基于计算全息图的双重加密算法研究

韩 超 万 芮 刘 洋 王凤随

安徽工程大学电气工程学院, 安徽 芜湖 241000

摘要 为了确保现代网络信息传输的安全性问题,提出了一种基于压缩感知理论和分块Arnold变换置乱的计算全息图双重加密算法。该方法制作出原始图像的纯相位全息图,利用压缩感知的随机测量矩阵作为密钥对全息图进行初次加密,将加密后的图像通过分块Arnold变换置乱再次加密。使用密钥对经过两次加密的图像解密可重现原始图像。该全息加密方法相较于传统光学加密设计灵活、光路简单,且两次加密均具有随机性,从而大大提高了信息传输的安全性。结果表明,解密恢复的图像质量理想、安全性高、稳健性强。通过搭建基于硅基液晶空间光调制器的全息显示系统对提出的加密方法进行了实验验证。

关键词 全息; 图像加密; 计算全息; 压缩感知; Arnold变换; 空间光调制器

中图分类号 O438 **文献标识码** A

doi: 10.3788/CJL201542.0909001

A Double Encryption Algorithm Research Based on Computer Generated Hologram

Han Chao Wan Rui Liu Yang Wang Fengsui

School of Electrical Engineering, Anhui Polytechnic University, Wuhu, Anhui 241000, *China*

Abstract To ensure the security issues of information transmission in modern network, a double encryption algorithm of computer generated hologram based on compressed sensing theory and block Arnold transformation scrambling has been proposed. The phase-only hologram of original image has been produced, the hologram has been encrypted by using the random measurement matrix of compressed sensing as a key. It has been encrypted again by block Arnold transformation scrambling. The image after two-time encryption can be decrypted by using the keys and reproduce the original one. Compare to conventional optical holographic encryption, this method has a more flexible design, simple optical path and the two encryptions both have randomness, so it improves the security of information transmission greatly. Result shows that the decryption image is ideal, safe and robust. The proposed method is verified by building a holographic display system based on silicon liquid crystal spatial light modulator.

Key words holography; image encryption; computer generated hologram; compressed sensing; arnold transformation; spatial light modulator

OCIS codes 090.1760; 060.4785; 070.6120; 090.2870

1 引 言

随着信息技术的快速发展,信息安全问题受到越来越多的重视。如何保证图像信息的安全传输,防止图像被第三方截获、恶意篡改、非法拷贝和传播,变得极其重要,因此图像数据传输中的保密性成了近年来研究的热点[1]。目前比较成熟的图像加密技术中,基于生物特征识别的加密方法因其不变性和唯一性而被广泛应用,但在网络环境中易遭受攻击[2];量子加密具有无条件安全性和对盗取密码的可检测性而具有极强保密性,但目前仍受到传输距离的限制[3]。双随机相位编码技术、利用相移干涉技术等光学加密方法,具有

收稿日期: 2015-03-27; 收到修改稿日期: 2015-04-20

基金项目: 安徽省自然科学基金(1508085MF121)、校基金(zryy1311)

作者简介: 韩 超(1974—),男,博士,副教授,主要从事光信息处理、图像处理、全息显示等方面的研究。

E-mail: hanchaozh@126.com

高速、并行、大信息量等特点，但光路复杂，硬件要求高，且如果不做数字化处理，很难在网络上进行传输[4-5]。计算全息加密术是基于全息术原理在计算机中实现全息加密和解密的过程[6-8]，相比于传统的光学加密技术，它不再过分依赖于实验设备，整个操作过程也更加简单，因此是一种备受欢迎的加密方法。

计算全息(CGH)具有可以根据需要调整系统结构参数、可以记录自然界不存在的虚拟物体、信息量大、不可撕毁等优点[9]。本文将压缩感知理论与计算全息术相结合，不仅可以使待加密的数据量大大增加，且可利用压缩感知理论中测量矩阵的高随机性对全息图进行加密。通过提出的分块 Arnold 变换对传输信息再次加密，即可实现数据的高度安全传输。此外，为了使全息图的衍射效率更高，采用将待传输的图像制作成纯相位全息图，将该全息图作为加密对象。为了验证该方法的正确性，搭建了基于硅基液晶空间光调制器的全息显示系统对提出的方法进行了实验。

2　加密解密方案

图像加密及解密方案示意图如图 1 所示。在加密过程中，首先制作原始图像的纯相位计算全息图，在小波域将其稀疏得到稀疏系数，使用高斯随机矩阵作为测量矩阵即密钥 1，对稀疏后的数据进行压缩采样和初次加密；然后对图像进行分块 Arnold 变换置乱，置乱次数与分块位置作为密钥 2 得到最终加密图像。解密时，先使用密钥 2 进行 Arnold 逆变换，然后使用密钥 1 通过 ROMP 算法重构全息图，最终通过全息再现得到解密后的原始图像。

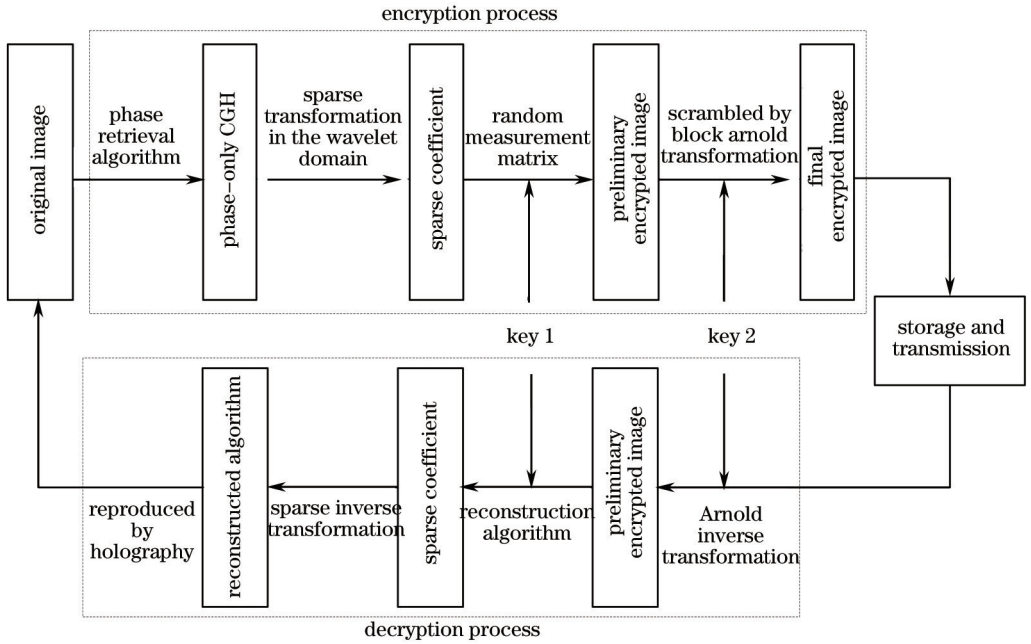

图 1　图像加密及解密方案示意图

Fig.1　Schematic of the image encryption and decryption method

3　纯相位计算全息图

一般来说，全息图的透射率函数是一个复函数，它描述照明光波通过全息图传播时振幅和相位所受到的调制[10]，通常表示为

$$t_{\mathrm{H}}(x,y)=t_0(x,y)\cdot\exp[\mathrm{j}\phi_{\mathrm{H}}(x,y)],\tag{1}$$

式中 $t_0(x,y)$ 是振幅透射函数，$\phi_{\mathrm{H}}(x,y)$ 是相应的相位信息。而当 t_0 为常数时，全息图变为纯相位全息图。由于纯相位全息图不衰减光的能量，其衍射效率一般比较高，在全息术中占有相当重要的地位。对于一般图像，直接提取相位信息会造成振幅信息的丢失，导致图像无法清晰再现，通过相位恢复算法可以解决这个问题。在已知衍射波函数的振幅和其傅里叶谱振幅的情况下，在空间域与空间频率域之间反复做交替性迭代与约束，检索需要的相位信息。本文采用迭代傅里叶变换算法[11-12]，得出原始图像的纯相位全息图，即待加

密的纯相位计算全息图。

4　压缩感知加密

由压缩感知理论[13-15]可知，对于稀疏信号或在某些正交基下展开后为稀疏的N维信号$\boldsymbol{x}$，可通过一个满足有限等距性质的测量矩阵$\boldsymbol{\Phi}$，对其进行测量，得到一个M维观测值$\boldsymbol{y}$，其中，$\boldsymbol{\Phi}$可为随机矩阵，$M \ll N$。因此可以选择具有随机性的$\boldsymbol{\Phi}$(即$\boldsymbol{\Phi}$为随机矩阵)对待加密的全息图进行随机测量，得到一个维数更小的测量值$\boldsymbol{y}$作为传输对象。由$\boldsymbol{y}$恢复出$\boldsymbol{x}$是一个病态问题，存在多个解，但由于$\boldsymbol{x}$具有稀疏性，这个问题可以通过下式求解：

$$\min\|x\|_0, \ \text{subject to} \quad \boldsymbol{y}=\boldsymbol{\Phi x}, \tag{2}$$

则问题转化为求解该最优化即l_0最优化问题，由于最l_0优化是NP问题，所以往往将(2)式的求解转化为l_1模最小化问题进行求解，得到稀疏域的系数，最后通过稀疏反变换即可以得到原始信号。本文选用贪婪算法中正则化的正交匹配算法重构原始数据，它综合了贪婪算法的快速性和凸优化方法的精确性的优点，具有一定的优越性[16]。

5　分块Arnold变换置乱加密

经过压缩感知初次加密后的图像被投影到低维空间，图像的像素数比加密前大大减少。Arnold变换要求图像为方阵，即像素数为S pixel×S pixel，而此时图像为不规则的，无法直接用Arnold变换置乱。为此提出分块Arnold变换模型来进行置乱加密。

若经过压缩感知理论加密后的全息图恰巧可以分为像素数为S pixel×S pixel的两个图像块，例如原始图像50%压缩感知采样后变为像素数为S pixel×2S pixel的图像，可将其分为两块。为了进一步增加破解加密图像的难度，随机取图像第n列至第$n+S-1$列作为一块，剩下两块拼作一块，形成如图2(a)所示的像素数均为S pixel×S pixel的A、B，然后对两幅图A、B分别进行Arnold变换置乱。此外，若想继续增加破解加密图像的难度，可将A、B再细分为若干份分别置乱，此处不再赘述。

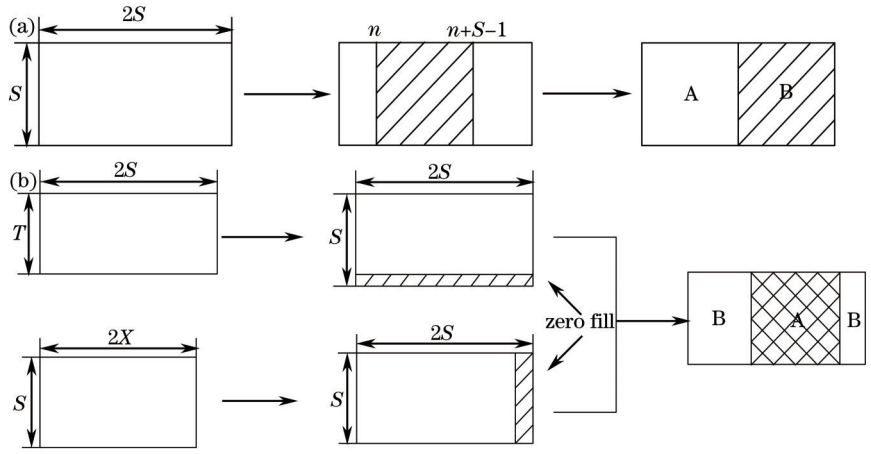

图2　分块Arnold变换置乱方法示意图

Fig.2　Schematic of block Arnold transformation scrambling method

若经过压缩感知加密后的图像不可以直接划分为方阵，则可以将它通过补零填充为列数是行数2倍的图像后，再利用上述方法分成两个方阵分别置乱。若图像像素点行数的2倍小于列数，如图2(b)所示$T<S$，则可以对不足的行数补零；若图像像素点行数的2倍大于列数，如图$S>X$，则可以对相应的列数补零，最终都可以填充为S pixel×2S pixel的图像再利用上述方法随机分块置乱。

例如对于像素数为512 pixel×512 pixel的原始图像，在45%压缩采样后变为像素数为230 pixel×512 pixel的图像如图3(a)所示，其行数的2倍小于列数，对于缺少的行补零填充为256 pixel×512 piexl的图像如图3(b)，再随机划分为256 pixel×256 pixel的两个图像块，分别进行Arnold置乱，最终得到加密图像如图3(c)所示。原始图像在55%压缩采样后变为像素数为281 pixel×512 pixel的图像如图3(d)所示，其行数的2倍大于列数，对

于缺少的列补零填充为281 pixel×562 pixel的图像如图3(e)，再随机划分为281 pixel×281 pixel的两个图像块，分别进行Arnold置乱，最终得到加密图像如图3(f)。

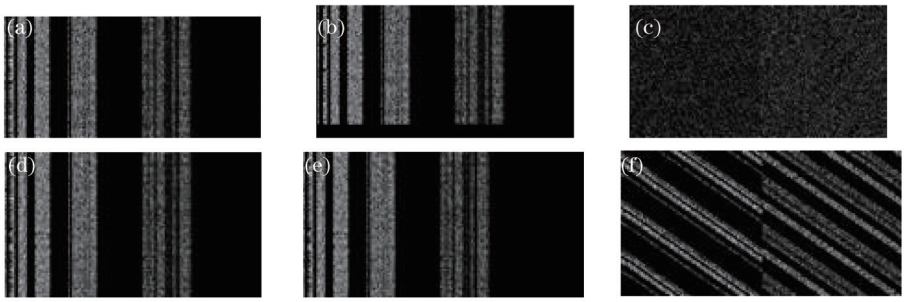

图3 (a) 45%压缩采样的图像; (b) 由(a)填充后的图像; (c) 45%压缩采样最终加密图像; (d) 55%压缩采样的图像; (e) 由(d)填充后的图像; (f) 55%压缩采样最终加密图像

Fig.3 (a) Image when the compressed sampling rate is 45%; (b) image after filling with (a); (c) final encryption image when the compressed sampling rate is 45%; (d) image when the compressed sampling rate is 55%; (e) image after filling with (d); (f) final encryption image when the compressed sampling rate is 55%

运用这种随机分块Arnold变换置乱的方法，第三方无法得知置乱的具体步骤，即使知道置乱次数，恢复的图像包含无法预测的补零信息，因此很难正确解密图像。

6　实验与仿真

6.1　计算机仿真实验

在理论分析的基础上，利用计算机进行仿真模拟，首先将如图4(a)所示像素数为512 pixel×512 pixel的原始图像，通过相位恢复算法生成纯相位计算全息图得到图4(b)，对图4(b)中的全息图压缩采样，选取合适的随机测量矩阵进行初次加密，随机测量矩阵用来作为密钥1。图4(c)为压缩采样率为50%时，经过压缩感知加密后的图像。然后对图像利用分块Arnold变换置乱，得到最终加密图像如图5(a)所示。

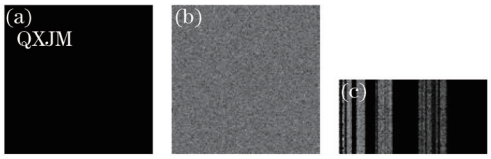

图4 (a) 原始图像; (b) 纯相位全息图; (c) 压缩感知加密的图像

Fig.4 (a) Original image; (b) phase-only hologram; (c) encrypted image using compressed sensing

在接收端，首先通过正确密钥2对图像进行Arnold逆变换，得到初步解密图像如图5(b)所示，再利用密钥1通过ROMP算法恢复得到解密的全息图如图5(c)所示，图5(d)为最终再现的原始图像。此时原始图像与解密图像的归一化互相关系数为0.9921，峰值信噪比为74.1025 dB。当密钥1错误时，重构再现的图像如图6(a)所示；密钥2错误时，再现的图像如图6(b)所示。由此可见，该方案具有较强的抗攻击能力，解密图像对密钥非常敏感，在无法确定密钥的前提下，极难破译原始图像，能够保证信息的安全传输。

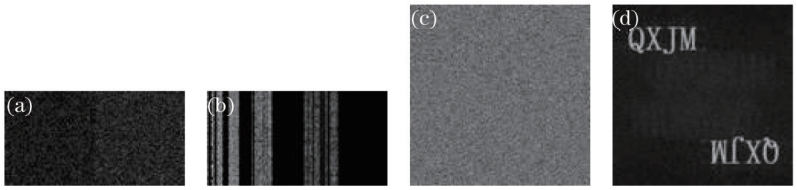

图5 (a) 50%压缩采样最终加密图像; (b) 用密钥2解密的图像; (c) 用密钥1解密的图像; (d) 最终再现图像

Fig.5 (a) Final encryption image when the compressed sampling rate is 50%; (b) decrypted image using key 2; (c) decrypted image using key 1; (d) final reconstructed image

6.2　光电重构实验

空间光调制器是一种对光波光场分布进行调制的器件，它能够对光波的相位、振幅等特性进行调制[17]，

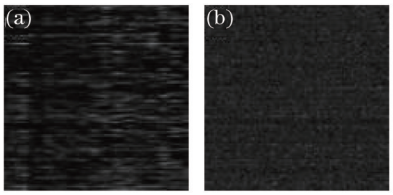

图 6 (a) 密钥 1 错误的再现图像;(b) 密钥 2 错误的再现图像

Fig.6 (a) Reconstructed image using wrong key 1; (b) reconstructed image using wrong key2

本文选用 Holoeye 公司生产的纯相位液晶空间光调制器,它具有衍射效率高、像素小、清晰度好等优点。

在理论探讨与计算机仿真模拟后,在精密光学平台上搭建了一套如图 7 所示的基于硅基液晶空间光调制器(LCOS-SLM)的全息显示系统来验证本文所提出的方法。系统主要器件包括波长为 637 nm 的红光单膜激光器,准直扩束器、透镜、分辨率为 1920 pixel×1080 pixel、像素大小为 6.4 μm、填充率约为 93% 的 LCOS-SLM 及计算机。

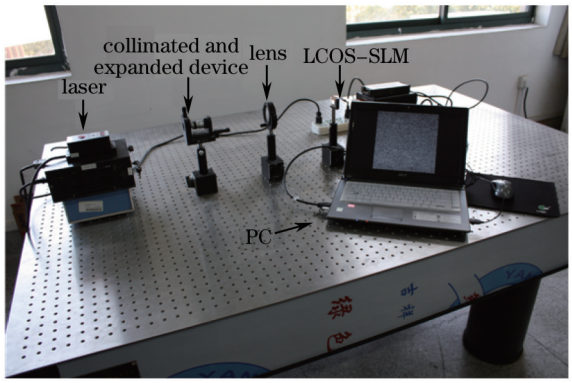

图 7　全息显示系统示意图

Fig.7　Diagram of holographic display system

将解密后的全息图通过计算机加载到空间光调制器中,此时激光器发出的光线经过准直扩束器后得到均匀的出射光束,光束经过透镜照射到 LCOS-SLM 上,经过 LCOS-SLM 调制后反射光线投射到接收屏幕上,从而重构出原始图像,见图 8。为了比较实验效果,图 8(a)为直接全息再现的图像,图 8(b)为经过双重加密后解密再现的图像。由拍摄的图片可以看出,经过压缩感知加密后再现的图像清晰可靠,由此得知此加密方案是可行的。

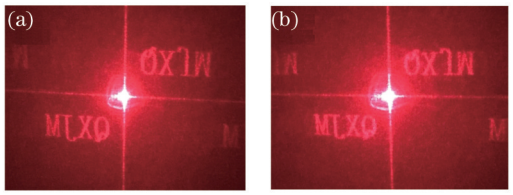

图 8　(a)全息再现的图像;(b)解密后的再现图像

Fig.8　(a) Reproduced image; (b) reproduced image after decryption

7　结　　论

在运用了压缩感知理论和分块 Arnold 变换方法的基础上,提出了一种新型的计算全息图像加密方法。该方法能够在确保信息安全的前提下清晰显示解密图像,光路简单,不需要变换透镜和随机相位板。使用压缩感知理论结合分块 Arnold 置乱方法,使得两次加密都具有随机性,大大增加了破解图像的难度,同时减少了待加密信息的数据量,有利于加密全息图的存储与传输。通过计算机模拟和搭建以 LCOS 为核心的全息显示系统对所提出的方法做出验证,结果表明,此方法具有很好的加密效果。

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]. 计算机工程与应用, 2012, 34(5): 1-6.

2 Wang Desong. Research on Information Hiding and Authentication Based on Biometrics and Its Application[D]. Chengdu: University of Electronic Science and Technology of China, 2012: 4-8.
王德松. 基于生物特征信息隐藏与身份认证及其应用研究[D]. 成都: 电子科技大学, 2012: 4-8.

3 Meng Ying, Wei Xiaoma, Wang Lei, *et al*.. The physical basis and theoretical system on the quantum cryptography[J]. Practical Electronics, 2014, (19): 192.
孟　颖, 魏晓马, 汪　磊, 等. 量子加密技术的物理基础和理论体系[J]. 电子制作, 2014, (19): 192.

4 Chen Yixiang, Wang Xiaogang. Image encryption based on iterative amplitude-phase retrieval and nonlinear double random phase encoding[J]. Acta Optica Sinica, 2014, 34(8): 0810003.
陈翼翔, 汪小刚. 一种基于迭代振幅-相位恢复算法和非线性双随机相位编码的图像加密方法[J]. 光学学报, 2014, 34(8): 0810003.

5 Meng Xiangfeng. Study of Optical Information Security Techniques Based on Iterative Phase Retrieval Algorithm and Phase-Shifting Interferometry[D]. Jinan: Shandong University, 2008: 10-23.
孟祥锋. 基于迭代相位恢复算法和相移干涉术的光学信息安全技术的研究[D]. 济南: 山东大学, 2008: 10-23.

6 Liu Jian. Study on Encryption with Computer Generated Hologram[D]. Jinhua: Zhejiang Normal University, 2013: 14-41.
刘　健. 计算全息加密技术的研究[D]. 金华: 浙江师范大学, 2013: 14-41.

7 Kong Dezhao, Zhao Yan, Cao Liangcai, *et al*.. Three-dimensional object encryption and reconstruction based on computer generated hologram[C]. International Workshop on Holography and Related Technologies, 2014: 84-85.

8 Kong Dezhao, Shen Xueju, Shen Yaqin, *et al*.. Multi-image encryption based on interference of computer generated hologram[J]. Optik, 2014, 125(10): 2365-2368.

9 Zhang Yaping, Zhang Jianqiang, Chen wei, *et al*.. Fast computer generated hologram algorithm of triangle mesh models[J]. Chinese J Lasers, 2013, 40(7): 0709001.
张亚萍, 张建强, 陈　伟, 等. 基于三角模型的计算全息快速算法[J]. 中国激光, 2013, 40(7): 0709001.

10 Liu Kaifeng, Shen Chuan, Zhang Cheng, *et al*.. Iterative feedback algorithm for phase-only Fresnel hologram and display using liquid crystal on silicon[J]. Acta Photonica Sinaca, 2013, 43(5): 0509003.
刘凯峰, 沈　川, 张　成, 等. 纯相位菲涅尔全息图的反馈迭代算法及其硅基液晶显示[J]. 光子学报, 2013, 43(5): 0509003.

11 Tsang P W M, Poon T C. Novel method for converting digital Fresnel hologram to phase-only hologram based on bidirectional error diffusion[J]. Opt Express, 2013, 21(20): 680-685.

12 Wang Haiyan. Study on Phase Retrieval Algorithm and Its Application[D]. Hefei: Anhui University, 2011: 1-31.
王海燕. 相位恢复算法及应用研究[D]. 合肥: 安徽大学, 2011: 1-31.

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

14 Han Chao, Wu Wei, Li Mengmeng. Encoding and reconstruction of lensless off-axis Fourier hologram based on the theory of compressed sensing[J]. Chinese J Lasers, 2014, 41(2): 0209015.
韩　超, 吴　伟, 李蒙蒙. 基于压缩感知理论的无透镜离轴傅里叶全息编码与重建[J]. 中国激光, 2014, 41(2): 0209015.

15 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.

16 Yang Hairong, Zhang Cheng, Mo Wei, *et al*.. The theory of compressed sensing and reconstruction algorithm[J]. Acta Electronica Sinica, 2011, 39(1): 142-148.
杨海蓉, 张　成, 末　为, 等. 压缩传感理论与重构算法[J]. 电子学报, 2011, 39(1): 142-148.

17 Dai Haitao. Characteristics of LCOS Phase-Only Spatial Light Modulator and Its Applications[D]. Shanghai: Fudan University, 2005: 3-82.
戴海涛. LCOS相位空间光调制器的特性及其应用研究[D]. 上海: 复旦大学, 2005: 3-82.

栏目编辑: 何卓铭