基于螺旋相位变换和广义Fibonacci混沌的光学图像加密

郭 媛 许 鑫* 敬世伟 金 涛 金 梅
(齐齐哈尔大学计算机与控制工程学院 齐齐哈尔 161006)

摘 要：为了解决光学加密技术中混沌序列分布不均匀，抗选择明文攻击能力弱以及菲涅尔域双随机相位编码系统对第1个衍射距离不敏感等问题，该文基于螺旋相位变换和新型广义Fibonacci混沌系统，提出一种光学图像加密算法。在菲涅尔域的双随机相位编码中对明文图像进行相位编码和螺旋相位变换，克服系统对第1块随机模板和衍射距离不敏感的缺陷，提高光学密钥敏感性。添加安全图像与明文进行加权干涉，进一步提高光学密钥敏感性和密钥维度。构造可产生均匀混沌序列的广义Fibonacci混沌系统生成随机模板，解决密钥体积过大分发传递困难问题，克服Logistic混沌分布不均匀的缺点，提高密钥传输效率及密钥敏感性。同时用明文哈希值SHA-256生成混沌初值和螺旋相位变换参数，使得密钥流随明文自适应变化，达到“一次一密”的效果，提高算法抵抗选择明文攻击能力和明文敏感性，雪崩效应更强。实验对比表明该算法明文及密钥敏感性高，密钥空间大，鲁棒性好，能有效抵御各种攻击，是一种高安全性的光学图像加密方法。

关键词：光学图像加密；广义Fibonacci混沌；螺旋相位变换；菲涅尔变换；一次一密
中图分类号：TP309.7 **文献标识码**：A **文章编号**：1009-5896(2020)04-0988-09
DOI: 10.11999/JEIT190514

Optical Image Encryption Based on Spiral Phase Transform and Generalized Fibonacci Chaos

GUO Yuan XU Xin JING Shiwei JIN Tao JIN Mei
(*College of Computer and Control Engineering*, *Qiqihar University*, *Qiqihar* 161006, *China*)

Abstract: In this paper, an optical image encryption algorithm based on spiral phase transform and new generalized fibonacci chaotic system is proposed to solve the problems of the Fresnel domain double random phase coding system is insensitive to the first diffraction distance，uneven distribution of chaotic sequences and weak resistance to choice plaintext attack. The plaintext image is encoded as phase information and spiral phase transformed to overcame the insensitivity of the first random phase template and diffraction distance of the Fresnel diffraction transform-double random phase encoding system. The sensitivity of the optical keys is improved. The weighted interference between secure image and plaintext image is added to further increase the sensitivity of the optical keys and dimension of key . A generalized Fibonacci chaotic system, which could generate uniform sequences, is constructed to generate phase templates to overcame uneven distribution of logistic chaos and improve the efficiency of key transmission and the sensitivity of the keys. The chaotic initial value and parameters of spiral phase transform are related to SHA-256. It makes the keys change with the plaintext and achieved the effect of “one encryption at a time”, and enhanced the sensitivity of the plaintext and the ability of the resistance to choice plaintext attack and avalanche effect.Experimental comparison shows that this method can effectively increase the plaintext sensitivity and key sensitivity. This method’ robustness and the key space are sufficiently secure. It is a high security optical image encryption method.

Key words: Optical image encryption; Generalized Fibonacci chaos; Spiral phase transform; Fresnel transform; One encryption at a time

收稿日期：2019-07-10；改回日期：2020-02-27；网络出版：2020-03-12
*通信作者： 许鑫 2254512063@qq.com
基金项目：国家自然科学基金(61872204)，黑龙江省自然科学基金(F2017029)，黑龙江省省属高等学校基本科研业务费科研项目(135109236)
Foundation Items: The National Natural Science Foundation of China (61872204), Heilongjiang Provincial Natural Science Fund (F2017029), Heilongjiang Provincial Basic Scientific Research Operating Expenses of Institutions of Higher Learning (135109236)

1　引言

图像具有直观生动的特性成为信息表达的重要形式之一，其安全性越来越重要，由于光学的多密钥维度，高速并行性等特点，被广泛运用到图像加密中[1–3]。最具代表性是1995年Refregier和Javidi[4]提出的双随机相位编码系统(Double Random Phase Encoding, DRPE)，简称4f系统，系统具有高速并行的数据处理能力，但对光学元件排列有高精度要求。后又衍生出菲涅耳域的双随机相位编码系统[5](Fresnel Diffraction Transform-Double Random Phase Encoding, FDT-DRPE)，不需透镜装置更为简单紧凑，引入衍射距离增加密钥维度，但对第1块随机模板和第1次衍射距离不够敏感。同时上述两个加密系统的固有线性和对称性使其易受已知明文，选择明文和唯密文的攻击[6–8]。为解决上述攻击问题，提高加密算法的安全性，有学者通过改变线性特性，Qin等人[9]提出基于切相傅里叶变换的光学非对称算法，引入相位剪切改变线性特性，文献[10]将此方法推广到菲涅尔变换，增加密钥维度，进一步提高系统安全性，但当加密密钥作为公钥时这类加密算法会被迭代相位恢复算法破解[11,12]。Wang等人[13]提出基于相位恢复算法的非对称加密算法，可以有效抵抗文献[11,12]的破解方式，但因多次迭代计算量增大。又有学者将密钥和明文进行联系，刘禹佳等人[14]提出基于矢量分解和副像相位掩模的遥感图像加密技术，引入矢量运算使得解密相位板与明文密切相关，但系统抗噪声能力较弱。同时以上两种抗攻击方式的加密系统存在密钥体积过大，无法有效解决密钥的管理与分发传递问题。

因混沌的伪随机性与光学系统随机模板要求一致，将混沌初值和参数替代随机模板作为密钥，可解决上述密钥的问题，故许多学者将混沌引入到光学加密中，其中Logistic混沌因结构简单，具有很好的混沌特性被广泛使用[15–19]。为有效抵御选择明密文攻击，其中文献[18,19]将混沌和明文进行联系。文献[18]用明文像素值生成混沌初值，文献[19]将混沌与明文级联构成一个与明文相关的新参数。但这两种联系方式与明文的关联性不强，无法达到“一次一密”的效果，雪崩效应不够明显，抵御攻击能力较弱。同时所用的Logistic混沌具有分布不均匀、存在奇异点和低随机性等缺点，存在安全隐患[20,21]。

本文构造一种新型的广义Fibonacci混沌系统，产生均匀分布的混沌序列，增强系统对密文的隐藏性和密钥的敏感性。明文图像通过螺旋相位变换，克服FDT-DRPE系统对第1次菲涅尔衍射距离不敏感缺陷，提高光学密钥敏感性。引入安全图像与明文加权干涉，进一步提高光学密钥敏感性，并将权重作为密钥，增加算法设计自由度。另外将明文哈希值SHA-256与混沌初值和螺旋相位变换参数进行强关联，使其达到“一次一密”的加密效果，极大地提高明文敏感性和抵御选择明文攻击能力。

2　加密原理

本文提出一种基于螺旋相位变换和广义Fibonacci混沌的光学图像加密方法，加密原理如图1。

明文图像F与另一大小类型完全一致的安全图像G同时进行相位编码和螺旋相位变换得到F_2和G_2，将二者加权干涉得到K，由可产生均匀混沌序列但参数不同的广义Fibonacci混沌a和b构造随机模板RM1和RM2，进行菲涅尔域的双随机相位编码加密。其中混沌初值X_1和W_1，螺旋相位变换参数Q分别与明文图像F哈希值SHA-256相联系，使加密系统达到“一次一密”的效果，以抵御选择明密文攻击。

3　理论分析

3.1　菲涅尔域的双随机相位编码系统

菲涅尔域的双随机相位编码[5]加密系统如图2，加解密原理为

$$e(x'',y'')=\mathrm{FDT}_{d_2}\{\mathrm{FDT}_{d_1}[f(x,y)\cdot \mathrm{RM1}]\cdot \mathrm{RM2}\} \tag{1}$$

$$F(x,y)=\mathrm{FDT}_{-d_1}\{\mathrm{FDT}_{-d_2}[e(x'',y'')]\,\mathrm{RM2}^*\}\mathrm{RM1}^* \tag{2}$$

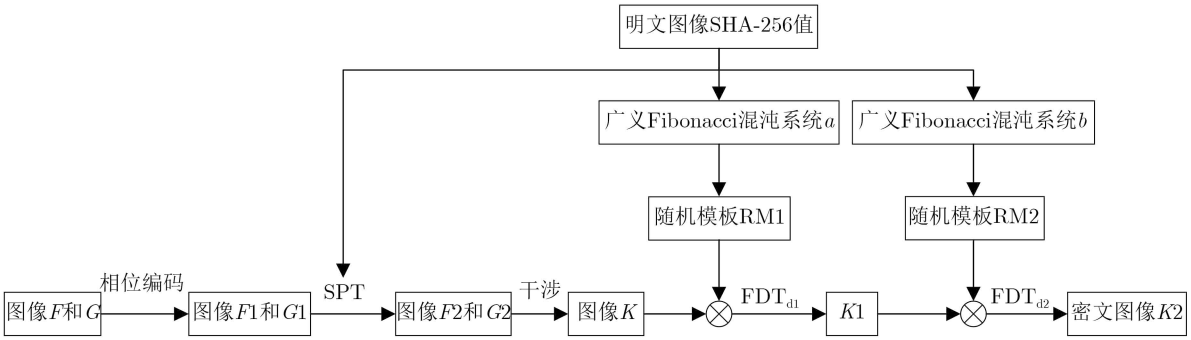


图 1 加密原理框图

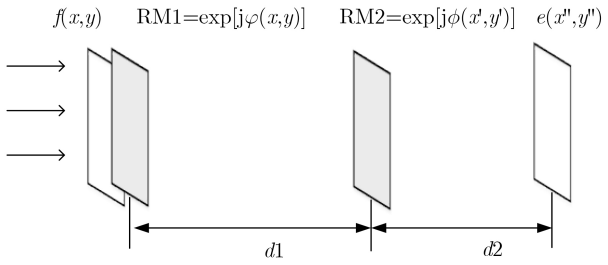


图 2 FDT-DRPE加密系统

其中，$f(x,y)$为明文图像，$e(x'',y'')$为密文图像，$F(x,y)$为解密图像，随机模板RM1和RM2为[0 , 2π]上均匀分布的独立白噪声序列，RM1*和RM2*为复共轭，FDT_{d_1}和FDT_{d_2}为距离为d_1和d_2的菲涅尔衍射变换。

3.2 新型广义Fibonacci混沌系统

构造产生均匀非相关混沌序列的广义Fibonacci混沌，其中广义变参数3阶Fibonacci数列[22]为

$$F_i=(AF_{i-1}+BF_{i-2}+CF_{i-3})\bmod M \tag{3}$$

其中，A, B, C为3个变量, $F_1=F_2=F_3=1$, $i=4, 5, \cdots, M$。

量子Logistic混沌系统[23]表达式为

$$\left.\begin{aligned} x_{i+1}&=\gamma\left(x_i-|x_i|^2\right)-\gamma y_i\\ y_{i+1}&=-y\mathrm{e}^{-2\beta}+\gamma\mathrm{e}^{-\beta}\times[(2-x_i-x_i^*)\,y_i-x_iz_i^*-x_i^*z_i]\\ z_{i+1}&=-z_i\mathrm{e}^{-2\beta}+\gamma\mathrm{e}^{-\beta}\times[(2-x_i^*)\,z_i-2x_iy_i-x_i] \end{aligned}\right\} \tag{4}$$

式(4)可调参数$\gamma\in(3.74, 4)$，耗散参数$\beta\geq 3.5$，状态值$x_i\in(0, 1)$,$y_i\in(0, 0.2461)$,$z_i\in(0,0.2461)$，系统处于混沌状态，x_i^*, z_i^*分别是x_i和z_i的复共轭。

为增加序列随机性，降低相关性，用量子Logistic混沌产生序列x_i, y_i, z_i作为广义3阶Fibonacci函数参数A, B, C，再用此广义Fibonacci函数对Logistic混沌$w_{i+1}=\mu w_i(1-w_i)$, $w_1\in(0, 1)$, $\mu\in[3.57, 4]$扰动得到广义Fibonacci混沌为

$$C_{\mathrm{FQL}}=\{F[Q(\gamma,\beta,X_1,y_1,z_1)]+L(W_1,\mu)\}\bmod 1 \tag{5}$$

其中，$Q(\gamma,\beta,X_1,y_1,z_1)$为初值$X_1$, y_1和z_1的量子Logistic混沌，$F[Q(\gamma,\beta,X_1,y_1,z_1)]$为广义Fibonacci函数，$L(W_1,\mu)$为初值$W_1$的Logistic混沌。其中，初值$X_1$和$W_1$与明文SHA-256及给定初值$x_1$, w_1联系，明文图像F哈希值是长度为256 bit的$H=\{H_1,H_2,\cdots,H_{64}\}$，初值$X_1$和$W_1$计算方式为

$$X_1=\mathrm{mod}\left\{x_1+\left(\sum_{i=1}^{16}H_{32-i}\times 16^{i-1}\right)\Big/10^{18},1\right\} \tag{6}$$

$$W_1=\mathrm{mod}\left\{w_1+\left(\sum_{i=1}^{16}H_{16-i}\times 16^{i-1}\right)\Big/10^{18},1\right\} \tag{7}$$

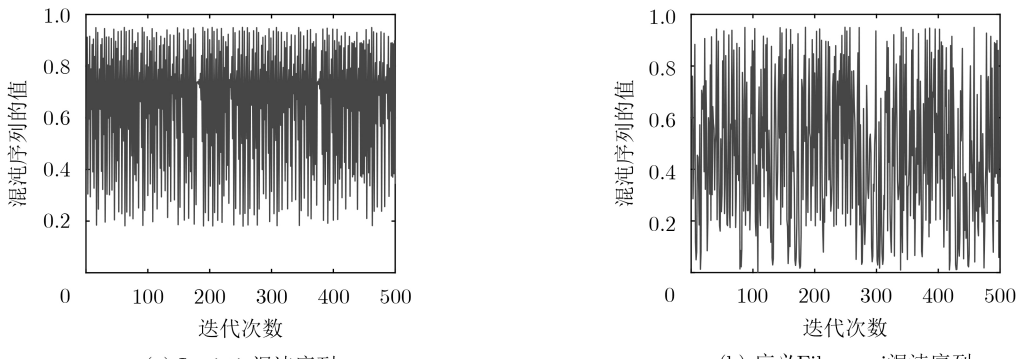
在加密过程中，即使明文图像只有一个像素的区别，它们的Hash值也完全不同，对应初值X_1和W_1也完全不同，其攻击复杂度为2^{256}，足以抵抗任何暴力攻击。不断迭代式(5)，其中Logistic混沌参数$\mu=3.8$, $w_1=0.4$；量子Logistic混沌参数$\gamma=3.99$, $\beta=6.2$, $x_1=0.2$, $y_1=0.01$, $z_1=0.0019$。将Logistic混沌与广义Fibonacci混沌分别迭代500次序列分布如图3。

由图3可知，广义Fibonacci混沌图3(b)比Logistic混沌图3(a)序列分布更均匀，随机性更好，弥补Logistic混沌序列分布不均匀缺点，用其构成随机模板元素更加均匀，更好对密文进行隐藏，加密更安全。

3.3 改进螺旋相位变换

在螺旋相位变换(Spiral Phase Transform, SPT)中，SPT将1维希尔伯特变换到2维即螺旋相位函数(Spiral Phase Function, SPF)，可定义为纯螺旋相位空间函数[24]为

$$\mathrm{SPF}=\mathrm{sgn}(u,v)=\frac{u+\mathrm{j}v}{\sqrt{u^2+v^2}}=\exp\{\mathrm{j}\varphi\ (u,\ v)\} \tag{8}$$



(a) Logistic混沌序列　　(b) 广义Fibonacci混沌序列

图 3 Logistic混沌系统和广义Fibonacci混沌系统序列分布图

SPF在原点无定义，函数值可按0或1处理，称为奇点[25]。本文引入参数q，并将q与明文图像哈希值SHA-256进行联系，构成一个新的参数Q，构造一个与明文相关的修正函数SPF_b，关联方式如式(10)

$$\mathrm{SPF}_b=\exp\{\mathrm{j}Q\varphi\ (u,\ v)\} \tag{9}$$

$$Q=q+\left(\sum_{i=1}^{32}H_{64-i}\times 32^{i-1}\right)\Big/10^{17} \tag{10}$$

其中，$\varphi(u,v)$为频率空间极角坐标，j为虚数单位。对于SPF_b, 2维信号$f(x,y)$的SPT及其逆变换为[24]

$$\mathrm{SPT}\{f\ (x,y)\}=\mathrm{IFT}\{\mathrm{SPF}_b\cdot\mathrm{FT}\ \{f\ (x,y)\}\} \tag{11}$$

$$\mathrm{ISPT}\{f\ (x,y)\}=\mathrm{IFT}\{\mathrm{SPF}_b^{*}\cdot\mathrm{FT}\ \{f\ (x,y)\}\} \tag{12}$$

其中，FT和IFT为2维傅里叶变换和其逆变换，SPF_b^{*}为复共轭。SPF_b即使参数q相同，但不同图像对应不同哈希值即Q不同，对应不同的螺旋相位函数，进行不同的螺旋相位变换，能达到一次加密，一次螺旋相位变换的效果。将明文图像，螺旋相位模板及SPT后图像对比如图4。由图4可知，通过SPT对明文信息扰乱，无明显视觉信息泄露，为加密提供安全保障。

4　加解密过程

假设明文图像F和安全图像G大小为$M\times N$，得到像素矩阵$\boldsymbol{F}(x,y)$和$\boldsymbol{G}(x,y)$，加解密步骤为：

(1) 计算$\boldsymbol{F}(x,y)$的SHA-256值$H=\{H_1,H_2,\cdots,H_{64}\}$，对$\boldsymbol{F}(x,y)$和$\boldsymbol{G}(x,y)$进行相位编码得到

$$F_1(x,y)=\exp[\mathrm{j}\boldsymbol{F}(x,y)],G_1(x,y)=\exp[\mathrm{j}\boldsymbol{G}(x,y)] \tag{13}$$

(2) 给定不同参数q_1和q_2，结合H代入式(9)，式(10)，构造螺旋相位模板

$$\mathrm{SPF}_{b_1}=\exp\{\mathrm{j}Q_1\varphi\ (u,\ \mathrm{v})\},\mathrm{SPF}_{b_2}=\exp\{\mathrm{j}Q_2\varphi\ (u,v)\} \tag{14}$$

(3) 对$F_1(x,y)$和$G_1(x,y)$进行SPT得到

$$\left.\begin{aligned}F_2(x,y)&=\mathrm{SPT}\{F_1(x,y)\}\\&=\mathrm{IFT}\{\mathrm{SPF}_{b_1}\cdot\mathrm{FT}\ \{F_1\ (x,y)\}\}\\G_2(x,y)&=\mathrm{SPT}\{G_1(x,y)\}\\&=\mathrm{IFT}\{\mathrm{SPF}_{b_2}\cdot\mathrm{FT}\ \{G_1(x,y)\}\}\end{aligned}\right\} \tag{15}$$

(4) 引入权重v，进行干涉得到

$$K(x,y)=v\cdot F_2(x,y)+(1-\ v)\cdot G_2(x,y) \tag{16}$$

(5) 将初值x_1, w_1和H代入式(6)，式(7)，用广义Fibonacci混沌a和b构造随机模板RM1和RM2

$$\left.\begin{aligned}\mathrm{RM1}&=\exp[\mathrm{j}2\pi a(W_{1a},\mu_a,X_{1a},y_{1a},z_{1a},\gamma_a,\beta_a)]\\\mathrm{RM2}&=\exp[\mathrm{j}2\pi b(W_{1b},\mu_b,X_{1b},y_{1b},z_{1b},\gamma_b,\beta_b)]\end{aligned}\right\} \tag{17}$$

(6) $K(x,y)$与RM1相乘，经距离为$d1$的菲涅尔衍射变换(FDT)后得到

$$\begin{aligned}K_1(\alpha,\beta)&=\mathrm{FDT}_{d_1}[K(x,y)\cdot\mathrm{RM1}]\\&=\mathrm{FDT}_{d_1}\{[v\ \cdot F_2(x,y)+(1-\ v)\cdot G_2(x,y)]\\&\quad\cdot\exp[\mathrm{j}2\pi a(W_{1a},\mu_a,X_{1a},y_{1a},z_{1a},\gamma_a,\beta_a)]\end{aligned} \tag{18}$$

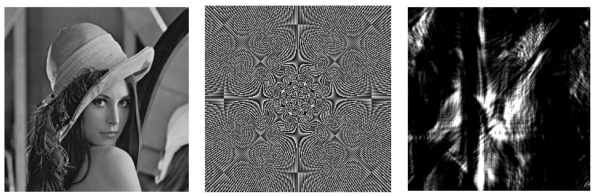
(7) $K_1(\alpha,\beta)$再与RM2相乘，做距离为d_2的FDT，得到最终加密图像

$$\begin{aligned}K_2(x,y)=&\mathrm{FDT}_{d_2}\{\mathrm{FDT}_{d_1}[K(x,y)\ \cdot\mathrm{RM1}]\cdot\mathrm{RM2}\}\\=&\mathrm{FDT}_{d_2}\{\mathrm{FDT}_{d_1}\{[v\cdot F_2(x,y)\\&+(1-v)\cdot G_2(x,y)]\\&\cdot\exp[\mathrm{j}2\pi a(W_{1a},\mu_a,X_{1a},y_{1a},z_{1a},\gamma_a,\beta_a)]\}\\&\cdot\exp[\mathrm{j}2\pi b(W_{1b},\mu_b,X_{1b},y_{1b},z_{1b},\gamma_b,\beta_b)]\}\end{aligned} \tag{19}$$

(8)解密即为加密的逆过程。

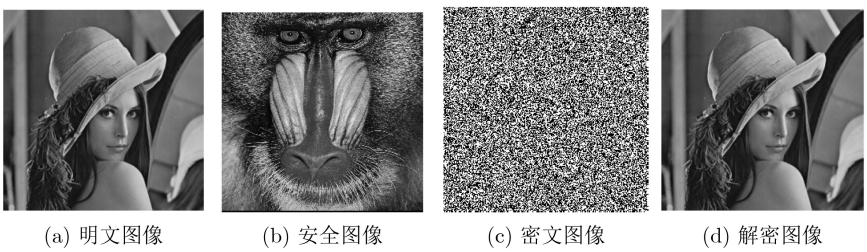
5　实验及算法性能分析

选取Lena(256×256)灰度图像作为实验仿真对象。加密算法在matlab2014a环境进行实验仿真。实验密钥如下：广义Fibonacci混沌a密钥$\gamma_a=3.99$, $\beta_a=6$, x_{1a}=0.2, y_{1a}= 0.01, z_{1a}= 0.0019, w_{1a}= 0.4, μ_a= 3.99；广义Fibonacci混沌b密钥γ_b= 3.90, β_b= 6.2, x_{1b}= 0.3, y_{1b}= 0.03, z_{1b}= 0.0015, w_{1b}= 0.39, μ_b= 4; SPT参数q_1=70, q_2=40；权重因子$v=0.3$; d_1= 3, d_2= 4, λ=633×10^{-9}。加解密仿真结果如图5。



(a) 明文图像　(b) 螺旋相位模板　(c) SPT后的明文图像

图 4 效果分析图



(a) 明文图像　(b) 安全图像　(c) 密文图像　(d) 解密图像

图 5 算法的加解密图像

密文图5(c)已看不出明文图像任何轮廓，类似于白噪声。解密图5(d)和明文图5(a)在视觉上，几乎看不出差别，说明本文算法加解密效果良好。

5.1 敏感性分析

5.1.1 明文敏感性分析

一个好的加密算法应具有好的明文敏感性，即当明文图像发生微小变化，引起密文图像巨大改变。用像素数改变率(Number of Pixels Change Rate, NPCR)和归一化平均变化强度(Unified Average Changing Intensity, UACI)，计算加密算法对明文的敏感性。设密文图像在(i,j)点像素值分别为$C_1(i,j)$和$C_2(i,j)$。若$C_1(i,j)=C_2(i,j)$，$D(i,j)=0$；若$C_1(i,j)\neq C_2(i,j)$，$D(i,j)=1$。NPCR和UACI定义为

$$\mathrm{NPCR}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)\times 100\% \tag{20}$$

$$\mathrm{UACI}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C_1(i,j)-C_2(i,j)|}{255}\times 100\% \tag{21}$$

对明文图像采取不同改变方式，即任取明文一点坐标，将其像素值加1；再任取像素值不同两点进行位置互换，计算NPCR和UACI。表1为本文算法，文献[14,19]不同改变方式的NPCR和UACI值。

由表1可知，在两种改变方式下，文献[14,19]密文基本不变，而本文算法NPCR都达到99%，说明本算法密文每个像素值基本都发生变化，这是因为本算法将明文哈希值SHA-256与混沌初值及螺旋相位变换参数关联，故对明文更加敏感，雪崩效应更强，加密系统更安全。

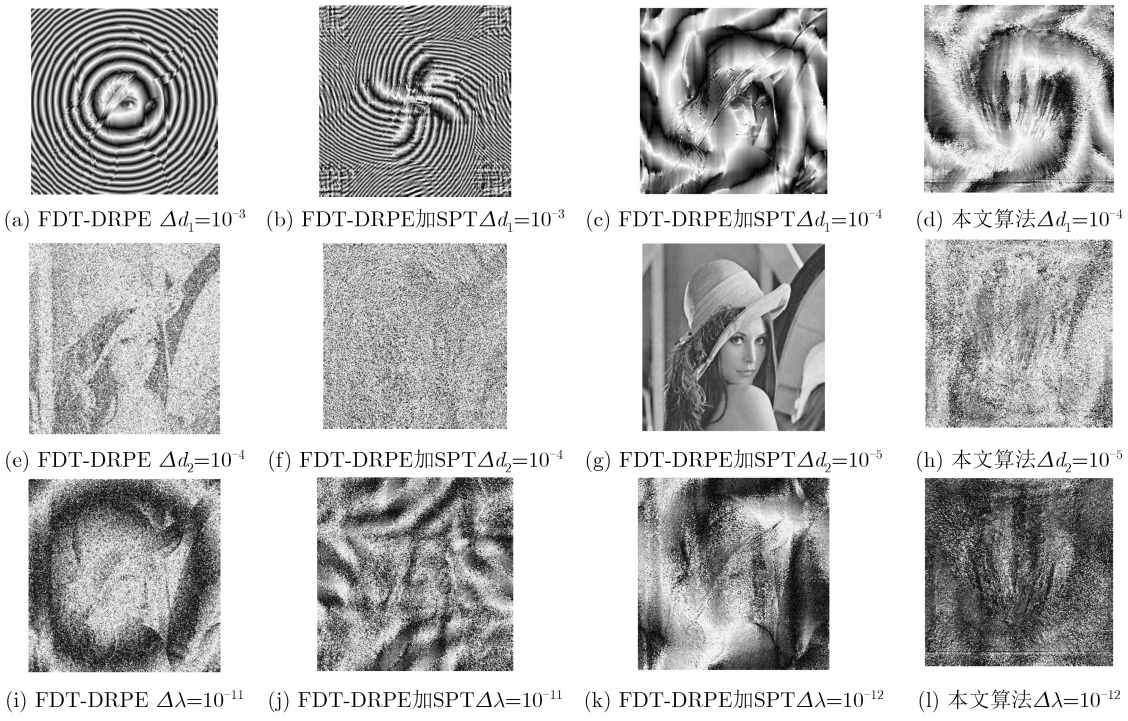
5.1.2 密钥敏感性分析

为分析光学密钥敏感性，将FDT-DRPE加密系统，加入SPT的FDT-DRPE加密系统，和本文加密系统这3个系统进行比较，改变光学密钥d_1, d_2和λ进行解密效果分析如图6。

对比图6(a), 6(e), 6(i)和6(b), 6(f), 6(j)，光学密钥出现同样偏差时，FDT-DRPE系统能看到明文图像轮廓，FDT-DRPE加入SPT对明文扰动，看不到明文图像信息，提高光学密钥敏感性。对比图6(c), 6(g), 6(k)和6(d), 6(h), 6(l)，密钥误差减

表 1 NPCR和UACI值对比

改变方式	比较项	文献[14]	文献[19]	本文算法
像素值加1	NPCR	1.0082×10^{-5}	1.5259×10^{-5}	0.9910
	UACI	0	0	0.0787
两像素点交换位置	NPCR	3.0025×10^{-5}	3.0518×10^{-5}	0.9917
	UACI	1.0003×10^{-5}	1.1070×10^{-5}	0.0700



(a) FDT-DRPE $\Delta d_1=10^{-3}$ (b) FDT-DRPE加SPT$\Delta d_1=10^{-3}$ (c) FDT-DRPE加SPT$\Delta d_1=10^{-4}$ (d) 本文算法$\Delta d_1=10^{-4}$

(e) FDT-DRPE $\Delta d_2=10^{-4}$ (f) FDT-DRPE加SPT$\Delta d_2=10^{-4}$ (g) FDT-DRPE加SPT$\Delta d_2=10^{-5}$ (h) 本文算法$\Delta d_2=10^{-5}$

(i) FDT-DRPE $\Delta\lambda=10^{-11}$ (j) FDT-DRPE加SPT$\Delta\lambda=10^{-11}$ (k) FDT-DRPE加SPT$\Delta\lambda=10^{-12}$ (l) 本文算法$\Delta\lambda=10^{-12}$

图 6 密钥敏感性对比分析

小，FDT-DRPE加入SPT后能看到明文图像轮廓，本算法加入SPT并添加安全图像G与明文进行干涉运算，很好隐藏明文信息，进一步提高光学密钥敏感性，d_1, d_2和λ灵敏度分别为10^{-4}, 10^{-5}, 10^{-12}。其他密钥w_1, μ, γ和x_1灵敏度为10^{-16}, 10^{-15}, 10^{-15}和10^{-17}。

5.2 抗选择明文攻击分析

若加密系统能抵抗选择明文攻击，则可抵抗已知明文、选择密文、唯密文3种攻击方式[26]。本文用选择明文攻击测试系统安全性，将Lena第1个像素点加1得到伪明文图像Lena2，再选取另一安全图像作为伪明文图像Lena3。分别对其进行加密，获得解密密钥后对图5(c)密文解密，结果如图7(b)和7(d)。

由图7可知，Lena2与明文只有一个像素点不同，无法从解密图得到明文任何信息，不存在“轮廓现象”，换成与明文差距更大图像Lena3，解密图更无法看到明文信息。这是因为本文密钥是由明文SHA-256产生，明文微小变化都会使哈希值发生巨大变化，即不同明文所用密钥流不同，对应不同解密密钥，攻击者不可能通过其他明文密文对来攻击系统获得解密明文密钥获取明文，达到了“一次一密”的效果。

5.3 鲁棒性分析

图像在传输过程中有可能会受到噪声污染或者损坏造成图像失真，本文就此做了相应的鲁棒性测试。

5.3.1 抗剪切攻击分析

图8(a)和8(c)，密文图像左上角的1/16和1/4被剪切，图8(b)和8(d)能清晰地恢复出明文信息。说明本加密系统可以有效对抗剪切攻击。

5.3.2 抗噪声攻击分析

对密文图像进行高斯噪声污染，高斯噪声污染形式为

$$Q_2' = Q_2\,(1+\ kG) \tag{22}$$

Q_2'为污染后的密文图像，Q_2为密文图像，G为均值为0、方差为1的高斯噪声，k为高斯噪声强度系数。用相关系数(Correlation Coefficient, CC)来评估解密图像质量，$f\,(x,y)$为明文图像，$F\,(x,y)$为解密图像，$\overline{f}$和$\overline{F}$分别为明文和解密图像某像素点灰度值平均值

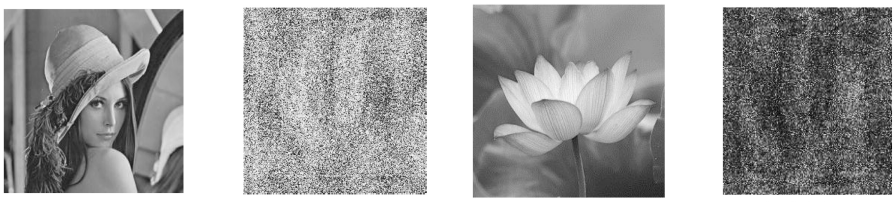
$$\mathrm{CC} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[f(x,y)-\overline{f}][F(x,y)-\overline{F}]}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[f(x,y)-\overline{f}]^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[F(x,y)-\overline{F}]^2}} \tag{23}$$

将文献[14]、文献[19]和本文算法都进行式(22)的高斯噪声污染，相应的解密图像对比如图9。给出相关系数CC随强度系数k的变化曲线如图10。

由图9(a)可知，文献[14]k仅为0.04，噪声对解密结果影响较大。对比图9(b)和9(c)k为0.4，本文算法比文献[19]解密图像更加清晰，抗噪声能力更强。图9(d)当k高达0.8时，本文算法仍然能辨别图像的整体内容和基本轮廓。由图10可知，随着k不断增大，本文算法比文献[14]和文献[19]的解密图像质量更好。由此本算法具有更高抗噪声攻击能力。通过对抗剪切和抗噪声分析，本文算法有很好的鲁棒性，能有效地提高混沌和光学图像加密技术的实际应用能力，安全性高。

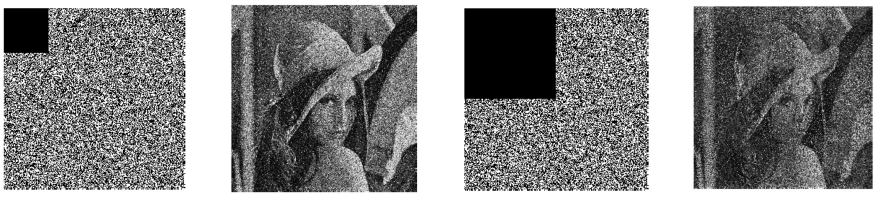
5.4 统计特性分析

本文从两个方面对统计特性进行分析，即直方图和相邻像素点相关性。图11(a)和11(b)为明密文图像的灰度直方图，图11(c)和11(d)为明密文图像垂直方向相邻像素分布图。



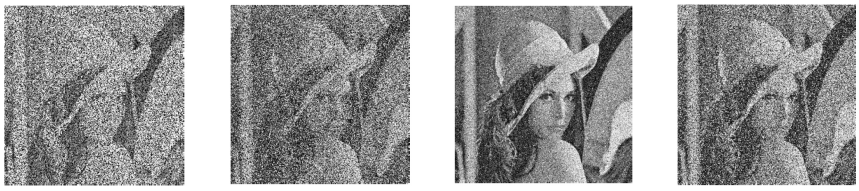
(a) 伪明文图像Lena2　(b) 解密图Lena2　(c) 伪明文图像Lena3　(d)解密图Lena3

图 7 选择明文攻击模拟结果



(a) 1/16剪切　(b) 解密图像　(c) 1/4剪切　(d) 解密图像

图 8 剪切攻击下密文和解密图像



(a) 文献[14]k=0.04 (b)文献[19]k=0. 4 (c)本文算法k=0.4 (d) 本文算法k=0.8

图 9 噪声污染下的解密图像

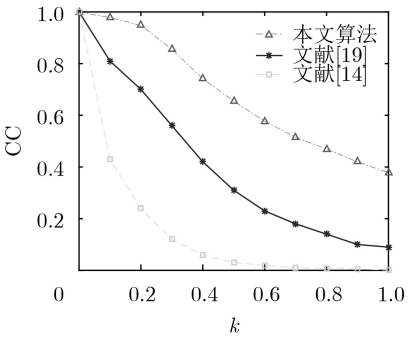


图 10 相关系数随噪声强度系数变化图

图11(a)和11(b)可知，明文灰度值分布不均匀，呈现出明显分布统计规律。密文直方图更加平坦，很好隐藏了明文信息。图11(c)和11(d)可知，明文相邻像素点具有强相关性，密文像素点更加均匀，扩散性更好，有效破坏明文相邻像素相关性。

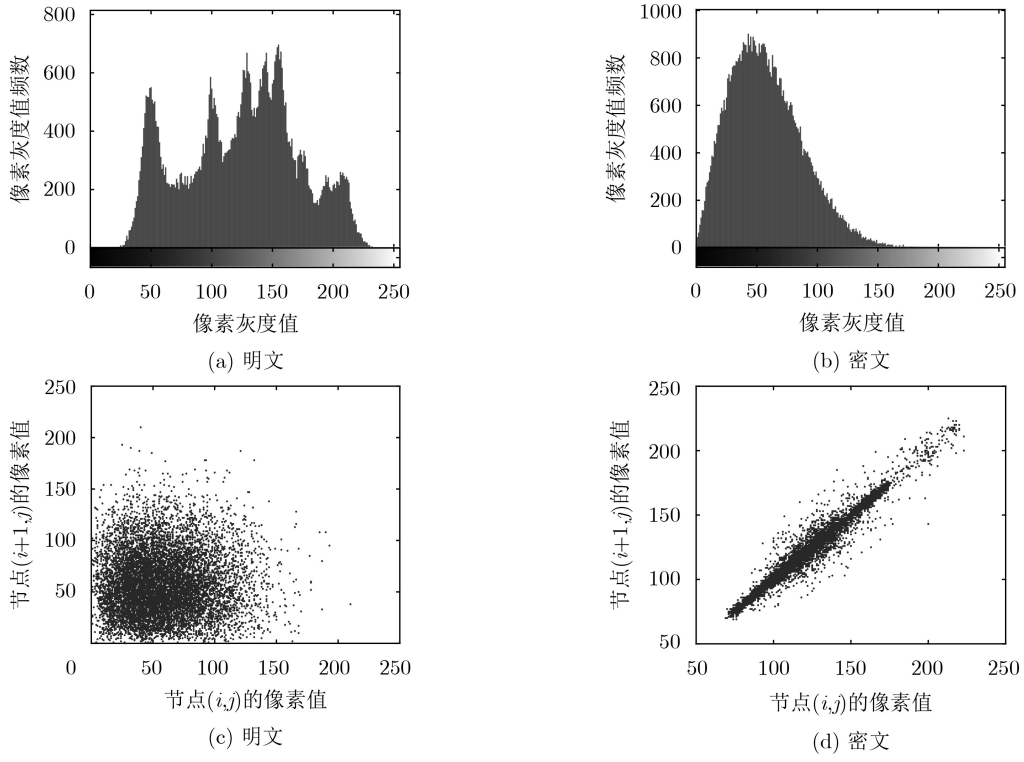
5.5 抗穷举攻击分析

密钥空间是衡量加密系统抵御穷举攻击的重要指标。本文以量子Logistic混沌参数γ_a和γ_b,β_a和β_b，初值x_{1a}和x_{1b}, y_{1a}和y_{1b}, z_{1a}和z_{1b}; Logistic混沌参数μ_a和μ_b，初值w_{1a}和w_{1b}; SPT参数q_1和q_2，权重因子v，光学密钥d_1, d_2和λ作为加密密钥。本文20个加密密钥采用数据都为双精度类型，每个密钥都可以用包含1位整数和14位小数的15位精度实数表示，可得密钥空间为$\left(10^{15}\right)^{20}=10^{300}$，从安全的角度，密钥空间$\geq 2^{100}\approx 10^{30}$就能满足较高的安全级别，因此对于穷举攻击，本算法密钥空间是安全的。

5.6 性能对比分析

将本文算法与文献[14]、文献[19]进行加密系统性能比较，对比结果如表2。

由表2可知，本文算法相邻像素相关性优于文献[14]，光学密钥敏感性高于文献[14]和文献[19]，且加密算法依赖于明文，有效抵御选择明文的攻击，密钥空间更大能更好的抵御穷举攻击，具有较高的安全性。



(a) 明文 (b) 密文

(c) 明文 (d) 密文

图 11 明密文直方图和垂直方向相邻像素分布图

表 2　性能对比结果

比较项		文献[19]	文献[14]	本文算法
相邻像素相关性	水平	0.0001	0.0334	-0.0036
	垂直	0.0014	0.0248	0.0004
	对角	0.0014	0.0288	-0.0082
光学密钥敏感性	d_1	10^{-3}	10^{-4}	10^{-4}
	d_2	10^{-4}	10^{-5}	10^{-5}
	λ	10^{-11}	10^{-9}	10^{-12}
抵御选择明文攻击		否	是	是
是否依赖于明文		否	是	是
密钥空间		10^{114}	10^{203}	10^{300}

6　结论

本文将光学信息安全技术和混沌密码学有效结合，提出一种基于螺旋相位变换和广义Fibonacci混沌系统的光学图像加密算法。将明文图像通过螺旋相位变换和安全图像的加权干涉，提高光学密钥敏感性，增强对明文隐藏性及算法的安全性。由高随机性和低相关性的广义Fibonacci混沌系统构造元素均匀的随机模板，用于图像加密安全性更高，且有效解决密钥分发和传递困难的问题。混沌的初值和螺旋相位变换的参数通过明文哈希值SHA-256产生，可有效地抵御选择明文攻击，提高明文敏感性。本文算法明文及密钥敏感性强，实现“一次一密”的加密效果，达到雪崩效应，具有更高安全性和实用性。

参 考 文 献

[1] WANG Qu, XIONG Deping, ALFALOU A, *et al*. Optical image encryption method based on incoherent imaging and polarized light encoding[J]. *Optics Communications*, 2018, 415: 56–63. doi: 10.1016/j.optcom.2018.01.018.

[2] LI Xiaowei, ZHAO Min, XING Yan, *et al*. Designing optical 3D images encryption and reconstruction using monospectral synthetic aperture integral imaging[J]. *Optics Express*, 2018, 26(9): 11084–11099. doi: 10.1364/OE.26.011084.

[3] LI Chengqing, ZHANG Yun, and XIE E Y. When an attacker meets a cipher-image in 2018: A year in review[J]. arXiv: 1903.11764, 2019.

[4] REFREGIER P and JAVIDI B. Optical image encryption based on input plane and Fourier plane random encoding[J]. *Optics Letters*, 1995, 20(7): 767–769. doi: 10.1364/OL.20.000767.

[5] SITU G, PEDRINI G, and OSTEN W. Strategy for cryptanalysis of optical encryption in the Fresnel domain[J]. *Applied Optics*, 2010, 49(3): 457–462. doi: 10.1364/AO.49.000457.

[6] PENG Xiang, ZHANG Peng, WEI Hengzheng, *et al*. Known-plaintext attack on optical encryption based on double random phase keys[J]. *Optics Letters*, 2006, 31(8): 1044–1046. doi: 10.1364/OL.31.001044.

[7] 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. doi: 10.3321/j.issn:1000-3290.2006.03.021.

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. doi: 10.3321/j.issn:1000-3290.2006.03.021.

[8] LIU Xiaoli, WU Jiachen, HE Wenqi, *et al*. Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding[J]. *Optics Express*, 2015, 23(15): 18955–18968. doi: 10.1364/OE.23.018955.

[9] QIN Wan and PENG Xiang. Asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. *Optics Letters*, 2010, 35(2): 118–120. doi: 10.1364/OL.35.000118.

[10] WANG Yong, QUAN Chenggen, and TAY C J. Optical color image encryption without information disclosure using phase-truncated Fresnel transform and a random amplitude mask[J]. *Optics Communications*, 2015, 344: 147–155. doi: 10.1016/j.optcom.2015.01.045.

[11] WANG Yong, QUAN Chenggen, and TAY C J. Improved method of attack on an asymmetric cryptosystem based on phase-truncated Fourier transform[J]. *Applied Optics*, 2015, 54(22): 6874–6881. doi: 10.1364/AO.54.006874.

[12] RAJPUT S K and NISHCHAL N K. Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform[J]. *Applied Optics*, 2013, 52(4): 871–878. doi: 10.1364/AO.52.000871.

[13] WANG Yong, QUAN Chenggen, and TAY C J. Asymmetric optical image encryption based on an improved amplitude-phase retrieval algorithm[J]. *Optics and Lasers in Engineering*, 2016, 78: 8–16. doi: 10.1016/j.optlaseng.2015.09.008.

[14] 刘禹佳, 徐熙平, 徐嘉鸿, 等. 基于矢量运算和副像相位掩模的

遥感图像加密技术[J]. 光子学报, 2019, 48(2): 0210002. doi: 10.3788/gzxb20194802.0210002.

LIU Yujia, XU Xiping, XU Jiahong, *et al*. Remote sensing image encryption using vector operations and secondary image phase masks[J]. *Acta Photonica Sinica*, 2019, 48(2): 0210002. doi: 10.3788/gzxb20194802.0210002.

[15] 常杰. 基于分数傅里叶变换的双图像光学加密技术研究[D]. [硕士论文], 哈尔滨工程大学, 2013.

CHANG Jei. Research on double image optical encryption in the fractional Fourier-domain[D]. [Master dissertation], Harbin Engineering University, 2013.

[16] 朱薇, 杨庚, 陈蕾, 等. 基于小波变换和改进双随机相位编码的多图像加密算法[J]. 南京邮电大学学报: 自然科学版, 2014, 34(5): 87–92.

ZHU Wei, YANG Geng, CHEN Lei, *et al*. Multiple-image encryption based on wavelet transform and improved double random phase encoding[J]. *Journal of Nanjing University of Posts and Telecommunications*: *Natural Science*, 2014, 34(5): 87–92.

[17] 孙杰. 基于多混沌系统的双图像光学加密算法[J]. 光学技术, 2017, 43(3): 279–283.

SUN Jie. Double optical images encryption method based on chaotic systems[J]. *Optical Technique*, 2017, 43(3): 279–283.

[18] 张博, 龙慧, 江沸菠. 基于相干叠加与模均等矢量分解的光学图像加密算法[J]. 电子与信息学报, 2018, 40(2): 438–446. doi: 10.11999/JEIT170489.

ZHANG Bo, LONG Hui, and JIANG Feibo. Optical image encryption algorithm based on coherent superposition and equal modulus vector decomposition[J]. *Journal of Electronics & Information Technology*, 2018, 40(2): 438–446. doi: 10.11999/JEIT170489.

[19] 朱薇, 杨庚, 陈蕾, 等. 基于混沌的改进双随机相位编码图像加密算法[J]. 光学学报, 2014, 34(6): 0607001. doi: 10.3788/AOS201434.0607001.

ZHU Wei, YANG Geng, CHEN Lei, *et al*. An improved image encryption algorithm based on double random phase encoding and chaos[J]. *Acta Optica Sinica*, 2014, 34(6): 0607001. doi: 10.3788/AOS201434.0607001.

[20] 陈志刚, 梁涤青, 邓小鸿, 等. Logistic混沌映射性能分析与改进[J]. 电子与信息学报, 2016, 38(6): 1547–1551.

CHEN Zhigang, LIANG Diqing, DENG Xiaohong, *et al*. Performance analysis and improvement of Logistic chaotic mapping[J]. *Journal of Electronics & Information Technology*, 2016, 38(6): 1547–1551.

[21] LI Chengqing, LIN Dongdong, LÜ Jinhu, *et al*. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography[J]. *IEEE MultiMedia*, 2018, 25(4): 46–56. doi: 10.1109/MMUL.2018.2873472.

[22] HU Xubo, YANG Xiangbo, and LIU Songhao. Optical transmission through generalized third-order Fibonacci multilayers[J]. *Modern Physics Letters B*, 2014, 28(16): 1450129. doi: 10.1142/S0217984914501292.

[23] SINGH R K, KUMAR B, SHAW D K, *et al*. Level by level image compression-encryption algorithm based on quantum chaos map[J]. *Journal of King Saud University - Computer and Information Sciences*, 2018, S1319157817304123. doi: 10.1016/j.jksuci.2018.05.012.

[24] LARKIN K G, BONE D J, and OLDFIELD M A. Natural demodulation of two-dimensional fringe patterns. I. General background of the spiral phase quadrature transform[J]. *Journal of the Optical Society of America A*, 2001, 18(8): 1862–1870. doi: 10.1364/JOSAA.18.001862.

[25] LU Yuzhen, LI R, and LU Renfu. Fast demodulation of pattern images by spiral phase transform in structured-illumination reflectance imaging for detection of bruises in apples[J]. *Computers and Electronics in Agriculture*, 2016, 127: 652–658. doi: 10.1016/j.compag.2016.07.012.

[26] ZHANG Yushu and XIAO Di. Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform[J]. *Optics and Lasers in Engineering*, 2013, 51(4): 472–480. doi: 10.1016/j.optlaseng.2012.11.001.

郭 媛：女，1974年生，教授，研究方向为光电检测与传感器技术、光学散斑测量、光学图像加密与隐私保护.

许 鑫：女，1994年生，硕士生，研究方向为信息安全、光学图像加密.

敬世伟：男，1995年生，硕士生，研究方向为信息安全、光学图像加密.

金 涛：男，1980年生，副教授，研究方向为图像加密.

金 梅：女，1977年生，讲师，研究方向为图像加密.