基于干涉原理的虚拟光学加密系统

秦 怡 张 帅 巩 琼 李根全 吕晓东*
(南阳师范学院物理与电子工程学院, 河南 南阳 473061)

摘要 提出了一种虚拟光学加密系统。该光学加密系统采用了同轴全息技术的基本架构,将被加密图像作为被记录物体,而在参考光波及干涉场光路中分别引入两个独立的随机相位板,全息面上的输出即为加密结果,这两个随机相位板即为加密及解密所用密钥。理论分析表明,在恰当设置物光波与参考光波衍射场比例的情况下,任意一灰度图像均可被加密为平稳的复随机白噪声,可以抵御盲反卷积攻击。采用计算机模拟,证实了该系统的加密效果及对抗暴力攻击的能力。研究了解密时附加参数及噪音攻击对解密结果的影响,结果表明本系统抗噪音攻击能力一般,但对附加参数有极高的敏感性。

关键词 傅里叶光学;图像加密;干涉原理;虚拟光学系统;盲反卷积
中图分类号 TP751 **文献标识码** A **doi**: 10.3788/AOS201232.1007001

Virtual Optical Image Encryption Based on Interference

Qin Yi Zhang Shuai Gong Qiong Li Genquan Lü Xiaodong
(*College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang, Henan* 473061, *China*)

Abstract A virtual optical encryption system is proposed. The system adopts the basic structure of in-line digital holography and the original image is taken as the object to be recorded. Two dependent random phase masks, which act as the encryption and decryption keys, are employed in both the reference light path and the interference field. The complex field in the hologram plane is the encryption result. The statistical properties of this technique is analyzed. It is shown that the encoding converts the input signal to stationary white noise if the scale coefficient is properly selected. Computer simulations prove the encryption effects and its robustness against brute-force attacks. The influence of noise and additional parameters on the decryption results is studied. The encryption system is not so robust to noise attack, but it is highly sensitive to additional parameters.

Key words Fourier optics; image encryption; principle of interference; virtue optical system; blind deconvolution
OCIS codes 070.4560; 070.7345; 070.2025

1 引 言

近年来,基于光学理论与方法的数据加密系统引起研究者的兴趣和关注,成为目前信息安全领域内研究的热点之一[1~12]。1995 年,Refregier 等[13]提出了双随机相位编码光学加密系统。该系统被提出后,其加密特性以及由其衍生出来的光学加密系统得到广泛研究。例如,彭翔等[14~16]针对该系统的安全性能问题进行了深入的分析,指出了该系统对于已知明文攻击、唯密文攻击和选择性明文攻击的脆弱性,Unnikrishnan 等[17,18]则分别将该方法推广到分数傅里叶域及菲涅耳域,实现了更为简单的加密结构。He 等[19]还将此技术与数字全息术结合起来对光学图像进行加密,取得了较好的效果。特别是近几年来,光学加密研究朝着结构更简单、性能更安全的方向发展,国内的学者在此领域取得了一系列重要的成果。例如,Qin 等[6]设计出一种非对称

收稿日期: 2012-04-19; **收到修改稿日期**: 2012-05-18
基金项目: 河南省科技厅科技攻关项目(112102210386)、南阳师范学院高层次人才启动资金(nytc2006k100)和南阳师范学院青年项目基金(QN2012052,QN2012053)资助课题。
作者简介: 秦 怡(1981—),男,硕士,讲师,主要从事光电信息处理方面的研究。E-mail: 27191249@qq.com
* **通信联系人**。E-mail: 641858757@qq.com

密钥加密系统，使得加密和解密信息时采用的密钥完全不同，因而解决了双随机相位加密系统因内在的线性而存在的安全隐患，极大地提高了光学加密系统的安全性；Zhang 等[9]提出基于干涉原理的加密方法，将图像隐藏于两个独立的纯随机相位板中，引出了一个光学加密领域的新方向。

本文提出一种虚拟光学加密系统，该系统采用同轴全息干涉的基本架构，将被加密图像作为全息记录物体，并在参考光以及干涉场中分别引入两个独立的随机相位板作为密钥。研究了该系统的统计学性质，指出该系统可以将图像编码成平稳随机白噪声，可以抵抗任何暴力攻击。使用计算机模拟验证了系统的性能。结果显示，任何一个密钥错误都将导致解密失败。解密过程对系统的附加参数特别敏感，因而极大地提升了系统的密钥空间。

2　理论分析

2.1　离散菲涅耳变换

根据傅里叶光学的理论可知，在菲涅耳近似下，用相干光照明位于 x_o-y_o 平面上的物体 $u(x_o,y_o)$，经过距离 d 衍射后，在 $\xi-\eta$ 平面上的复振幅分布 $U(\eta,\xi)$ 可表示为

$$U(\eta,\xi)=\iint_{x_o,y_o} u(x_o,y_o)h(\eta-x_o,\xi-y_o)\mathrm{d}x_o\mathrm{d}y_o, \tag{1}$$

式中 $h(x,y)$ 为自由空间衍射过程的脉冲响应函数，可表示为

$$h(x,y)=\frac{\exp(\mathrm{i}2\pi d/\lambda)}{\mathrm{i}\lambda d}\exp[\mathrm{i}\pi(x^2+y^2)/\lambda d], \tag{2}$$

式中 i 为虚数单位，λ 为相干照明所用的光波波长。在虚拟光学系统里面，所有被处理的对象均为计算机产生的数字对象。假设 $u(x_o,y_o)$ 被离散化为 $N\times N$ 的矩阵，那么其对应的衍射场由离散菲涅耳变换给出：

$$U(\eta,\xi)=\mathrm{DFD}[u(x_o,y_o);\lambda,d]=\sum_{\eta=0}^{N-1}\sum_{\xi=0}^{N-1}u(x_o,y_o)h(\eta-x_o,\xi-y_o), \tag{3}$$

其中 DFD 表示离散菲涅耳变换。

2.2　新型光学加密系统原理

所提出的虚拟光学加密系统如图 1 所示。被加密的图像 $f(x_o,y_o)$ 和随机相位板 RPM1 被单色平面波照射，并分别经过距离 d_o 和 d_r 的菲涅耳衍射后于平面 H 上叠加形成干涉场。之后，此干涉场被第二个随机相位板 RPM2 所调制，经过距离为 d_e 的菲涅耳衍射后在输出平面形成加密的密文 $U_E(x_e,y_e)$。假设所采用的单色平面光波的波长为 λ，两个随机相位板 RPM1 和 RPM2 的表达式分别为 $\exp[\mathrm{i}2\pi n(x_r,y_r)]$ 与 $\exp[\mathrm{i}2\pi b(\eta,\xi)]$，要求 $n(x_r,y_r)$ 和 $b(\eta,\xi)$ 为在 $[0,1]$ 上均匀分布的白噪声，且相互独立。(x_r,y_r)，(η,ξ) 以及 (x_e,y_e) 分别为各自所在平面的坐标。H 代表位于随机相位板 RPM2 前并与之紧贴的平面。因此，在 H 平面的复振幅分布为原始图像 $f(x_o,y_o)$ 与随机相位板 RPM1 分别经距离 d_o 和 d_r 后的复振幅的叠加，可以表示为

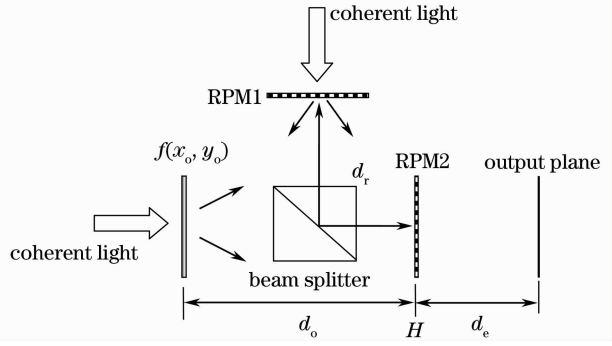

图 1　加密系统的结构框图

Fig. 1　Scheme of the proposed system

$$U_H(\eta,\xi)=\mathrm{DFD}[f(x_o,y_o);\lambda,d_o]+\mathrm{DFD}\{\exp[\mathrm{i}2\pi n(x_r,y_r)];\lambda,d_r\}, \tag{4}$$

因此可以认为 $U_H(\xi,\eta)$ 是一幅特殊的全息图。由于采用的是虚拟系统，因此可以在(4)式的基础上引入调节系数 κ，从而调节全息图中 $f(x_o,y_o)$ 的衍射场及随机相位板 RPM1 的衍射场所占的比例大小，即

$$U_H(\eta,\xi)=\kappa\mathrm{DFD}[f(x_o,y_o);\lambda,d_o]+\mathrm{DFD}\{\exp[\mathrm{i}2\pi n(x_r,y_r)];\lambda,d_r\}. \tag{5}$$

在加密过程中，选取适当的调节系数 κ，使得

$$\frac{\kappa\left|\mathrm{DFD}[f(x_o,y_o);\lambda,d_o]\right|}{\left|\mathrm{DFD}\{\exp[\mathrm{i}2\pi n(x_r,y_r)];\lambda,d_r\}\right|}\ll 1. \tag{6}$$

在研究 $U_H(\eta,\xi)$ 的统计性质时，若能满足(6)式，(5)式右边的第一项可以忽略不计。因此有

$$U_H(\eta,\xi)\approx\mathrm{DFD}\{\exp[\mathrm{i}2\pi n(x_r,y_r)];\lambda,d_r\}. \tag{7}$$

(7)式表明，平面 H 上的干涉场的复振幅分布由随机相位板 RPM1 的衍射光场所决定。在这种情况下，可以证明

$$E[U_H^*(\eta,\xi)U_H(\eta+\tau,\xi+\beta)]=\frac{1}{\lambda d}\delta(\tau,\beta), \tag{8}$$

式中 τ,β 为 H 平面坐标增量，算符 E 为求数学期望，$*$ 为求共轭操作，$\delta(\tau,\beta)$ 为克罗内克函数。(8)式表明，$U_H(\eta,\xi)$ 为平稳白噪声。尽管如此，由于 $U_H(\eta,\xi)$ 本质上是一个典型的全息图，只是被加密图像经菲

涅耳变换后与参考光的简单叠加，安全性能不高，所以，$U_H(\eta,\xi)$ 需要进一步编码加密成平稳的白噪声来提高其安全性能。因此，在平面 H 上引入第二个随机相位板 RPM2。经过 RPM2 调制并经过距离 d_e 的衍射之后，在输出平面上得到加密后的密文 $U_E(x_e,y_e)$，表示为

$$U_E(x_e,y_e)=\mathrm{DFD}\{\exp[\mathrm{i}2\pi b(\eta,\xi)]U_H(\eta,\xi);\lambda,d_e\}. \tag{9}$$

同样不难证明，$U_E(x_e,y_e)$ 的自相关函数为

$$\mathrm{E}[U_E^*(x_e,y_e)U_E^*(x_e+p,y_e+q)]=\left[\frac{1}{\lambda d}\sum_{\eta=0}^{N-1}\sum_{\xi=0}^{N-1}|U_H(\eta,\xi)|^2\right]\delta(p,q). \tag{10}$$

式中 p,q 为输出平面上的坐标增量。(10)式意味着密文 $U_E(x_e,y_e)$ 的自相关函数为克罗内克 δ 函数，即其为平稳的二维白噪声。在这种情况下，作为密钥的随机振幅板及随机相位板分辨率很高，因而密钥空间很大，在不知道振幅分布的情况下，很难通过盲反卷积运算恢复图像，具有较高的安全性。此外，由加密过程可以看出，加密中利用干涉形成全息场，再对全息场进行进一步的编码，破坏了系统加密的线性过程，因此对于常见的攻击方法，例如选择性明文攻击、唯密文攻击以及已知明文攻击等具有很强的稳健性。此外，由于引入了一些附加的参数，例如照明光波波长 λ，衍射距离 d_e，d_o，d_r 等参数，也极大地拓展了密钥空间，提高了系统的安全性能。

2.3　解密过程

解密方法是加密方法的逆过程，大致分为三个步骤：

1) 对密文 $U_E(x_e,y_e)$ 经过衍射距离 d_e 逆衍射到平面 H，然后乘以密钥 RPM2 的复共轭，$\exp[-\mathrm{i}2\pi b(\eta,\xi)]$，得到干涉场 $U_H(\eta,\xi)$；

2) 将 $U_H(\eta,\xi)$ 减去密钥 RPM1 在平面 H 上的衍射场，就得到被加密图像 $f(x_o,y_o)$ 的衍射场；

3) 将 $f(x_o,y_o)$ 的衍射场进行距离为 d_o 的逆衍射，即得到了恢复的图像 $f(x_o,y_o)$。

事实上，正是因为本方法是采用计算机虚拟的光学系统，解密过程的步骤 2)才得以进行。一般来说，在实际的同轴数字全息中，需要用相移法才能够获得物光波的衍射场[20]。

3　计算机模拟

为了验证所提方法的有效性，在 PC 机上使用 Matlab 7.0 软件进行了实验。用来进行加密的是一幅灰度图“nynu”(256 pixel×256 pixel×8 bit)，在图 2(a)中给出。在模拟中，所使用单色光波的波长 $\lambda=632.8$ nm，被加密的图像和随机相位板至平面 H 的距离均为 $d_o=d_r=100$ mm，$d_e=50$ mm，比例系数 $\kappa=0.01$。用提出的虚拟光学系统进行加密。图 2(b)和(c)是加密后图像的实部和虚部，可以看出，加密后的图像与原始图像无任何相关性，为白噪声信号。图 2(d)为加密后图像的自相关函数，为克罗内克 δ 函数，证实了前文的分析。

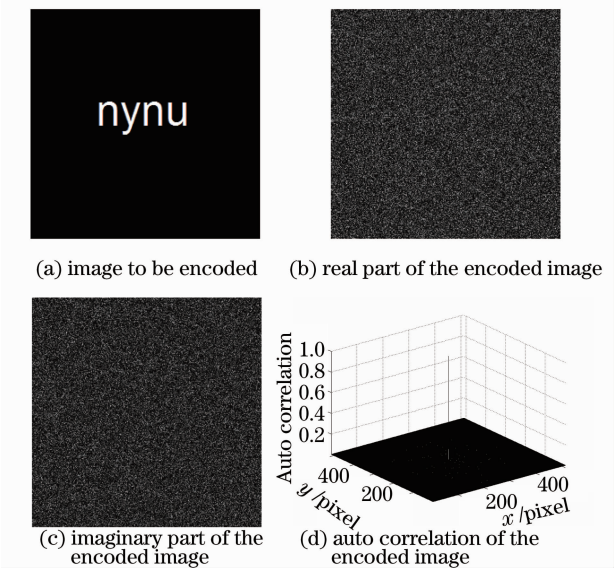

图 2　所提加密系统的加密结果

Fig. 2　Encoded images by the proposed system

在对密码系统进行密码分析时，通常认为攻击者已经知晓密码算法的工作过程，即满足 Kerekboffs 假设[21]。图 3(a)给出了在密文被截获并且已知除密钥之外所有其他参数的情况下，攻击者使用随机选取的错误的密钥得到的解密结果，可见这种解密结果与原始明文无任何相关性。图 3(b)和(c)给出了解密过程中 RPM1，RPM2 其中之一错误的解密结果，均为噪声信号。这说明即使在其他参数正确的情况下，只要两个密钥中的一个错误，均不能得到原始图像的任何信息。图 3(d)给出了使用正确密钥得到的解密结果，恢复出来的原始明文与真正的原始明文完全一致，同时证实了本方法的无损性。

为了研究附加参数对图像解密结果的影响，采用相关系数 C_C 来描述恢复出来的图像 f_{rec} 与原始图像 f 之间的符合程度。相关系数被定义为[22]

$$\rho=\frac{E\{[f-E(f)][|f_{rec}|-E(|f_{rec}|)]\}}{\{E\{[f-E(f)]^2\}E\{[|f_{rec}|-E(|f_{rec}|)]^2\}\}^{1/2}}, \tag{11}$$

这里省略了函数坐标。采用 $\Delta\lambda$ 表示恢复图像所使

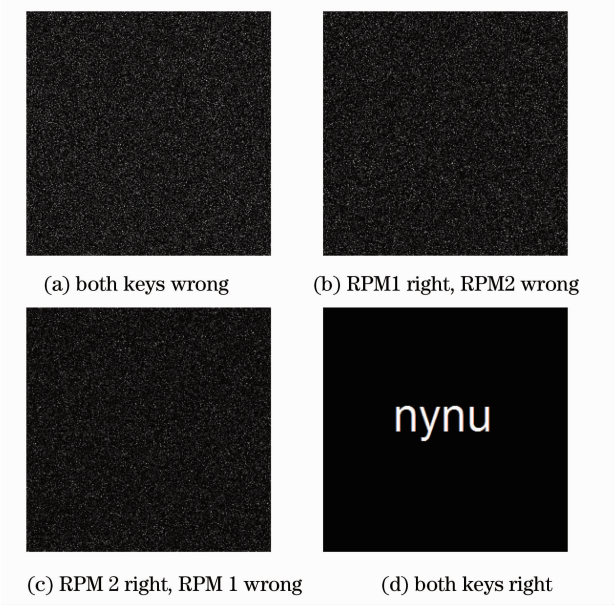

图 3　使用不同密钥得到的解密图像

Fig. 3　Decrypted image with different keys

用波长与实际波长之间的偏差，计算了 $\Delta\lambda$ 由 -0.5 μm变化到 0.5 μm 时其与 C_C 的关系，如图 4 所示。可以看出，在波长偏差不到1 μm时，C_C 即迅速下降至零附近，这说明本加密算法对波长相当敏感。图 5 则给出了 $\Delta\lambda=0.1,0.3,0.5,1$ μm 时的解密图像及 C_C 值。如图 5 所示，当波长偏差为 0.5 μm 的时候重建图像即已经与原始图像失去相关性，字符变得几乎不可辨识。

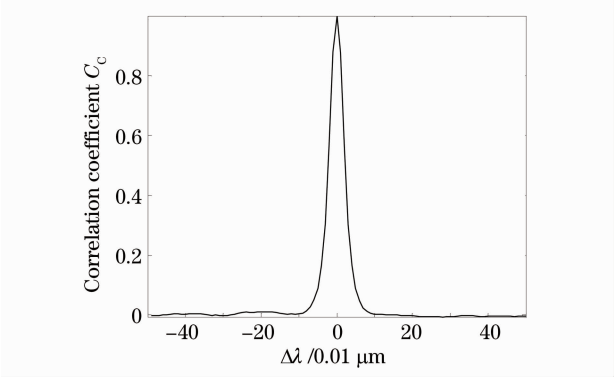

图 4　解密时波长偏差 $\Delta\lambda$ 与图像相关系数之间的关系

Fig. 4　Dependence of correlation coefficient on $\Delta\lambda$

采用类似的方法，研究了在解密过程第 1 步中重建距离与实际距离之间偏差 Δd_e 与 C_C 之间的函数关系，Δd_e 的变化范围为 $-100\sim100$ μm，变化间隔为 1 μm。结果如图 6 所示，当距离偏差 $\Delta d_e=1$ μm时，C_C 已经下降至零附近，显示出本加密系统对参数 Δd_e 同样非常敏感。图 7 给出了 $\Delta d_e=10,1,0.1,0.01$ μm 时的解密图像及 C_C。由图 7(c)可以

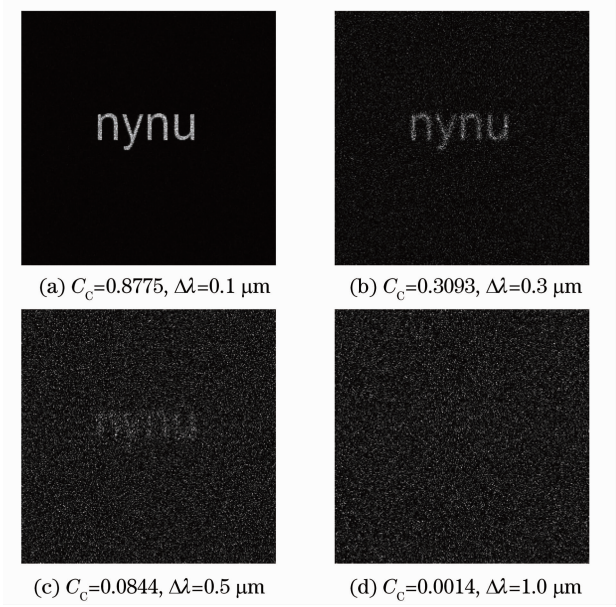

图 5　$\Delta\lambda$ 取不同数值时解密得到的图像

Fig. 5　Retrieved images with different $\Delta\lambda$

看出，当 $\Delta d_e=0.1$ μm 时，才能分辨出来与原始图像有关的部分信息，这说明本算法对重建距离的敏感度小于 1 μm。因而该系统拥有巨大的密钥空间，进一步证实了该系统的安全性能较高。

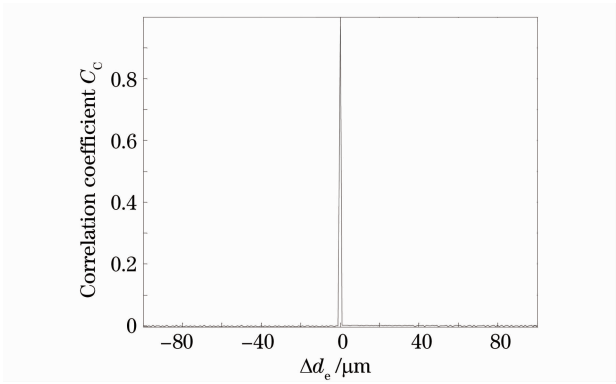

图 6　解密时重建距离偏差 Δd_e 与图像相关系数之间的关系

Fig. 6　Dependence of correlation coefficient on Δd_e

研究了该加密方法对噪音攻击的稳健性。在密文中加入分布于[0，0.01]的白噪音，该白噪音如图 8(a)所示，相应的重构的原始图像如图 8(b)所示，此时 $C_C=0.5287$。可以看出，在这种较弱的噪音攻击下，恢复得到的图像包含原始图像的足够信息。图 8(c)和(d)给出了密文中加入分布于[0，0.1]的白噪音的解密结果，此时 $C_C=0.0030$。可见，此时已经得不到原始图像的任何信息。相比于文献[13]来说，本方法抗噪音能力一般，其原因在于比例系数 κ 的引入，导致原始图像在最终输出加密数据

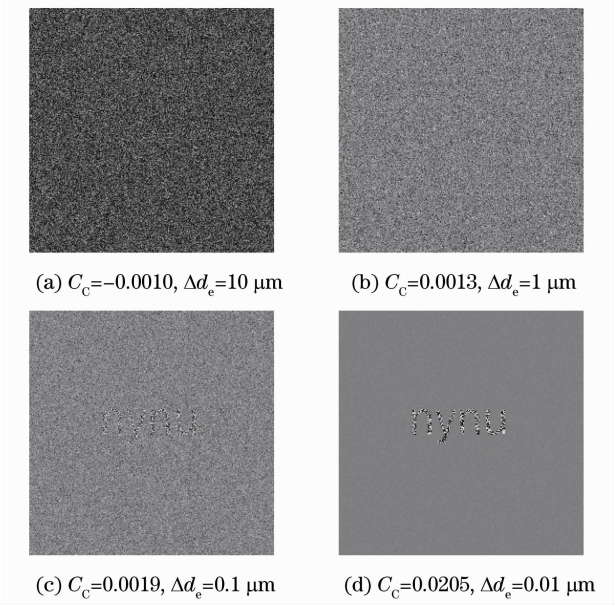

图 7　Δd_e 取不同数值时解密得到的图像

Fig. 7　Retrieved images with different Δd_e

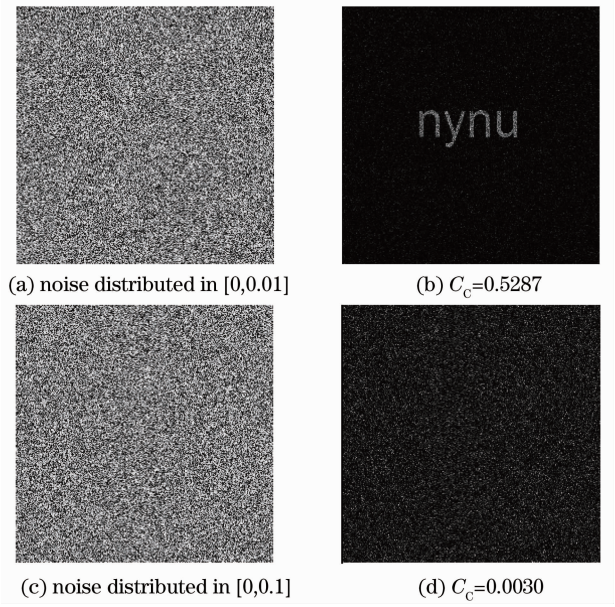

图 8　加性噪音存在时解密得到的图像

Fig. 8　Decoded images with additive noise

中占有的比例过小，因此应该合理选择 κ 的取值。

4　结　　论

从理论和实验两方面研究了所提出的虚拟光学加密系统。使用统计学理论证实了该方法与双随机相位加密系统具有相同的加密效果，可以把实值图像或者复矩阵加密成平稳的复随机白噪声。在不知密钥的情况下，不能通过暴力攻击的方法破解系统。该系统相比其他加密方法有一些明显的优点，即由于引入了全息比例系数，压缩了全息场中物光波的成分，破坏了明文和密文之间的线性关系，极大地增强了系统抵抗攻击的能力。该系统同样破坏了传统光学加密的线性关系，使得其对于唯密文攻击、选择性明文攻击以及已知明文攻击具有免疫性。

参　考　文　献

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

2 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

3 Chen Daqing, Zhou Hao, Tao Zhi *et al*.. Fourier computer-generated hologram digital watermarking with nonlinear amplitude limiting[J]. *Acta Optica Sinica*, 2011, **31**(2): 0207002
陈大庆，周　皓，陶　智 等. 非线性限幅傅里叶计算全息的数字水印方法[J]. 光学学报，2011，**31**(2)：0207002

4 Chen Yan, Yang Hongyu, Deng Ke. Effects of photon-number-splitting attacks on the security of satellite-to-ground quantum key distribution systems[J]. *Acta Optica Sinica*, 2009, **29**(11): 2889～2993
陈　彦，杨红宇，邓　科. 光子数分束攻击对星地量子密钥分配系统安全的影响[J]. 光学学报，2009，**29**(11)：2889～2993

5 Bo Wang, Yan Zhang. Double images hiding based on optical interference[J]. *Opt. Commun.*, 2009, **282**(17): 3439～3443

6 Wan Qin, Xiang Peng. Asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. *Opt. Lett.*, 2010, **35**(2): 118～120

7 Xiaogang Wang, Daomu Zhao. Security enhancement of a phase-truncation based image encryption algorithm[J]. *Appl. Opt.*, 2011, **50**(36): 6645～6651

8 Xiaogang Wang, Daomu Zhao. Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain[J]. *Opt. Commun.*, 2011, **284**(1): 148～152

9 Yan Zhang, Bo Wang. Optical image encryption based on interference[J]. *Opt. Lett.*, 2008, **33**(21): 2443～2445

10 Yujing Han, Yunhai Zhang. Optical image encryption based on two beams′ interference[J]. *Opt. Commun.*, 2010, **283**(9): 1690～1692

11 C. Niu, X. Wang, X. Mao. Multiple-image hiding based on interference principle[J]. *Opt. Quant. Electronum.*, 2012, **43**: 91～99

12 Wen Chen, Xudong Chen, Colin J. R. Sheppard. Optical image encryption based on diffractive imaging[J]. *Opt. Lett.*, 2010, **35**(22): 3817～3819

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

14 Peng Xiang, Tang Hongqiao, Tian Jindong. Ciphertext-only attack on double random phase encoding optical encryption system [J]. *Acta Physica Sinica*, 2007, **56**(5): 2629～2635
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)：2629～2635

15 Peng Xiang, Zhang Peng, Wei Hengzheng *et al*.. Known-plaintext attack on double phase encoding encryption technique [J]. *Acta Physica Sinica*, 2006, **55**(3): 1130～1135
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)：1130～1135

16 Peng Xiang, Zhang Peng, Wei Hengzheng *et al*.. Known-

plaintext attack on optical encryption based on double random phase keys[J]. *Opt. Lett.*, 2006, **31**(8): 1044～1046

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 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

20 I. Yamaguchi, T. Zhang. Phase-shifting digital holography[J]. *Opt. Lett.*, 1997, **22**(16): 1268～1270

21 Feng Dengguo. Cryptography Analysis[M]. Beijing: Tsinghua University Press, 2000. 50～51
冯登国. 密码分析学[M]. 北京: 清华大学出版社, 2000. 50～51

22 H. Hwang, H. T. Chang, W. Lie. Fast double-phase retrieval in Fresnel domain using modified Gerchberg-Saxton algorithm for lensless optical security systems [J]. *Opt. Express*, 2009, **17**(16): 13700～13710

栏目编辑: 韩 峰