基于离散分数随机变换的双彩色图像加密算法

张文全 周南润*
(南昌大学电子信息工程系 南昌 330031)

摘 要：该文基于离散分数随机变换和线性同余理论，提出一种单通道双彩色图像加密算法。输入的两幅 RGB 图像转换成相应的索引图像格式，其中一幅 2 维索引图像被编码为振幅部分，另一幅则被编码为空域相位掩模。分数域相位掩模由线性同余发生器 (LCG) 生成，并将彩色映射矩阵嵌入其中。引入光学幅相调制技术，在不增加光学元件的基础上实现了双彩色图像加密。离散分数随机变换的分数阶和线性同余函数的 4 个参数作为密钥提高了算法的安全性，对应所有密钥计算了输入图像和解密图像的均方误差。针对唯密文攻击，噪声叠加和抗裁剪性能分别进行了数值模拟，验证了该算法的可行性和有效性。

关键词：彩色图像加密；离散分数随机变换；傅里叶光学；相位编码；线性同余发生器
中图分类号：TP309.7 **文献标识码**：A **文章编号**：1009-5896(2012)07-1727-08
DOI: 10.3724/SP.J.1146.2011.01364

Double-color Image Encryption Based on Discrete Fractional Random Transform

Zhang Wen-quan Zhou Nan-run
(*Department of Electronic Information Engineering*, *Nanchang University*, *Nanchang* 330031, *China*)

Abstract: A new single-channel double-color image encryption algorithm is proposed by combining Discrete Fractional Random Transform (DFrRT) with linear congruence theory. The two input RGB images are converted into their indexed image formats, and one of the 2D indexed image is encoded in amplitude part and the other is encoded into the spatial domain phase mask. The two color map matrixes are embedded in the fractional domain phase mask which is generated by Linear Congruential Generator (LCG). The amplitude-phase encoding is introduced into the optical encryption system to implement the double-color image encryption algorithm without increasing other optical elements. The fractional order of DFrRT and the four parameters of the linear function are the keys to enhance the security of the proposed algorithm, and the Mean Square Error (MSE) between the decrypted images and the input ones for all keys are calculated. The performance of the proposed scheme is analyzed against ciphertext-only attack, noise addition and occlusion of the encrypted image, respectively. Numerical simulation results demonstrate the feasibility and effectiveness of the proposed method.

Key words: Color image encryption; Discrete Fractional Random Transform (DFrRT); Fourier optics; Phase encoding; Linear Congruence Generator (LCG)

1 引言

在图像信息安全问题的研究中，基于分数傅里叶变换(Fractional Fourier Transform, FrFT)理论的彩色图像加密成为学者关注的热点，提出了多种新方法[1–9]。文献[1]运用分数域双随机相位编码技术分别加密一幅 RGB 彩色图像的 3 个分量，3 个通道的密钥增大了算法的密钥空间，但光学实现需要 3 组加密装置，实用性受到限制。文献[5]把一幅 RGB 彩色图像变换为 HSI 彩色空间，用离散分数随机变换对强度分量进行像素值加密，用阿诺德变换对色调和饱和度分量进行位置加密，这种双重加密方式保证了算法的安全性。文献[6,7]提出了基于多路复用的多幅彩色图像加密算法，在该方法中，将 RGB 图像格式转换为索引图像格式，再将多幅图像数字合成为一幅复图像，通过单通道加密光路完成多幅图像加密。文献[9]提出一种新的单通道彩色图像加密算法，在 HSI 空间中，强度分量作为相位编码的原始待加密图像，将饱和度分量加密为随机相位，与色调分量一起构成了对强度分量加密的双相位。本文采用光学幅相调制技术设计了一种基于离散分数随机变换[10](DFrRT)的单通道双彩色图像加密算法，并给出了相应的光学实现。该加密算法两次重

2011-12-21 收到，2012-03-22 改回
国家自然科学基金(61141007)，江西省自然科学基金(2009GQS0080)和江西省教育厅科技项目(GJJ11339)资助课题
*通信作者：周南润 znr21@163.com

复使用一组光学元件完成两幅索引彩色图像加密，增加彩色图像加密方便性的同时节约了系统的成本，提高了多幅彩色图像加密的效率。

2 基于 DFrRT 的单通道双彩色图像加密算法

2.1 采用 LCG(Linear Congruential Generator)随机化分数傅里叶变换的核矩阵

2 维信号 $\boldsymbol{B}$ 的离散分数随机变换表示为

$$\boldsymbol{F}^p[\boldsymbol{B}]=\boldsymbol{H}^p\boldsymbol{B}\left(\boldsymbol{H}^p\right)^{\mathrm{T}} \tag{1}$$

式中 T 表示矩阵的转置运算， p 是 DFrRT 的分数阶。变换核矩阵 $\boldsymbol{H}^p$ 表示为

$$\boldsymbol{H}^p=\boldsymbol{V}\boldsymbol{D}^p\boldsymbol{V}^{\mathrm{T}} \tag{2}$$

其中 $\boldsymbol{V}$ 为本征向量矩阵， $\boldsymbol{D}^p$ 为 DFrRT 本征值的对角矩阵：

$$\boldsymbol{D}^p=\mathrm{diag}\left\{\left[1,\exp\left(-2\pi ip\frac{1}{t}\right),\cdots,\exp\left(-2\pi ip\frac{N-1}{t}\right)\right]\right\} \tag{3}$$

式中 t 是 DFrRT 的周期。随机化本征向量就使 $\boldsymbol{H}^p$ 具有了随机性[11]，因而生成随机化的本征向量是 DFrRT 的核心。目前利用计算机生成均匀随机数的常用方法是 LCG 法[12,13]，递推关系为

$$\left.\begin{aligned}x_n&=ax_{n-1}+c \pmod M\\ r_n&=x_n/M,\quad n=1,2,\cdots\end{aligned}\right\} \tag{4}$$

其中初值 $x_0\ (0\le x_0<M)$，乘数 $a\ (0\le a<M)$，增量 $c\ (0\le c<M)$，模数 $M(M>0)$ 为算法的 4 个参数。利用 LCG 生成的随机序列重构一个 2 维伪随机矩阵 $\boldsymbol{R}$，并生成一个实数对称矩阵 $\boldsymbol{S}$：

$$\boldsymbol{S}=(\boldsymbol{R}+\boldsymbol{R}^{\mathrm{T}})/2 \tag{5}$$

矩阵 $\boldsymbol{S}$ 与 $\boldsymbol{H}^p$ 满足 $\boldsymbol{H}^p\boldsymbol{S}=\boldsymbol{S}\boldsymbol{H}^p$，它们具有相同的本征向量，数值计算方法可以得到矩阵 $\boldsymbol{S}$ 的归一化本征向量。矩阵 $\boldsymbol{S}$ 是对称的随机矩阵，所以 $\boldsymbol{H}^p$ 的本征向量相互正交且具有随机性，LCG 参数的变化将导致 DFrRT 结果的改变。

2.2 单通道双彩色图像加密算法

RGB 图像可看作由红、绿、蓝分量形成的堆，索引图像是一种把像素值直接作为彩色映射矩阵下标的图像。索引图像包含两个分量：整数的数据矩阵和一个取值范围在 [0,1] 之间的彩色映射矩阵 $\boldsymbol{Z}$，$\boldsymbol{Z}$ 的每一行都定义单色的红、绿、蓝 3 个分量。索引图像将每个像素的颜色由对应的整数矩阵的值作为指向 $\boldsymbol{Z}$ 的一个指针决定。本文算法将两幅 RGB 格式的彩图 1 和彩图 2 分别转换成索引格式图像，对应的数据矩阵为 $\boldsymbol{A}_1$ 和 $\boldsymbol{A}_2$，对应的彩色映射矩阵为 $\boldsymbol{Z}_1$ 和 $\boldsymbol{Z}_2$，把 $\boldsymbol{Z}_1$ 和 $\boldsymbol{Z}_2$ 嵌入由 LCG 生成的伪随机矩阵 $\boldsymbol{R}$ 中作为相位信息 $\boldsymbol{A}_3$。由于 $\boldsymbol{R}$ 和 $\boldsymbol{Z}$ 的取值范围都在 [0,1] 之间， $\boldsymbol{A}_3$ 既保持了 $\boldsymbol{R}$ 的随机性和均匀性，又隐藏了 $\boldsymbol{Z}_1$ 和 $\boldsymbol{Z}_2$。分别对 $\boldsymbol{A}_1$， $\boldsymbol{A}_2$ 和 $\boldsymbol{A}_3$ 做归一化处理以限定它们在相位分布函数和振幅函数的范围中。

$$\begin{aligned}&\boldsymbol{I}_1=\frac{\boldsymbol{A}_1}{\mathrm{A}}\in(0,1),\ \boldsymbol{I}_2=2\pi\frac{\boldsymbol{A}_2}{\mathrm{A}}\in(0,2\pi),\\ &\boldsymbol{I}_3=2\pi\boldsymbol{A}_3\in(0,2\pi)\end{aligned} \tag{6}$$

这里取 A=1+max($\boldsymbol{A}_1,\boldsymbol{A}_2$)。加密过程如图 1(a)所示，运用空间光调制器(SLM)，分别将 $\boldsymbol{I}_2$ 和 $\boldsymbol{I}_3$ 调制成空域相位掩模 $\boldsymbol{M}_1(x,y)$ 和分数域相位掩模 $\boldsymbol{M}_2(u,v)$，即

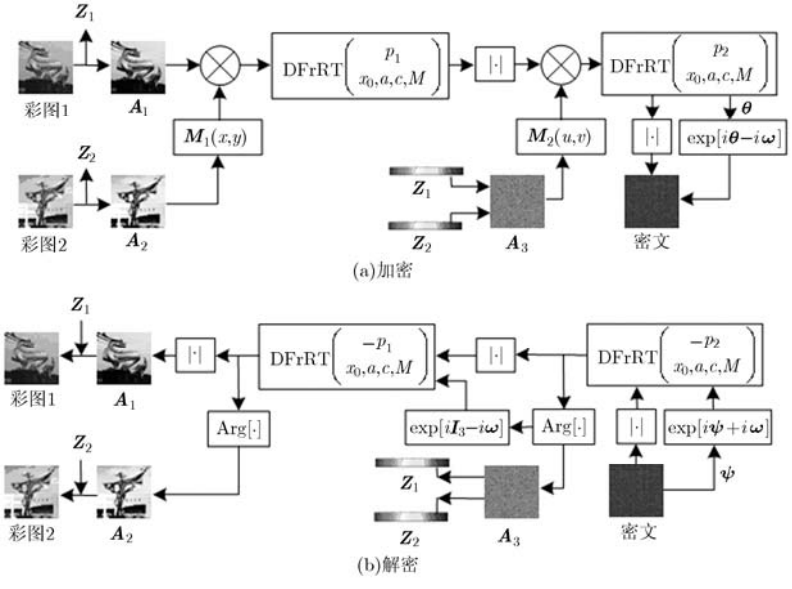


图 1 双彩色图像加密算法框架图

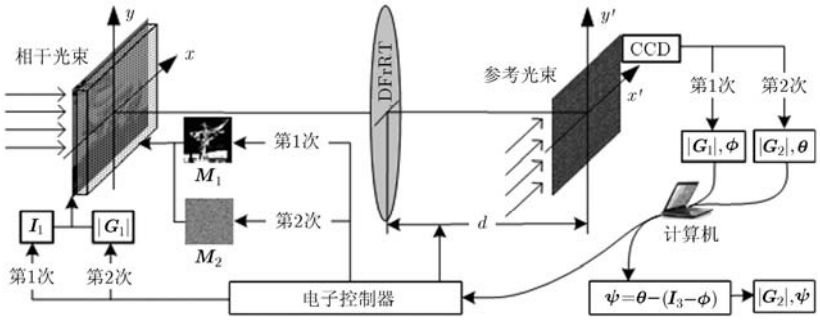


图 2 加密方案的光电混合装置

$$\left.\begin{aligned}\boldsymbol{M}_1(x,y)&=\exp\left[i\boldsymbol{I}_2(x,y)\right]\\ \boldsymbol{M}_2(u,v)&=\exp\left[i\boldsymbol{I}_3(u,v)\right]\end{aligned}\right\}\tag{7}$$

明文 $\boldsymbol{I}_1$ 在空域被 $\boldsymbol{M}_1$ 调制，构成入射波函数 $\boldsymbol{G}(x,y)=\boldsymbol{I}_1(x,y)\boldsymbol{M}_1(x,y)$，对 $\boldsymbol{G}(x,y)$ 进行一次 p_1 阶的 DFrRT，在分数域平面 (u,v) 上得到

$$\boldsymbol{G}_1(u,v)=\boldsymbol{F}^{p_1}\left\{\boldsymbol{I}_1(x,y)\exp\left[i\boldsymbol{I}_2(x,y)\right]\right\}\tag{8}$$

用分数域相位掩模 $\boldsymbol{M}_2$ 对 $|\boldsymbol{G}_1|$ 进行相位调制，$|\bullet|$ 表示计算复函数的模值。对调制后信息进行 p_2 阶 DFrRT，在输出平面上得到的密文为

$$\boldsymbol{G}_2(x',y')=\boldsymbol{F}^{p_2}\left\{\left|\boldsymbol{G}_1(u,v)\right|\exp\left[i\boldsymbol{I}_3(u,v)\right]\right\}\tag{9}$$

除了传统的分数阶参数 p_1，p_2 作为密钥外，本文算法还增加了随机化变换核矩阵时 LCG 的 4 个参数作为密钥。相位密钥是本文算法的关键，相位密钥 $\boldsymbol{\omega}$ 和输出相位 $\boldsymbol{\psi}$ 的关系为

$$\left.\begin{aligned}\boldsymbol{\phi}(u,v)&=\mathrm{Arg}\left[\boldsymbol{G}_1(u,v)\right]\\ \boldsymbol{\omega}&=\boldsymbol{I}_3-\boldsymbol{\phi}\\ \boldsymbol{\theta}(x',y')&=\mathrm{Arg}\left[\boldsymbol{G}_2(x',y')\right]\\ \boldsymbol{\psi}&=\boldsymbol{\theta}-\boldsymbol{\omega}\end{aligned}\right\}\tag{10}$$

其中 $\mathrm{Arg}[\bullet]$ 表示计算复函数相位值。输出密文为复振幅函数 $|\boldsymbol{G}_2(x',y')|\exp[i\boldsymbol{\psi}(x',y')]$。

图 1(b)所示为解密流程，是上述加密过程的逆过程。由密文相角 $\boldsymbol{\psi}$，密钥 $\boldsymbol{\omega}$ 和 $|\boldsymbol{G}_2|$ 还原复函数 $\boldsymbol{G}_2(x',y')$ 并进行 $-p_2$ 阶的 DFrRT，得到

$$|\boldsymbol{G}_1|\exp(i\boldsymbol{I}_3)=\boldsymbol{F}^{-p_2}\left[|\boldsymbol{G}_2|\exp(i\boldsymbol{\psi}+i\boldsymbol{\omega})\right]\tag{11}$$

由式中相位值能恢复明文 $\boldsymbol{I}_3$，通过 $\boldsymbol{I}_3$ 减去 $\boldsymbol{\omega}$ 计算相角 $\boldsymbol{\phi}$，结合 $|\boldsymbol{G}_1|$ 可以在分数域平面上恢复出 $\boldsymbol{G}_1(u,v)$。将 $\boldsymbol{G}_1(u,v)$ 进行 $-p_1$ 阶 DFrRT，$\boldsymbol{I}_1$ 和 $\boldsymbol{I}_2$ 的解密过程为

$$\left.\begin{aligned}\boldsymbol{I}_1&=\left|\boldsymbol{F}^{-p_1}\left[|\boldsymbol{G}_1|\exp(i\boldsymbol{I}_3-i\boldsymbol{\omega})\right]\right.\\ \boldsymbol{I}_2&=\mathrm{Arg}\left\{\boldsymbol{F}^{-p_1}\left[|\boldsymbol{G}_1|\exp(i\boldsymbol{I}_3-i\boldsymbol{\omega})\right]\right\}\end{aligned}\right\}\tag{12}$$

2.3 算法的光学实现

DFrRT 的实现目前还没有严格的光学结构[14]，本文采用文献[14]提出的一种模拟光学装置来实现 DFrRT。实现单通道双彩色图像加密算法的光电混合装置如图 2 所示。第 1 次光学加密实现式(8)，复函数 $\boldsymbol{G}_1(u,v)$ 的幅值可用 CCD 记录，相位可采用 3 步相移数字全息技术检测[15]。在第 2 次光学加密前，SLM 调制为 $\boldsymbol{M}_2$，$\boldsymbol{I}_1$ 更换为 $|\boldsymbol{G}_1|$，调整分数域距离 d 以实现分数阶次的改变。实现式(9)的加密过程后，再用 $\boldsymbol{\psi}$ 对 $|\boldsymbol{G}_2|$ 进行相位编码。与文献[6]双图像数字合成不同，本文采用的幅相调制技术同时完成双彩色图像单通道加密，便于用光学设备实现加密。

3 双图像加密算法的数值模拟

模拟中分数阶次 $p_1=0.3$，$p_2=0.6$；线性同余函数的参数 $x_0=100$，$a=16805$，$c=7$，$M=2^{31}-1$。待加密的两幅原始彩色图像如图 3(a), 3(b)所示，图 3(c)是嵌入了彩色映射矩阵 $\boldsymbol{Z}_1$ 和 $\boldsymbol{Z}_2$ 的伪随机相位矩阵 $\boldsymbol{A}_3$，图 3(d)是最终密文的振幅输出 $|\boldsymbol{G}_2|$，可以看出加密图像类似于噪音图像。图 3(e), 3(f)分别对应 2 维索引图像 $\boldsymbol{A}_1$ 和 $\boldsymbol{A}_2$ 的直方图，图 3(g)对应密文振幅的直方图，加密图像的直方图明显变平滑了，密码分析者难以通过统计特性获得原始图像的特征。在密钥相同的条件下，用归一化的 3 幅灰度图像替代 $\boldsymbol{I}_1$，$\boldsymbol{I}_2$ 和 $\boldsymbol{I}_3$，图 4 表明用此算法加密统计特性完全不同的图像，密文的直方图非常相似。证明加密算法符合经典密码理论中的混淆与扩散思想，可有效抵抗统计分析破译。

根据彩色映射矩阵的嵌入方式，解密者可从 $\boldsymbol{I}_3$ 还原 $\boldsymbol{Z}_1$ 和 $\boldsymbol{Z}_2$，结合 $\boldsymbol{I}_1$ 和 $\boldsymbol{I}_2$ 还原的 $\boldsymbol{A}_1$ 和 $\boldsymbol{A}_2$ 恢复两幅彩色图像。当所有密钥都正确时，解密的彩色图像如图 5(a)和图 6(a)所示，两幅图像间不存在相互串扰。文献[6]没考虑对矩阵 $\boldsymbol{Z}$ 进行加密，存在安全隐患。本文算法对不同 $\boldsymbol{Z}$ 矩阵同时加密，尤其适用于有高保密要求的彩色图像保护。

数值模拟中假设其它密钥均正确，仅分数阶 p_1 偏差 0.01 时的两幅解密图像如图 5(b)和图 6(b)所示；仅分数阶 p_2 偏差 0.01 时的解密图像如图 5(c)和

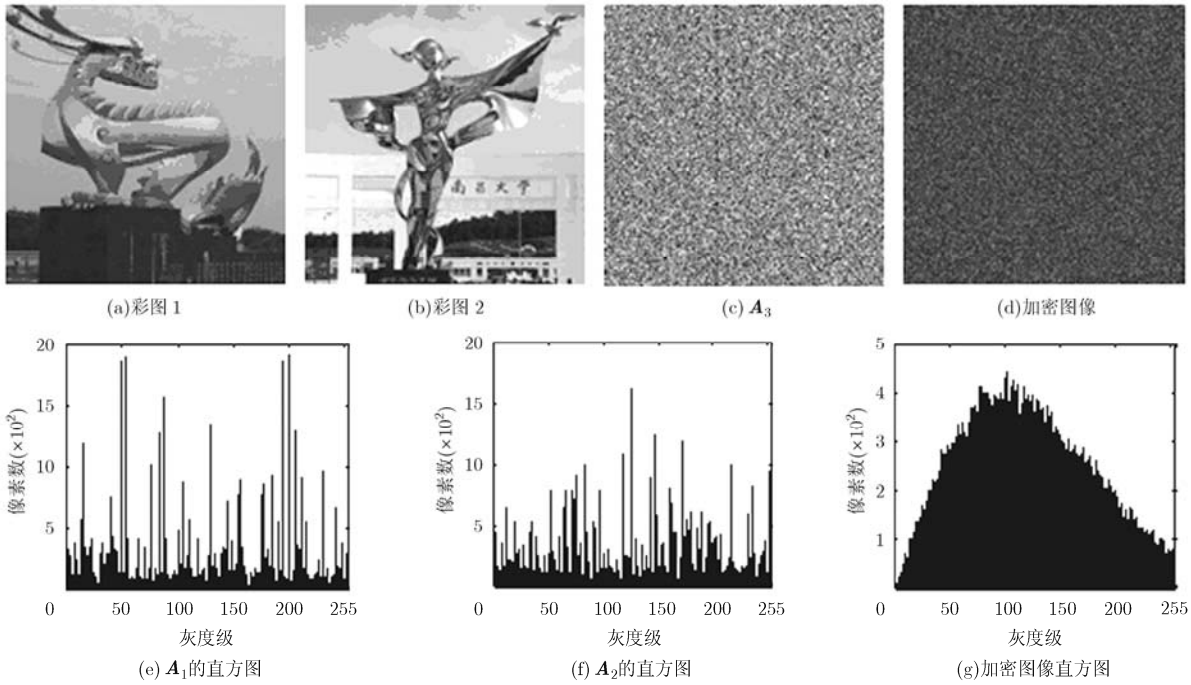


图 3 双彩色图像加密结果

图 4 3 幅灰度图像加密结果直方图

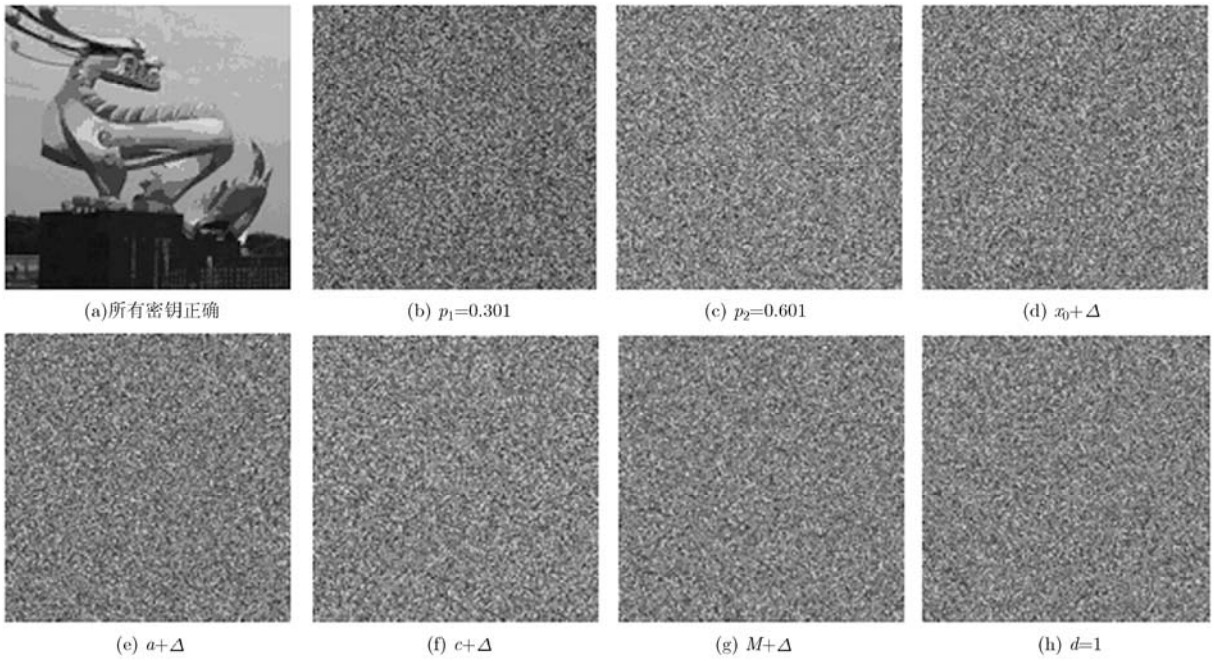


图 5 密钥对应的图像 1 解密结果 ($\Delta = 1$)

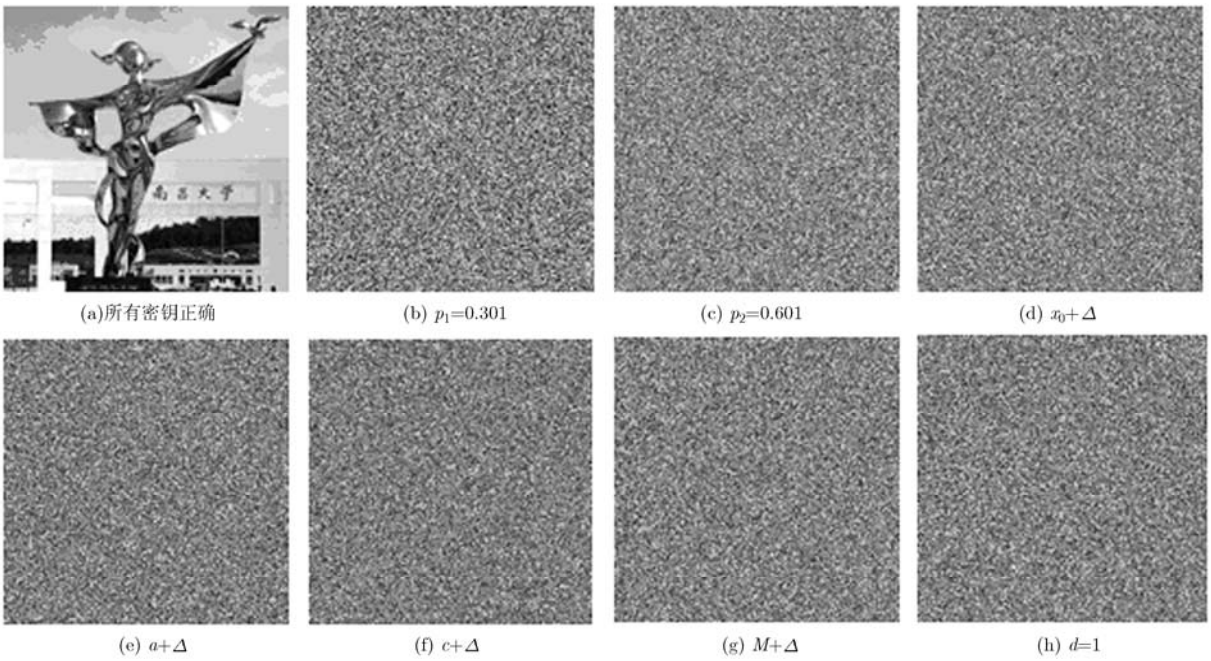


图 6 密钥对应的图像 2 解密结果 ($\Delta = 1$)

图 6(c)所示；验证了分数阶密钥的安全性。为了说明 LCG 参数密钥的安全性，引入偏差值 Δ，假设其它密钥均正确，图 5(d), 5(e), 5(f)和 5(g)表示 LCG 的 4 个参数分别偏差 $\Delta = 1$ 时对应于彩图 1 的解密图像；图 6(d), 6(e), 6(f)和 6(g)表示 LCG 的 4 个参数分别偏差 $\Delta = 1$ 时对应于彩图 2 的解密图像。

4　加密算法安全性分析

衡量解密图像和原始图像的相似程度一般采用均方误差(MSE)。$h_1(i,j)$ 和 $h_2(i,j)$ 分别代表原图和解密图像的灰度值，均方误差定义如下：

$$\mathrm{MSE}(h_1,h_2)=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|h_2(i,j)-h_1(i,j)\right|^2 \quad (13)$$

其中 $M\times N$ 为图像的大小。本文设定均方误差 3000 作为阈值，当均方误差低于此阈值时，图像的全部信息可以被复原。

4.1 相位密钥安全性分析

模拟中假设其它密钥正确，为了验证相位密钥 $\boldsymbol{\omega}$ 的安全性，给 $\boldsymbol{\omega}$ 加入一定范围的偏差，偏差后的相位密钥为 $\boldsymbol{\omega}' = \boldsymbol{\omega} + d\Delta r$，其中 d 是偏离的幅度，Δr 是均匀分布于区间 $[0,2\pi]$ 的随机相位。图 5(h)和图 6(h)所示为 $d = 1$ 时对应的两幅解密图像。d 在 $[-1,1]$ 之间变化时，对应 $\boldsymbol{I}_1$ 和 $\boldsymbol{I}_2$ 解密的两条 MSE 曲线如图 7(a)所示，图中用实线标明了 MSE 阈值。$\boldsymbol{I}_1$ 和 $\boldsymbol{I}_2$ 的 MSE 曲线在阈值以下部分 d 的变化范围 Δd_1 和 Δd_2 显示于图 7(a)中。相位密钥的大小为 (256×256)，其变化区间为 $[0,2\pi]$，且 $\Delta d_2 < \Delta d_1 = 0.25$，算法的密钥空间近似为 $(2\pi/0.25)^{256\times256} \approx 25^{256\times256}$，这个庞大的数字表明盲解密者很难实施穷举攻击。

本算法中，密文和相位密钥 $\boldsymbol{\omega}$ 都与输入图像的彩色映射矩阵有关，攻击者难以获得大量的资源(如明文密文对)用于选择密文攻击，已知明文攻击和选择明文攻击。唯密文攻击只需一个完整的密文[16]，也是常用的验证加密算法安全性的方法之一。如果攻击者已知整个加密算法和除 $\boldsymbol{\omega}$ 之外其它的密钥，且获得了密文 $|\boldsymbol{G}_2(x',y')|\exp[i\psi(x',y')]$，基于相位迭代算法的唯密文攻击[17]方案设计为：

(1)以任意随机相位 $\boldsymbol{\varphi}$ 替代相位密钥 $\boldsymbol{\omega}$，完成式(11)和式(12)的解密过程；

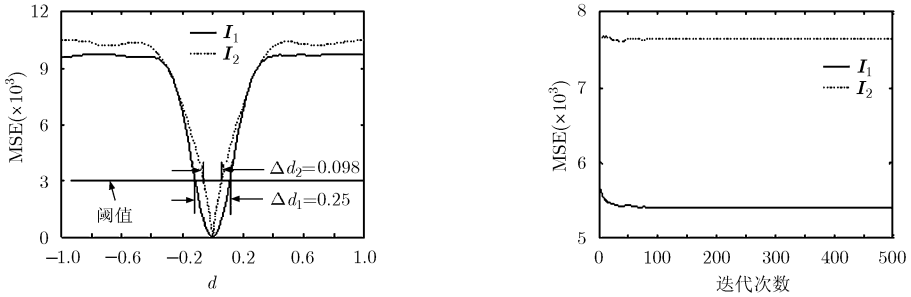
(2)将第(1)步解密得到的 $\boldsymbol{I}_1$，$\boldsymbol{I}_2$ 和 $\boldsymbol{I}_3$ 代入式(8)和式(9)的加密过程，并计算新的相位密钥 $\boldsymbol{\varphi}'$；

(3)用第(2)步计算的相位密钥 $\boldsymbol{\varphi}'$ 再次替代相位密钥 $\boldsymbol{\omega}$，重复(1)到(3)步的计算，直到计算完成设定的迭代次数。

图 7(b)是唯密文攻击者对图像解密进行 500 次迭代计算后，$\boldsymbol{I}_1$ 和 $\boldsymbol{I}_2$ 解密随迭代次数变化的均方误差曲线。由图可知，当迭代计算进行 100 次后，MSE 没有收敛趋势，并且始终大于阈值 3000，图像不能被恢复，表明本文算法可以很好地抵抗唯密文攻击。

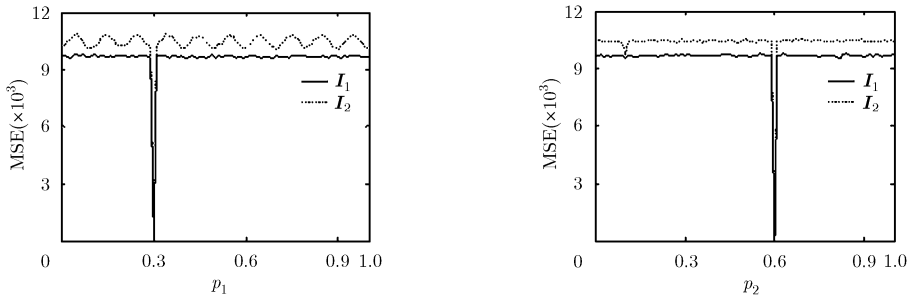
4.2 DFrRT 密钥安全性分析

为了考查加密方法对抗盲解密的能力，图 8(a), 8(b)分别对应分数阶密钥 p_1 和 p_2 进行了灵敏性分



(a) d 对应的解密MSE曲线　　(b)迭代次数的MSE曲线

图 7 相位密钥安全性分析



(a) p_1对应的解密MSE曲线　　(b) p_2对应的解密MSE曲线

图 8 分数阶密钥安全性分析

析，仅当 $p_1=0.3$，$p_2=0.6$，$\boldsymbol{I}_1$ 和 $\boldsymbol{I}_2$ 才能完全复原；测试发现任何一个分数阶的偏差值大于 0.005 时，MSE>3000，得到的解密图像有相当强的噪声。分数阶密钥具有很高的灵敏度，意味着密钥空间巨大，穷举攻击很难成功。

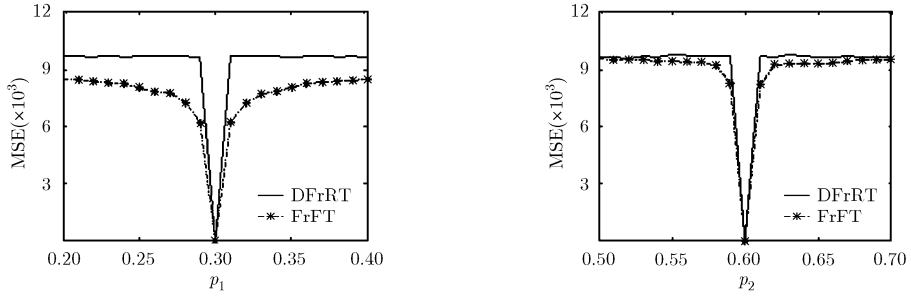
随机化离散 FrFT 的核矩阵时，把 LCG 产生的随机矩阵和 FrFT 集成为一个随机的变换，算法密钥数量由 2 重增加到 6 重，加密更为安全。图 9 给出两种变换分数阶密钥对应 $\boldsymbol{I}_1$ 解密的 MSE 对比，DFrRT 的灵敏性明显好于 FrFT。对应 LCG 的 4 个参数密钥的灵敏性分析如图 10 所示，任何一个 LCG 参数的偏差量 $|\Delta|\geq 1$ 时，MSE > 5000；线性同余函数的 4 个参数作为密钥具有几乎相同的灵敏性，拥有巨大的密钥空间，能有效抵抗穷举攻击。

4.3 鲁棒性分析

图像处理和传输过程中会有噪声的影响或物理损坏，算法抵抗噪声和裁剪攻击的鲁棒性很重要。均值为 0，方差为 0.1 的高斯噪声 $\boldsymbol{N}$ 加入 $|\boldsymbol{G}_2|$，噪声干扰后加密图像振幅为 $|\boldsymbol{G}_2|'$。

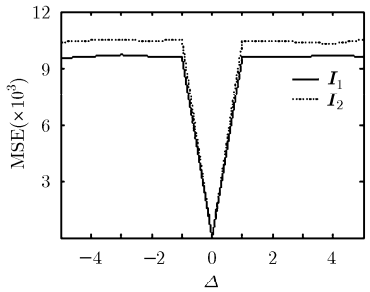
$$|\boldsymbol{G}_2|'=|\boldsymbol{G}_2|(1+k\boldsymbol{N}) \tag{14}$$

其中 k 是噪声强度的系数。对应 k 的变化，解密图像 $\boldsymbol{I}_1$ 和 $\boldsymbol{I}_2$ 的均方误差变化如图 11(a)所示，图 11(b)和11(c) 分别为加密图像受到 $k=0.5$ 强度高斯噪声攻击后 $\boldsymbol{I}_1$ 和 $\boldsymbol{I}_2$ 的解密图像，$\boldsymbol{I}_1$ 的解密效果明显强于 $\boldsymbol{I}_2$。由图 11(a)可知，随着 k 的增大，$\boldsymbol{I}_2$ 的 MSE 比 $\boldsymbol{I}_1$ 的 MSE 增加更快，说明调制在相位部分的图像比调制在振幅部分的图像更易受噪声干扰，但两者的 MSE 均小于 2000，表明加密算法具有良好的抗噪声攻击能力。

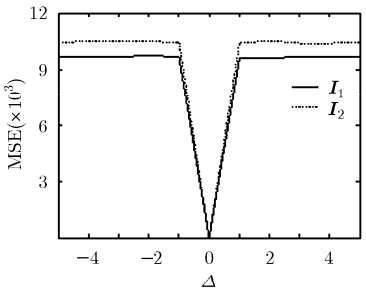


(a) p_1对应$\boldsymbol{I}_1$解密MSE曲线　　(b) p_2对应$\boldsymbol{I}_1$解密MSE曲线

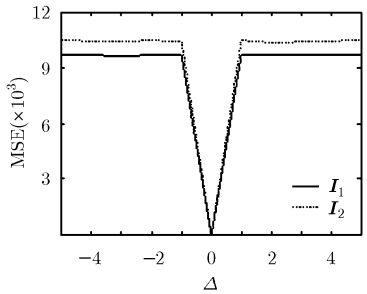
图 9 两种变换算法的安全性比较



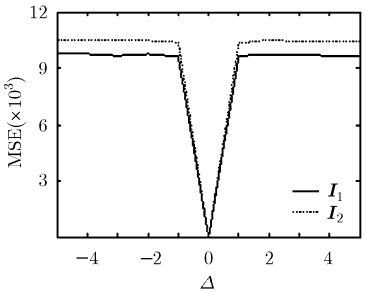
(a) x_0对应的解密MSE曲线



(b) a对应的解密MSE曲线

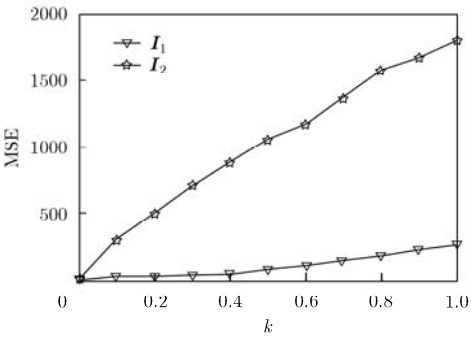


(c) c对应的解密MSE曲线



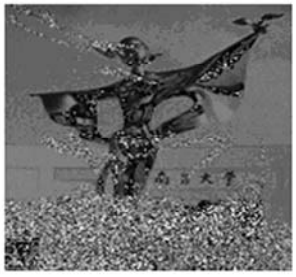
(d) M对应的解密MSE曲线

图 10 线性同余参数偏差量变化对应解密的 MSE 曲线



(a) k对应的MSE曲线

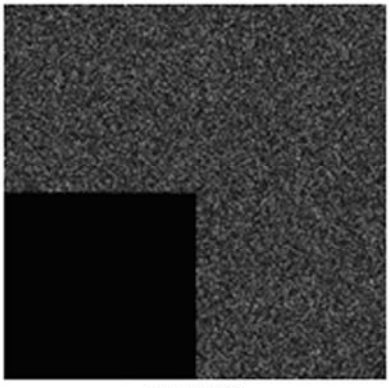
(b) k=0.5, $\boldsymbol{I}_1$的解密



(b) k=0.5, $\boldsymbol{I}_2$的解密

图 11 噪声攻击

图 12(a)为裁剪1/4后的加密图像，图 12(b)和 12(c)分别为裁剪攻击后 $\boldsymbol{I}_1$ 和 $\boldsymbol{I}_2$ 的解密图像。从模拟结果中可知，图像的大部分信息依旧能够恢复，该系统具有良好的抗裁剪攻击能力。



(a) 1/4裁剪

(b) $\boldsymbol{I}_1$的解密

(c) $\boldsymbol{I}_2$的解密

图 12 裁剪攻击

5 结论

本文基于离散分数随机变换设计了一种单通道无串扰的双彩色图像光学加密算法。加密系统满足密码学的混乱和扩散的原则，并且加密过程含有更换振幅操作，具有非线性加密性质，简单的密码分析不能破解此算法。结合线性同余理论对离散分数傅里叶变换的核矩阵进行了随机化，线性同余函数的 4 个参数增大了算法的密钥空间。利用变换后得到的复函数相位与分数域相位掩模的相位差值设计了相位密钥，并分析了相位密钥抵抗唯密文攻击的能力。数值分析了密钥的灵敏性和加密系统的抗噪声和裁剪攻击的能力，表明该双彩色图像加密算法具有较好的安全性。

参 考 文 献

[1] Joshi M, Shakher C, *et al*.. Color image encryption and decryption using fractional Fourier transform[J]. *Optics Communications*, 2007, 279(1): 35–42.

[2] Ge Fan, Chen Lin-fei, and Zhao Daomu. A half-blind color image hiding and encryption method in fractional Fourier domains[J]. *Optics Communications*, 2008, 281(17): 4254–4260.

[3] Chen Lin-fei and Zhao Dao-mu. Color image encoding in dual fractional Fourier-wavelet domain with random phases[J]. *Optics Communications*, 2009, 282(17): 3433–3438.

[4] Li Xin-xin and Zhao Dao-mu. Optical color image encryption with redefined fractional Hartley transform[J]. *Optik*, 2010, 121(7): 673–677.

[5] Guo Qing, Liu Zheng-jun, and Liu Shu-tian. Color image encryption by using Arnold and discrete fractional random transforms in IHS space[J]. *Optics and Lasers in Engineering*, 2010, 48(12): 1174–1181.

[6] Joshi M, Shakher C, *et al*.. Color image encryption and decryption for twin images in fractional Fourier domain[J]. *Optics Communications*, 2008, 281(23): 5713–5720.

[7] Joshi M, Shakher C, *et al*.. Fractional Fourier transform based image multiplexing and encryption technique for four-color images using input images as keys[J]. *Optics Communications*, 2010, 283(12): 2496–2505.

[8] 董太继, 周南润. 单通道彩色图像加密方案[J]. 光电子·激光, 2010, 21(10): 1542–1546.
Dong Tai-ji and Zhou Nan-run. An encryption scheme for single-channel color images[J]. *Journal of Optoelectronics. Laser*, 2010, 21(10): 1542–1546.

[9] Zhou Nan-run, Wang Yi-xian, *et al*.. Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform[J]. *Optics Communications*, 2011, 284(12): 2789–2796.

[10] Liu Zheng-jun, Liu Shu-tian, *et al*.. Image sharing scheme based on discrete fractional random transform[J]. *Optik*, 2010, 121(6): 495–499.

[11] Zhou Nan-run, Dong Tai-ji, and Wu Jian-hua. Novel image encryption algorithm based on multiple-parameter discrete fractional random transform[J]. *Optics Communications*, 2010, 283(15): 3037–3042.

[12] Tang Hui-chin. An analysis of linear congruential random number generators when multiplier restrictions exist [J]. *European Journal of Operational Research*, 2007, 182(2): 820–828.

[13] Wikramaratna R. Theoretical and empirical convergence results for additive congruential random number generators [J]. *Journal of Computational and Applied Mathematics*, 2010, 233(9): 2302–2311.

[14] Lang Jun, Tao Ran, and Wang Yue. Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function[J]. *Optics Communications*, 2010, 283(10): 2092–2096.

[15] Yamaguchi I and Zhang T. Phase-shifting digital holography [J]. *Optics Letters*, 1997, 22(16): 1268–1270.

[16] 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.
Peng Xiang, Tang Hong-qiao, and Tian Jin-dong. Ciphertext -only attack on double random phase encoding optical encryption system[J]. *Acta Physica Sinica*, 2007, 56(5): 2629–2636.

[17] Liu Zheng-jun, Dai Jing-min, *et al*.. Triple image encryption scheme in fractional Fourier transform domains[J]. *Optics Communications*, 2009, 282(4): 518–522.

张文全： 男，1969 年生，实验师，硕士，研究方向为光学图像加密.

周南润： 男，1976 年生，教授，博士，研究方向为信息安全、图像加密、量子通信.