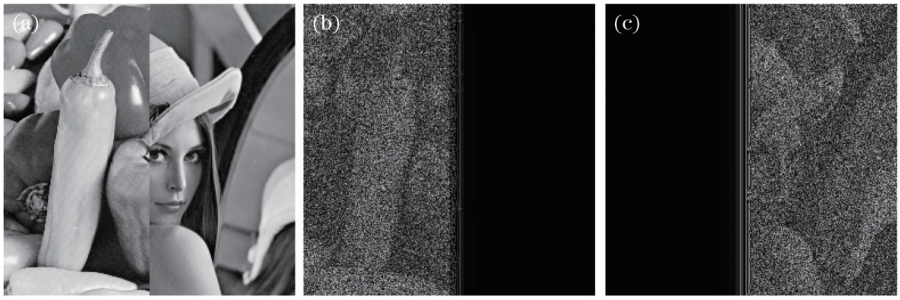

图6 (a) 合成图像; (b) 恢复出的Peppers; (c) 恢复出的Lena

Fig.6 (a) Synthetic image; (b) retrieved Peppers; (c) retrieved Lena

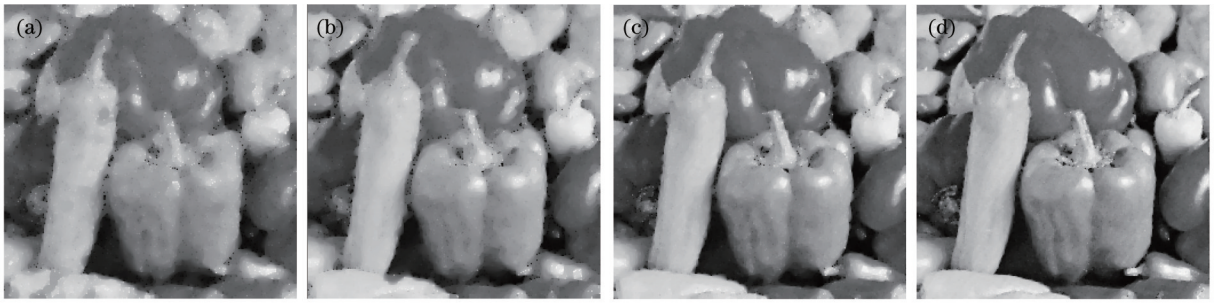

图7 加密N幅图像时恢复出来的原始图像。 (a) N=10; (b) N=8; (c) N=5; (d) N=3

Fig.7 Retrieved original images with encryption N images. (a) N=10; (b) N=8; (c) N=5; (d) N=3

4 结 论

在压缩感知的理论框架下,提出了一种新的光学加密系统,该系统成功地将两幅图像隐藏至三个纯随机相位板中。整个加密过程没有利用迭代算法,因此与先前的IBE系统中的多灰度图像加密方法相比,本文方法继承了IBE系统加密过程非常省时的优点。解密时采用压缩感知技术从部分图像信息中高质量地恢复出原始图像。不仅如此,本文方法也消除了基于干涉原理的加密方法中所谓的轮廓像问题,系统的安全性得到了进一步提升。

参 考 文 献

1 Han Chao, Wan Rui, Liu Yang, *et al*.. A double encry ption algorithm research based on computer generated hologram[J]. Chinese J Lasers, 2015, 42(9): 0909001.

韩超,万芮,刘洋,等. 基于计算全息图的双重加密算法研究[J]. 中国激光, 2015, 42(9): 0909001.

2 Hou Junfeng, Huang Sujuan, Situ Guohai. Nonlinear optical image encryption[J]. Acta Optica Sinica, 2015, 35(8): 0807001.

侯俊峰, 黄素娟, 司徒国海. 非线性光学图像加密[J]. 光学学报, 2015, 35(8): 0807001.

3 Liu Xiaoyong, Cao Yiping, Lu Pei. Research on optical image encryption technique with compressed sensing[J]. Acta Optica Sinica, 2014, 34(3): 0307002.

刘效勇, 曹益平, 卢 佩. 基于压缩感知的光学图像加密技术研究[J]. 光学学报, 2014, 34(3): 0307002.

4 Qin Yi, Li Jing, Ma Maofen, *et al*.. System for optical multiple binary image encryption by random phase mask multiplexing [J]. Acta Optica Sinica, 2014, 34(3): 0307001.

秦 怡, 李 婧, 马毛粉, 等. 一种基于随机相位板复用的光学多二值图像加密系统[J]. 光学学报, 2014, 34(3): 0307001.

5 Bai Yinbuhe, Li Genquan, Lü Linxia, *et al*.. Optical image encryption with ciphertext of a single diffraction intensity pattern [J]. Laser & Optoelectronics Progress, 2014, 51(10): 100701.

白音布和, 李根全, 吕林霞, 等. 以单幅衍射强度图像为密文的光学衍射成像加密系统[J]. 激光与光电子学进展, 2014, 51(10): 100701.

6 Z Liu, J Dai, X Sun, *et al*.. Generation of hollow Gaussian beam by phase-only filtering[J]. Opt Express, 2008, 16(24): 19926-19933.

7 Z Liu, S Liu. Random fractional Fourier transform[J]. Opt Lett, 2007, 32(15): 2088-2090.

8 N Zhou, T Dong, J Wu. Novel image encryption algorithm based on multiple-parameter discrete fractional random transform

[J]. Opt Commun, 2010, 283(15): 3037-3042.

9 N Zhou, Y Wang, L Gong. Novel optical image encryption scheme based on fractional Mellin transform[J]. Opt Commun, 2011, 284(13): 3234-3242.

10 Qin Yi, Zhang Shuai, Gong Qiong, *et al*.. Virtual optical image encryption based on interference[J]. Acta Optica Sinica, 2012, 32(10): 1007001.

秦 怡, 张 帅, 巩 琼, 等. 基于干涉原理的虚拟光学加密系统[J]. 光学学报, 2012, 32(10): 1007001.

11 N Zhou, Y Wang, L 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.

12 W Qin, X Peng. Asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. Opt Lett, 2010, 35(2): 118-120.

13 X Wang, D Zhao. Security enhancement of a phase-truncation based image encryption algorithm[J]. Appl Opt, 2011, 50(36): 6645-6651.

14 P Refregier, B Javidi. Optical image encryption based on input plane and Fourier plane random encoding[J]. Opt Lett, 1995, 20(7): 767-769.

15 Peng Xiang, Tang Hongqiao, Tian Jindong. Ciphertext-only attack on double random phase encoding optical encryption system[J]. Acta Physica Sinica, 2007, 56(5): 2629-2636.

彭 翔, 汤红乔, 田劲东. 双随机相位编码光学加密系统的唯密文攻击[J]. 物理学报, 2007, 56(5): 2629-2636.

16 Peng Xiang, Zhang Peng, Wei Hengzheng, *et al*.. Known-plaintext attack on double phase encoding encryption technique [J]. Acta Physica Sinica, 2006, 55(3): 1130-1136.

彭 翔, 张 鹏, 位恒政, 等. 双随机相位加密系统的已知明文攻击[J]. 物理学报, 2006, 55(3): 1130-1136.

17 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.

18 G Situ, J Zhang. Double random-phase encoding in the Fresnel domain[J]. Opt Lett, 2004, 29(14): 1584-1586.

19 H T Chang, W C Lu, C J Kuo. Multiple-phase retrieval for optical security systems by use of random-phase encoding[J]. Appl Opt, 2002, 41(23): 4825-4834.

20 Y Li, K Kreske, J Rosen. Security and encryption optical systems based on a correlator with significant output images[J]. Appl Opt, 2000, 39(29): 5295-5301.

21 Y Zhang, B Wang. Optical image encryption based on interference[J]. Opt Lett, 2008, 33(21): 2443-2445.

22 Qin Yi, Gong Qiong, Li Genquan, *et al*.. An 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.

23 Y Han, Y Zhang. Optical image encryption based on two beams' interference[J]. Opt Commun, 2010, 283(9): 1690-1692.

24 Y Zhang, B Wang, Z Dong. Enhancement of image hiding by exchanging two phase masks[J]. Journal of Optics A: Pure and Applied Optics, 2009, 11(12): 125406.

25 X Wang, D Zhao. Optical image hiding with silhouette removal based on the optical interference principle[J]. Appl Opt, 2012, 51(6): 686-691.

26 M Z He, L Z Cai, Q Liu, *et al*.. Multiple image encryption and watermarking by random phase matching[J]. Opt Commun, 2005, 247(1-3): 29-37.

27 X Yong-Liang, X Su, S Li, *et al*.. Key rotation multiplexing for multiple-image optical encryption in the Fresnel domain[J]. Optics & Laser Technology, 2011, 43(4): 889-894.

28 W Liu, Z Xie, Z Liu, *et al*.. Multiple-image encryption based on optical asymmetric key cryptosystem[J]. Opt Commun, 2015, 335: 205-211.

29 X Wang, D Zhao. Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain[J]. Opt Commun, 2011, 284(1): 148-152.

30 Y Qin, Q Gong. Interference-based multiple-image encryption with silhouette removal by position multiplexing[J]. Appl Opt, 2013, 52(17): 3987-3992.

31 B Wang, Y Zhang. Double images hiding based on optical interference[J]. Opt Commun, 2009, 282(17) : 3439-3443.

32 W Chen, X Chen. Optical multiple-image encryption based on multi-plane phase retrieval and interference[J]. Journal of Optics, 2011, 13(11): 115401.

33 N Rawat, B Kim, I Muniraj, *et al*.. Compressive sensing based robust multispectral double-image encryption[J]. Appl Opt,

2015, 54(7): 1782-1793.

34 E Candes, J Romberg, T Tao. Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information[J]. IEEE Transactions on Information Theory, 2006, 52(2): 489-509.

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

36 Y Rivenson, A Stern, B Javidi. Overview of compressive sensing techniques applied in holography[J]. Appl Opt, 2013, 52(1): A423-A432.

37 D Qi, S Wei. The physics of compressive sensing and the gradient-based recovery algorithms[J]. Arxiv Org, 2009: 1-7.

38 M Lustig, D Donoho, J M Pauly. Sparse MRI: The application of compressed sensing for rapid MR imaging[J]. Magnetic Resonance in Medicine, 2007, 58(6): 1182-1195.

栏目编辑：苏 岑