基于柱面衍射和彩色空间转换的单通道彩色图像加密

常柯明,陈 叶,王 莹,王 君

(四川大学 电子信息学院,四川 成都 610065)

摘 要:为了解决传统密码系统由于对称特性导致的安全性低的问题,提出了一种新的基于柱面衍射和彩色空间转换的单通道彩色图像加密方法。在加密过程中,首先将彩色图像变换为 YCbCr4:2:0 格式的单通道图像,然后经过两次柱面衍射和相位截断操作对图像进行加密。在解密过程中,将密钥与密文结合,经过两次柱面逆衍射后重建出彩色原图。由于柱面衍射过程是一个非对称的过程,此算法可以克服基于平面衍射的加密系统的对称特性,将其应用到基于相位截断的加密系统中可以进一步有效提高加密系统的安全性。仿真结果表明,该算法能够有效地对彩色图像进行单通道加密,不仅可以高质量地恢复原始彩色图像,而且加密系统具有较高的安全性。

关键词:信息光学; 彩色图像加密; 柱面衍射; 非对称加密

中图分类号:O438 **文献标志码**:A **DOI**:10.3788/IRLA201847.0603003

Single-channel color image encryption using cylindrical diffraction and color space converting

Chang Keming, Chen Ye, Wang Ying, Wang Jun

(School of Electronics and Information Engineering, Sichuan University, Chengdu 610065, China)

Abstract: In order to solve the problem of vulnerable to attacks caused by symmetry in traditional cryptographic systems, a new single-channel color image encryption using detour cylindrical diffraction and color space conversion algorithm was proposed in this paper. In the process of encryption, firstly, the color image was transformed into a single channel image in YCbCr4:2:0 format, then the image was encrypted by twice cylindrical diffraction and phase truncation operations. In the process of decryption, the keys were combined with the cipher text, and the color original image was reconstructed after twice inverse cylindrical diffraction. Because the cylindrical diffraction process was an asymmetric process, the proposed algorithm can overcome the symmetry characteristic of the encryption system based on plane diffraction. Applying it to the encryption system based on phase truncation can further improve the security of the encryption system. The simulation results show that the algorithm can effectively encrypt the color image with single channel, which not only can restore the original color image with high quality, but also has high security.

Key words: information optics; color image encryption; cylindrical diffraction; asymmetric encryption

收稿日期:2018-01-11; **修订日期**:2018-02-10

基金项目:国家重点研发计划(2017YFB1002900)

作者简介:常柯明(1994-),男,硕士生,主要从事光学图像加密和全息 3D 显示方面的研究。Email:372921192@qq.com

通讯作者:王君(1980-),男,副教授,博士,主要从事于全息 3D 显示、光学图像加密、GPU 并行计算方面的研究。

Email:jwang@scu.edu.cn

0 引 言

随着网络技术的快速发展，信息安全的保护变得日益重要[1]。基于光学信息处理的信息保护是数据保护，加密和认证最有前途的方法之一[2]。光学加密领域，由 Refregier 和 Javidi 率先提出的基于双随机相位编码 (Double Random Phase Encoding，DRPE)[3]的光学图像加密技术以其快速的并行处理速度、多加密维度等独特优势引起了广大学者的研究兴趣，成为最广泛使用和研究的光学加密技术之一。其中彩色图像比灰度图像包含了更丰富的信息，因此，彩色图像的加密正受到越来越多的关注[4]。传统的彩色图像加密算法有基于菲涅尔变换[5]，分数傅里叶变换[6]，gyrator 变换[7]等加密算法。

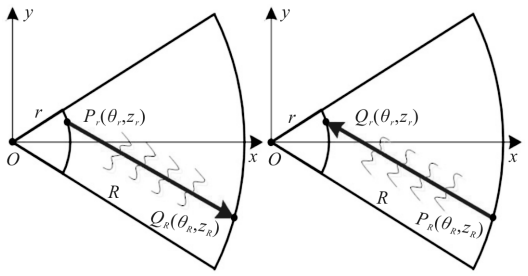
但是，上述的彩色图像加密算法都是对称的加密系统，即加密密钥和解密密钥相同，这容易受到如“已知明文攻击”，“选择明文攻击”[8-9]，“相位检索攻击”等攻击，信息的安全性得不到保证。为了解决这个问题，提出了非对称的彩色图像加密算法，如基于相位截断傅里叶变换的非对称密码体制[10]、使用随机二进制相位调制和混合相位恢复算法的非对称密码系统以及非对称相干叠加和等模分解的光学密码系统[11]。这些加密算法的解密密钥和加密密钥不同，破坏了传统 DRPE 加密系统的对称性，提高了系统的安全性。其中相位截断的非线性操作使非对称的加密系统具有很强的鲁棒性[12]。

因此，文中提出了一种新的基于柱面衍射和彩色空间转换的单通道彩色图像加密方法。在加密过程中，首先将彩色图像转换为 YCbCr4:2:0 格式的单通道图像，然后经过两次柱面衍射和相位截断操作对图像进行加密。解密过程是加密过程的反过程，通过使用正确的密钥可以重建出 YUV 图像，最后恢复出彩色原图。柱面衍射的非对称特性使得基于柱面衍射的图像加密系统可以克服基于平面衍射的加密系统的对称性。将其应用到基于相位截断的加密系统中有效地提高了加密系统的安全性。此外，柱面衍射的柱面的内外半径、高度和衍射距离可以作为加密系统的额外密钥，进一步提高系统的安全性。数值模拟结果证明了所提出的密码系统的有效性和灵活性。

1 理论分析

1.1 柱面衍射理论

在柱面衍射理论[13-15]中，物面和观察面是一对同心圆柱面，如图 1 所示，其中 r 和 R 分别表示内表面和外表面的半径。显然如图 1(a)、图 1(b)所示，根据物面的位置不同可以分为由内而外和由外而内两种传播模型。



(a) IOP 模型 (b) OIP 模型

(a) IOP model (b) OIP model

图 1 圆柱形衍射中几何关系的俯视图示意图

Fig.1 Illustration of geometrical relation in cylindrical diffraction with top-view

在由内而外传播(IOP)模型下，物体和观察点分别由圆柱坐标中的 $P_r(\theta_r,z_r)$ 和 $Q_R(\theta_R,z_R)$ 表示。而在由外而内传播(OIP)模型下，物体和观察点分别用圆柱坐标中的 $P_R(\theta_R,z_R)$ 和 $Q_r(\theta_r,z_r)$ 表示。这里，z_r 和 z_R 在 $-H/2\sim H/2$ 的范围内，其中 H 是圆柱形表面的高度。如果内表面和外表面上的分布分别由 $U_r(\theta_r,z_r)$ 和 $U_R(\theta_R,z_R)$ 表示，则其对应形式的瑞利-索末菲衍射积分公式可写为：

$$U_R(\theta_R,z_R)=C\iint_s u_r(\theta_r,z_r)\frac{\exp(ikd_{P_rQ_R})}{d_{P_rQ_R}}\mathrm{d}\theta_r\mathrm{d}z_r \tag{1}$$

$$U_r(\theta_r,z_r)=C\iint_s u_R(\theta_R,z_R)\frac{\exp(ikd_{P_RQ_r})[r-R\cos(\theta_r-\theta_R)]}{d^2_{P_RQ_r}}\times \mathrm{d}\theta_R\mathrm{d}z_R \tag{2}$$

$$d=d_{P_rQ_R}=d_{P_RQ_r}=[R^2+r^2-2Rr\cos(\theta_R-\theta_r)+(z_R-z_r)^2]^{1/2} \tag{3}$$

式中：k 表示入射光的波数；C 为任意常数；d 表示物面上 P 点和观察表面 Q 点两点之间的距离。这两个公式可以通过 FFT 算法加速[13-15]。

1.2 迂回柱面随机相位编码

将柱面衍射直接应用到随机相位编码中，单方

向的多次柱面衍射存在采样间距过大的问题。为了克服这个问题，文中提出了一种迂回柱面随机相位编码算法(DCPE)，以双随机编码为例，如图 2 所示。其中物面是半径为 R_1 的圆柱面，$CRPM_1$ 和 $CRPM_2$ 是柱面随机相位掩模，半径分别为 R_1，r。物光 $U_{R1}(\theta_{R1},z_{R1})$首先经过柱面随机相位掩模 CRPM1 的调制，之后经过距离为 d_1 的柱面衍射(OIP 模型)，生成 $U_r(\theta_r,z_r)$，再经过随机相位掩模 $CRPM_2$ 的调制和反射，之后经过距离为 d_2 的柱面衍射(OIP 模型)生成复振幅 $U_{R2}(\theta_{R2},z_{R2})$，并由 CCD 接收面接收。

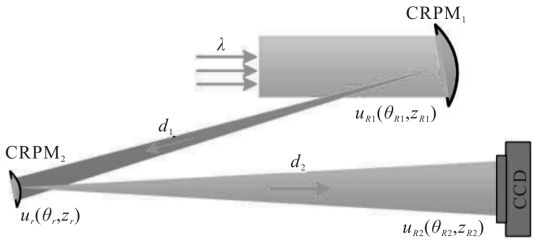


图 2 迂回圆柱衍射双随机相位编码方案

Fig.2 Scheme of double random phase encoding with detour cylindrical diffraction

1.3 加密和解密过程

文中提出的非对称密钥的加密和解密流程图如图 3 所示，在加密过程中，原始图像 I_0 被设置为半径为 R_1 的圆柱面，它首先与柱面随机相位掩模 $CRPM_1$ 调制，再经过距离为 d_1 的 OIP 模型柱面衍射后得到 U_r，即：

$$U_r(\theta_r,z_r)=\mathrm{COIP}_{\mathrm{R1},r,H,\lambda}[I_0(\theta_{R1},z_{R1})*\mathrm{CRPM}_1] \quad (4)$$

式中：(θ_{R1},z_{R1})为输入平面坐标；(θ_r,z_r)为中间平面坐标；$\mathrm{COIP}_{\mathrm{R1},r,H,\lambda}$ 表示参数为(R_1,r,H,λ)的 OIP 柱面衍射，可以由公式 (2) 计算得出。柱面随机相位掩模 CRPM1 的数学表达式为：

$$\mathrm{CRPM}_1=\exp[i2\pi\times R_{x_1,\mu_1}(\theta_{R1},z_{R1})] \quad (5)$$

式中：R_{x_1,μ_1}是由 Chaos 算法[16]生成的随机矩阵。

接下来对 U_r 进行振幅和相位截断操作得到振幅部分 I_1 和相位部分 P_1，即：

$$I_1=|U_r(\theta_r,z_r)| \quad (6)$$

$$P_1=\mathrm{Phase}[U_r(\theta_r,z_r)] \quad (7)$$

式中：Phase [·]的操作符表示获取输入的相位部分；|·|表示获取输入的振幅部分。

将截取后的相位 P_1 除以 $CRPM_2$，得到非对称的解密密钥 PK_1，即：

$$\mathrm{PK}_1=P_1/\mathrm{CRPM}_2 \quad (8)$$

振幅部分 I_1 受到柱面随机相位掩模 $CRPM_2$ 的调制，在 IOP 模型中衍射 d_2 的距离之后，得到 U_{R2}，即：

$$U_{R2}(\theta_{R2},z_{R2})=\mathrm{CIOP}_{r,\mathrm{R2},H,\lambda}\{|U_r(\theta_r,z_r)|*\mathrm{CRPM}_2\} \quad (9)$$

式中：(θ_r,z_r)为中间平面坐标；(θ_{R2},z_{R2})输出平面坐标：

$$\mathrm{CRPM}_2=\exp[i2\pi\times R_{x_2,\mu_2}(\theta_r,z_r)] \quad (10)$$

U_{R2} 经过振幅和相位截断操作后，得到振幅部分 I_2 和相位部分 P_2，即：

$$I_2(\theta_{R2},z_{R2})=|u_{R2}(\theta_{R2},z_{R2})| \quad (11)$$

$$P_2=\mathrm{Phase}[u_{R2}(\theta_{R2},z_{R2})] \quad (12)$$

振幅部分 I_2 由 CCD 相机记录作为加密密文，而相位部分 P_2 则作为另一个非对称的解密密钥 PK_2。

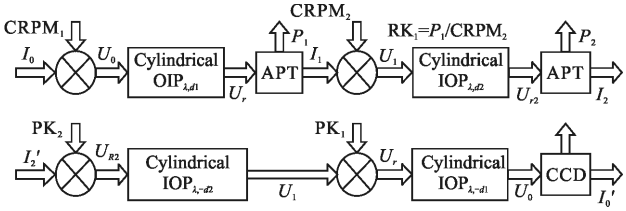


图 3 所提出密码系统的加密和解密

Fig.3 Encryption and decryption of the proposed crypto system

解密过程是加密过程的反过程，但比加密过程简单。与 $CRPM_1$ 和 $CRPM_2$ 加密密钥不同，解密密钥是 PK_1 和 PK_2，它们取决于输入图像。因此，密文可抵御已知明文和选择明文攻击。在解密过程中，第一次柱面衍射为 IOP 模型，其对应逆过程为 OIP 模型，第二次柱面衍射为 OIP 模型，其对应逆过程为 IOP 模型。根据公式(1)、(2)可以看出在不同衍射模型下对应的衍射角度不同，因此，这种密码体制是非对称的。比基于平面衍射的密码体系安全性更高。

解密过程在数学上可以抽象为：

$$I_0'(\theta_{R1},z_{R1})=|\mathrm{ICOIP}_{\mathrm{R1},r,H,\lambda}\{\mathrm{ICIOP}_{r,\mathrm{R2},H,\lambda}[I_2'(\theta_{R2},z_{R2})*\mathrm{PK}_2]*\mathrm{PK}_1\}| \quad (13)$$

式中：ICOIP 和 ICIOP 分别为 COIP 和 CIOP 的逆向计算。

1.4 彩色图像的单通道转换

YCbCr4:2:0 格式是流行的图像或视频格式，易于压缩和传输。它具有降低采样率的优点，数据量只有 RGB 格式的一半。为了降低彩色图像加密系统的复杂度，文中利用 YCbCr4:2:0 格式对彩色图像进行预处理以实现彩色图像的单通道加密。其实现方案

如图 4 所示。

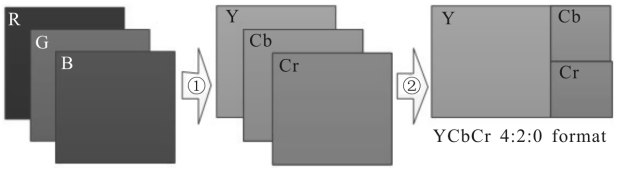


图 4 三种颜色分量的单通道方案

Fig.4 Single channel scheme for three color components

首先将彩色图像从RGB 转换为 YCbCr，即操作①，然后对 YCbCr 三分量进行下采样生成单幅复合图像即操作②。最后通过相应的上采样操作和反变换可以恢复出原始的彩色图像信息。其中 RGB 格式到 YCbCr 格式的转换操作及其反转换可以分别表示：

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \frac{1}{255} \times \begin{bmatrix} 65.481 & 128.533 & 24.966 \\ -37.797 & -74.203 & 112 \\ 112 & -93.786 & -18.214 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} + \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} \tag{14}$$

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1.164\,4 & 0 & 1.596\,0 \\ 1.164\,4 & -0.391\,8 & -0.813\,0 \\ 1.164\,4 & 2.017\,2 & 0 \end{bmatrix} \begin{bmatrix} Y-16 \\ Cb-128 \\ Cr-128 \end{bmatrix} \tag{15}$$

上下采样之间的转换可以表示为：

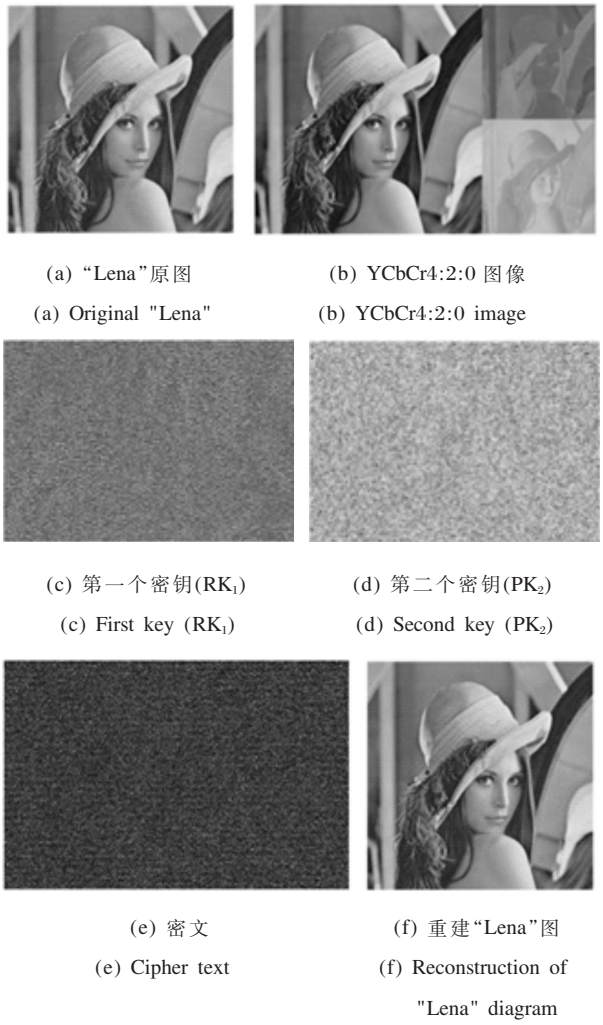
$$\begin{aligned} Ck^u(2*i-1,2*j-1)&=Ck^d(i,j) \\ Ck^u(2*i-1,2*j)&=Ck^d(i,j) \\ Ck^u(2*i,2*j-1)&=Ck^d(i,j) \\ Ck^u(2*i,2*j)&=Ck^d(i,j) \\ Ck^d(i,j)&=Ck(2*i,2*j) \end{aligned} \tag{16}$$

$$i\in[1,2,\cdots,n/2],j\in[1,2,\cdots,m/2],k\in[b,r] \tag{17}$$

式中：m 和 n 是图像的水平和垂直样本数；Ck 是格式为 YCbCr4:4:4 的全采样率下的 Cr 或 Cb 分量，Ck^d 是下采样格式 YCbCr4:2:0；Ck^u 是上采样方式恢复的全采样格式 YCbCr4:4:4。

2 仿真结果和安全性分析

通过数值模拟来验证所提出的基于柱面衍射的非对称彩色图像加密算法的可行性和安全性。采用“Lena”(512 pxiel×512 pxiel)作为输入明文图像，并使用 matlab R2010b 平台进行仿真，参数 r、R_1、R_2、H 的值分别为 10、200、210、32 mm，加密过程中所使用的波长是 288 nm。实验结果图如图 5 所示，其中图 5(e)为加密密文，从中无法看出原始图像信息。



(a) “Lena”原图 (b) YCbCr4:2:0 图像

(a) Original "Lena" (b) YCbCr4:2:0 image

(c) 第一个密钥(RK_1) (d) 第二个密钥(PK_2)

(c) First key (RK_1) (d) Second key (PK_2)

(e) 密文 (f) 重建“Lena”图

(e) Cipher text (f) Reconstruction of "Lena" diagram

图 5 基于柱面衍射和彩色空间转换的单通道彩色图像加密解密实验结果图

Fig.5 Single-channel color image encryption and decryption using cylindrical diffraction and color space converting

从解密结果中，可以清晰地看到重建的“Lena”图。为了评估重建图像的质量，文中使用相关系数(CC)值。其中 CC 值可以由下面的公式计算得出：

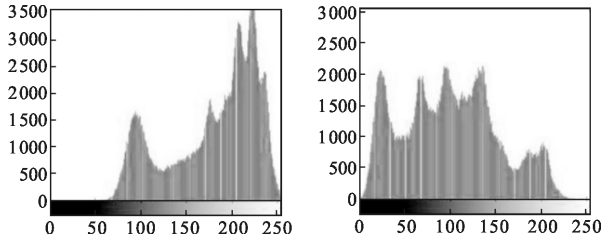
$$CC=[\mathrm{cov}(f,f')]/(\sigma_f\times\sigma_{f'}) \tag{18}$$

式中：cov 表示交叉协方差；σ 表示标准差。经仿真得到的加密图像和重建图像的 CC 值分别为 0.037 和 0.999，可以看出：上述算法具有解密图质量好，加密安全性高的优点。

2.1 统计分析

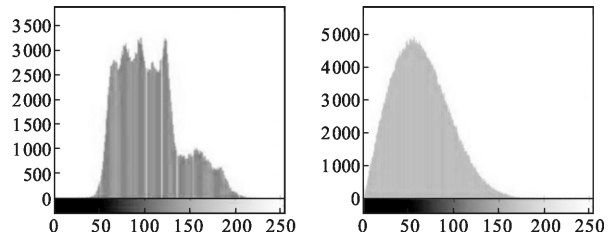
良好的加密方案，能够使不同原图像的加密图

像具有均匀的分布或者类似的灰度直方图。图 6(a)~(c)分别是彩色图像“Lena”图 R、G、B 三个分量的直方图。图 6(d)为加密密文的直方图。很明显,加密的图像直方图与原图像的直方图明显不同,呈均匀分布。



(a) R 分量的直方图 (b) G 分量的直方图

(a) Histogram of R component (b) Histogram of G component



(c) B 分量的直方图 (d) 加密图像的直方图

(c) Histogram of B component (d) Histogram of encrypted image

图 6 彩色图像“Lena”图的直方图

Fig.6 Histogram of the "Lena" graph for color images

为了使实验具有普遍性, 对不同的加密图像进行了数值仿真。图 7 (a) 为其中一幅加密图像“Fruits”, 其密文的直方图如图 7(b)所示。

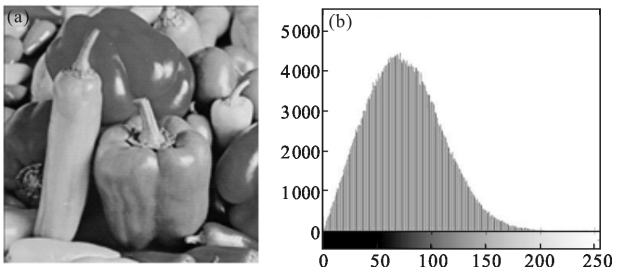


图 7 (a) 彩色图像“Fruits”和(b) 加密图像直方图

Fig.7 (a) Color image "Fruits" and (b) Encrypted image histogram

由图 6(d)和图7(b)可以看出,不同原始图像的加密图像的直方图呈相似的分布,这说明,直方图不能够给攻击者提供任何的统计线索。因此,文中提出的算法能够有效地抵抗统计攻击。

2.2 密钥空间及密钥安全性分析

一个具有高安全性的加密算法,密钥空间应该足够大,以使任何暴力攻击无效。文中所提出的加密算法的密钥包括系统参数 λ、r、H、R_2 和初始条件 μ_2、x_2。密钥的数量被扩展,并且密钥空间为 $10^{(4+4+4+4+4+10)}$。此外,一个良好的加密算法还应该对密钥敏感,以密钥 R_2 为例,对“Lena”的 R_2 分量进行密钥敏感性测试,在密钥 R_2 改变了 mm 而其他密钥不变时,加密图像的 CC 值为 0.009 4。所以可以得出所提出的方案对密钥 R_2 很敏感。表 1 显示了密钥 λ、r、H、R_2 和混沌序列初值 μ_2、x_2 在细小的改变 Δ 之后对应的解密图像的 CC 值。从表中可以看出密钥的微小变化会导致加密图像发生剧烈改变, 因此可以得出所提出的方案具备较高的密钥敏感性。

表 1 部分密钥不正确时的解密图像的 CC 值

Tab.1 CC value of the decrypted image when the partial key is incorrect

CC value of th decrypted image	Lena
$R_2=R_2\times(1+10\times10^{-4})$	0.009 4
$r=r\times(1+10\times10^{-4})$	0.045 9
$H=H\times(1+10\times10^{-4})$	$1.668\,9\times10^{-4}$
$\lambda=\lambda\times(1+10\times10^{-4})$	0.018 6
$\mu_2=\mu_2+10\times10^{-4}$	0.006 0
$x_2=x_2+10\times10^{-10}$	0.002 4

3 结 论

文中提出了一种基于柱面衍射和彩色空间转换的单通道彩色图像加密算法,明文图像可以通过两步柱面衍射和相位截断对明文进行加密,其中双随机相位掩模位于物体表面和第一个衍射面上。与传统的基于 DRPE 的加密算法相比,由于增加了两个额外的密钥,扩大了密钥空间,提高了密码系统的安全性。此外,由于两个同心圆柱面之间的衍射是非对称衍射,因此系统可以抵抗相位恢复攻击[17]。数值仿真结果证明了所提出的密码系统具有较高的安全性和好的解密图质量。而这种基于柱面衍射的 DRPE 方案可以扩展到三维物体加密和多图像加密。

参考文献：

[1] He Fengtao, Zhang Min, Bai Ke, et al. Image encryption method based on laser speckle and henon mapping [J]. ***Infrared and Laser Engineering***, 2016, 45(4): 268-272. (in Chinese)
贺锋涛, 张敏, 白可, 等. 基于激光散斑和 Henon 映射的图像加密方法[J]. 红外与激光工程, 2016, 45(4): 268-272.

[2] Javidi B, Carnicer A, Yamaguchi M, et al. Road map on optical security[J]. ***Journal of Optics***, 2016, 18(8): 083001.

[3] Javidi B, Zhang Guanshen, Li Jian. Encrypted optical memory using double-random phase encoding[C]//Lasers and Electro-Optics Society Meeting, 1996, 1997: 364-365.

[4] Yao Lili, Yuan Caojin, Qiang Junjie, et al. An asymmetric color image encryption method by using deduced gyrator transform [J]. ***Optics & Lasers in Engineering***, 2016, 89: 72-79.

[5] Hwang Hone-Ene. Optical color image encryption based on the wavelength multiplexing using cascaded phase-only masks in Fresnel transform domain [J]. ***Optics Communications***, 2012, 285(5): 567-573.

[6] Joshi M, Chandrashakher, Singh K. Color image encryption and decryption using fractional Fourier transform [J]. ***Optics Communication***, 2007, 279(1): 35-42.

[7] Chen Hang, Du Xiaoping, Liu Zhengjun, et al. Color image encryption based on the affine transform and gyrator transform[J]. ***Optics & Lasers in Engineering***, 2013, 51(6): 768-775.

[8] Fraue Y, Castro A, Naughton T J, et al. Resistance of the double random phase encryption against various attacks [J]. ***Optics Express***, 2007, 15(16): 10253-10265.

[9] Kong Dezhao, Shen Xueju, Cao Liangcai, et al. Phase retrieval for attacking fractional Fourier transform encryption [J]. ***Applied Optics***, 2017, 56(12): 3449.

[10] Wan Qin, Xiang Peng. Asymmetric cryptosystem based on phase-truncated Fourier transforms [J]. ***Optics Letters***, 2010, 35(2): 118-120.

[11] Deng Xiaopeng. Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition: comment[J]. ***Optics Letters***, 2015, 40(4): 475-478.

[12] Ding Xiangling, Cui Yongzhong. Analysis and improvement for asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. ***Laser Journal***, 2013, 34(2): 27-29. (in Chinese)
丁湘陵, 崔永忠. 基于相位截断的非对称加密系统安全性的分析与改进[J]. 激光杂志, 2013, 34(2): 27-29.

[13] Sando Y, Itoh M, Yatagai M. Fast calculation method for cylindrical computer-generated holograms[J]. ***Optics Express***, 2005, 13(5): 1418-1423.

[14] Wang Jun, Wang Qionghua, Hu Yuhen. Fast diffraction calculation of cylindrical computer generated hologram based on outside-in propagation model[J]. ***Optics Communications***, 2017, 403(22): 296-303.

[15] Liu Jungping, Poon Tingchung. Two-step-only quadrature phase-shifting digital holography[J]. ***Optics Letters***, 2009, 34 (3): 250-252.

[16] Wang Xingyuan, Zhao Jiangfeng, Liu Hongjun. A new image encryption algorithm based on chaos [J]. ***Optics Communications***, 2012, 285(5): 562-566.

[17] Wang Jun, Li Xiaowei, Hu Yuhen, et al. Phase-retrieval attack free cryptosystem based on cylindrical asymmetric diffraction and double-random phase encoding [J]. ***Optics Communications***, 2018, 410: 468-474.