基于混沌的改进双随机相位编码图像加密算法

朱 薇[1,2] 杨 庚[2] 陈 蕾[2] 陈正宇[2]

([1] 南京邮电大学理学院, 江苏 南京 210003
[2] 南京邮电大学宽带无线通信与传感网技术教育部重点实验室, 江苏 南京 210003)

摘要 针对菲涅耳域双随机相位编码提出的一种改进图像加密系统。该系统通过预先将原图像编码为相位信息克服了原算法对第一块相位模板和第一次衍射距离不敏感的缺陷。在双随机相位编码模块后基于复值图像振幅及相位替代的再次加密,使得加密图像像素值分布更为均匀。另外,改进算法引入三种不同的混沌系统来生成所需要的随机模板,借助于混沌系统的非线性性、初值敏感性,加密系统在减小密钥体积的同时增大了密钥空间、增加了系统的复杂性。仿真实验对算法进行了有效性分析、统计分析以及密钥敏感性测试,结果表明改进的算法有效提升了原算法的安全性。

关键词 傅里叶光学;图像加密;随机相位编码;菲涅耳衍射;混沌

中图分类号 TP309.7 **文献标识码** A **doi**: 10.3788/AOS201434.0607001

An Improved Image Encryption Algorithm Based on Double Random Phase Encoding and Chaos

Zhu Wei[1,2] Yang Geng[2] Chen Lei[2] Chen Zhengyu[2]

([1] *College of Science, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu* 210003, *China*
[2] *Key Laboratory of Broadband Wireless Communication and Sensor Network Technology of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu* 210003, *China*)

Abstract Aiming at the safety of double random phase encoding system in the Fresnel domain, an improved encryption algorithm is proposed. By means of the phase encoding in advance, the new system overcome the flaws of insensitivity to the first random phase mask and the first diffraction distance in original system. After the double random phase encoding module, the secondary encryption based on the amplitude-phase substitution of complex value image makes the pixel value distribution of encrypted image is more uniform. Random masks in the proposed algorithm are generated from three different chaotic systems. With the dynamics of chaotic systems, such as nonlinearity and sensitivity to initial values, the key volume is reduced, the key space is enlarged and complexity of the system is increased. Simulation is conducted on statistical analysis, correlation analysis and key sensitivity test. The experimental results show that the improved algorithm has higher security.

Key words Fourier optics; image encryption; random phase encoding; Fresnel diffraction; chaos

OCIS codes 070.4560; 070.7345; 070.2025

1 引 言

近年来,光学信息安全理论与技术因其固有的并行处理能力在大规模信息处理,尤其是图像、视频加密领域引起广泛关注,主要借助于光的衍射、干涉、成像、全息等过程对数据进行加密和信息隐藏[1-10]。1995 年,Refregier 等[1]提出了基于 4f 系

收稿日期: 2013-12-24; **收到修改稿日期**: 2014-02-12

基金项目: 国家 973 计划(2011CB302903)、国家自然科学基金(61272084,61202004,61202353)、江苏省自然科学基金(BK2011754)、江苏省高校自然科学研究重大项目(11KJA520002)、高等学校博士学科点专项科研基金(20113223110003,20093223120001)、中国博士后科学基金资助项目(2011M500095)、江苏省博士后科研资助计划项目(1102103C)

作者简介: 朱 薇(1980—),女,博士研究生,讲师,主要从事信息安全方面的研究。E-mail: zhuwei@njupt.edu.cn

导师简介: 杨 庚(1961—),男,博士,教授,主要从事信息安全方面的研究。E-mail: yangg@njupt.edu.cn

统的双随机相位编码算法，在其基础上产生了很多改进和衍生算法，如基于菲涅耳域的双随机相位编码系统（FDT-DRPE）[2]，虚拟透镜成像系统（VOI）[3]，基于分数傅里叶变换的双随机相位编码[4]等。傅里叶变换的线性本质使得双随机相位编码算法的安全性受到限制，彭翔等已经提出了已知明文攻击、选择明文攻击等破译算法[5]。近几年也出现了另外一些改进算法[11-19]，如 Liu 等[11-13]将混沌映射和光学变换相结合提出了一些新颖的加密算法。文献[11]将两幅待加密图像分别作为实部和虚部构成复值图像，对其进行 Gyrator 变换，对变换后的图像再利用混沌映射生成的随机二值矩阵进行编码，并且采用迭代的方式来增强算法的安全性。文献[12]提出了一种彩色图像的信息隐藏技术，首先通过 Baker 映射将彩色图像的三基色分量拼成一个单色分量，转换到球坐标系下再利用光学 Hartley 变换进行编码。文献[13]在一维分数傅里叶变换域利用 Baker 映射进行反复迭代加密，将输出的复值函数提取实数域内的振幅和相位两部分，分别作为加密系统的密文和密钥，便于存储和传输。文献[16]提出了一种基于傅里叶域的非线性操作的多图像加密方法，由于非线性操作，提高了算法的安全性。文献[17]设计了一个混合密码系统，采用两个双随机相位编码（DRPE）和两步相移干涉进行图像的加密，然后采用三个非对称密钥对进行会话密钥的加解密，这种方法可以解决密钥管理和调度的问题，增加安全强度。文献[19]采用两块独立的随机相位模板，提出了基于干涉原理的虚拟光学成像系统。但是，此类对称加密算法都以随机模板（与明文图像同规模）作为密钥，密钥体积太大，采用非对称加密来保护密钥安全，加密效率受到极大限制。另外，密文图像像素值分布不足够均匀，是该类算法的另外一个不足。就应用广泛的 FDT-DRPE 算法而言，还存在其他的安全问题，如在解密实值图像时完全不需要第一块随机相位模板便可通过 CCD 直接探测得到原图像[5]，并且解密算法对第一次菲涅耳衍射的距离也不敏感。

针对上述问题，本文基于 FDT-DRPE 提出了一种新的加密系统，借助于混沌理论来生成随机相位模板，解决密钥体积和密钥传递问题。另外，在双随机相位编码模块后对复值图像进行振幅相位的二次加密，使得密文像素值分布更加均匀，能够有效地抵御统计分析。同时，改进算法还克服了原 FDT-DRPE 系统对第一次衍射距离和第一块随机模板不敏感的缺陷。本文对所提算法进行了详细的安全性分析和仿真实验。

2　菲涅耳域的双随机相位编码系统

Situ 等[2]提出了 FDT-DRPE，如图 1 所示。

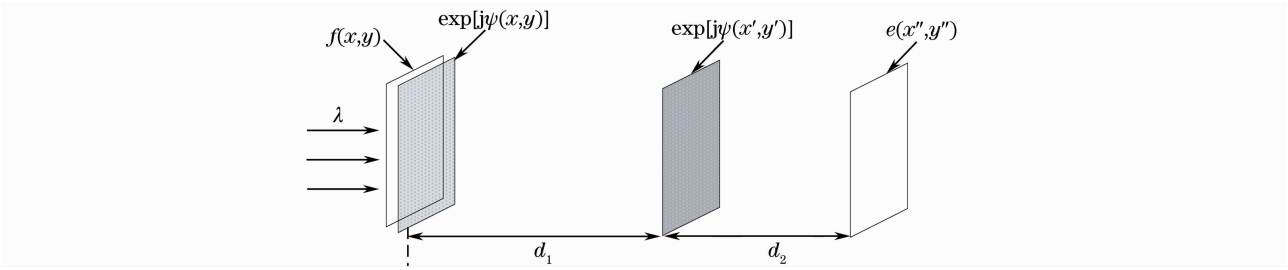

图 1　FDT-DRPE 加密系统

Fig. 1　Scheme of FDT-DRPE

该系统可以近似看作无透镜的 $4f$ 系统，其中使用两个相互独立的随机相位模板对图像进行调制，最终在输出平面得到的加密结果类似白噪声。加密过程可以描述为：原始图像 $f(x,y)$ 与相位模板 $R_{\mathrm{RM1}}(x,y)$ 相乘的结果经距离为 d_1 的菲涅耳衍射变换（FDT）后，与相位模板 $R_{\mathrm{RM2}}(x',y')$ 相乘，然后再做距离为 d_2 的 FDT，就得到了最终的加密结果 $e(x'',y'')$。其中 $R_{\mathrm{RM1}}(x,y)=\exp[\mathrm{j}\psi(x,y)]$，$R_{\mathrm{RM2}}(x',y')=\exp[\mathrm{j}\varphi(x',y')]$。$\psi(x,y)$ 和 $\varphi(x',y')$ 是两个均匀分布于 $[0,2\pi]$ 的独立白噪声序列，整个加密过程可以用以下公式表示：

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

式中 $f(x,y)$ 为原始图像，$F_{\mathrm{FDT\_}d}[\cdot]$ 表示距离为 d 的菲涅耳衍射变换，其展开式为

$$F_{\mathrm{FDT\_}d}[f(x',y')]=\frac{\exp(\mathrm{j}kd)}{\mathrm{j}\lambda d}\iint_{-\infty}^{+\infty}f(x,y)\exp\left\{\mathrm{j}\frac{\pi}{\lambda d}[(x'-x)^2+(y'-y)^2]\right\}\mathrm{d}x\mathrm{d}y=$$

$$\frac{\exp(\mathrm{j}kd)}{\mathrm{j}\lambda d}\exp\left\{\mathrm{j}\frac{\pi}{\lambda d}(x'^2+y'^2)\right\}\cdot\mathscr{F}\left\{f(x,y)\exp\left[\mathrm{j}\frac{\pi}{\lambda d}(x^2+y^2)\right]\right\},\tag{2}$$

式中 λ 为波长，$k=\frac{2\pi}{\lambda}$ 为波数，$\mathscr{F}$ 表示傅里叶变换。

在加密系统中两次菲涅耳衍射的距离是任意的，衍射结果对照射光的波长敏感，因此在加密系统中衍射距离和光波波长都可以作为密钥，由此 FDT-DRPE 系统的多维密钥为 $(\lambda,d_1,d_2,R_{\mathrm{RM1}},R_{\mathrm{RM2}})$，较之 $4f$ 系统有更大的密钥空间，增强了系统的安全性。

解密是对加密的逆过程，可以表示为

$$f_{\mathrm{D}}(x,y)=F_{-d_1}\{F_{-d_2}[e(x'',y'')]R^{*}_{\mathrm{RM2}}(x',y')\}\times R^{*}_{\mathrm{RM1}}(x,y),\tag{3}$$

式中 R^{*}_{RM2}，R^{*}_{RM1} 分别代表两个随机相位模板的复共轭，$-d_1$，$-d_2$ 表示衍射距离。

3　相关混沌系统

非线性科学领域的混沌因其特有的伪随机性、遍历性和初值敏感性等特性被广泛的应用于信息安全领域。利用混沌系统，可以产生数量众多、非相关、类似噪声、又可以再生的混沌序列，将混沌序列进行适当的预处理便可生成指定取值范围内的伪随机序列，应用于密码编码和保密通信领域[20-22]。下面简单介绍用于生成随机模板的三种混沌系统。

3.1　Logistic 映射

Logistic 映射[21]是个简单而重要的非线性动力系统。其映射方程为

$$x_{n+1}=\mu x_n(1-x_n),\quad x_n\in[0,1].\tag{4}$$

当参数 $\mu\in(3.5699456,4]$ 时，Logistic 映射处于混沌状态。对任意的初值 x_0，经过(4)式的迭代产生的序列是非周期、长期不可预测的，并且 μ 越接近于 4，混沌序列在[0,1]区间内分布越均匀。

3.2　基于耦合帐篷映射的时空混沌

时空混沌是一种在时间和空间方向上都具有混沌行为的非线性动力系统，该二维系统有更好的混沌特性。一般情况下，可以使用耦合常微分方程、元胞自动机、耦合映像格子等模型来构造时空混沌的在时间和空间上的混沌行为。使用基于耦合帐篷映射的时空混沌系统，其数学模型为耦合映像格子模型[22]

$$x^{i}_{n+1}=(1-\varepsilon)f(x^{i}_{n})+\frac{\varepsilon}{2}[f(x^{i-1}_{n})+f(x^{i+1}_{n})],\tag{5}$$

式中 $\varepsilon\in(0,1)$ 为耦合系数，$n=0,1,2,\cdots$ 为离散时间步数，$i=1,2,\cdots,L$ 为离散点坐标(L 为格子数，由系统大小决定)，x^{i}_{n} 表示第 i 个格子在 n 时刻的状态。$f(x)$ 为格子的局部状态演化方程，这里采用帐篷混沌映射

$$f(x^{i})=\begin{cases}\dfrac{x^{i-1}}{\alpha}, & 0\leqslant x^{i-1}<\alpha\\[2ex] \dfrac{1-x^{i-1}}{1-\alpha}, & \alpha\leqslant x^{i-1}\leqslant 1\end{cases},\tag{6}$$

式中帐篷映射参数 $\alpha\in(0,1)$，取 $\alpha=0.4$。

系统按时间步数迭代，边界条件为 $x^{L}_{n}=x^{0}_{n}$，初始时刻状态 $x^{0}_{0},x^{1}_{0},\cdots,x^{L}_{0}$，采用 Logistic 映射产生，即 $x^{i}_{0}=f_{\mathrm{Logistic}}(x_0,\mu)$，其中 x_0 为初值，μ 为参数。文献[22]表明，当耦合系数 ε 的取值小于 0.01 时，基于耦合帐篷映射的时空混沌系统可以生成具有均匀分布的混沌序列。

3.3　Chen 系统

Chen 系统是在对 Lorenz 系统研究的基础上由 Chen 等[23]提出的，可以用如下非线性微分方程组来描述：

$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=(c-a)x-xz+cy\\ \dot{z}=xy-bz\end{cases},\tag{7}$$

式中 x,y,z 是状态变量，a,b,c 是三个系统参数. 当 $a=35,b=3,c\in[20,28.4]$ 时，系统处于混沌状态。变量 y 前的参数 c 使得 Chen 系统比著名的 Lorenz 混沌系统具有更复杂的动力学特性，适合用于安全通信。采用文献[24]的方法将混沌输出序列进行预处理，生成随机相位模板。

4　基于混沌的 FDT-DRPE 和像素值替代相结合的加密算法

4.1　算法基本思想

提出的改进图像加密算法结合了菲涅耳衍射，混沌伪随机序列和图像像素值替代等几方面的理论。图 2 为加密系统的算法框图，主要分为两大模块：FDT-DRPE 模块和像素值替代模块。原图像 U_0 首先被编码为复值图像，然后经 FDT-DRPE 模块后得到图像 U_1，图像 U_1 再经过像素值替代模块

后得到最终的密文图像 U_2。如图 2 所示，可以把加密系统的多维密钥分为四个部分：Key-Ⅰ；Key-Ⅱ；Key-Ⅲ；Key-Ⅳ。其中 Key-Ⅰ，Key-Ⅱ，Key-Ⅲ分别代表三个混沌系统的初值和参数密钥；Key-Ⅳ＝(λ，d_1，d_2)为 FDT-DRPE 模块的光学密钥，包含衍射光波波长 λ 和两次衍射距离 d_1，d_2。

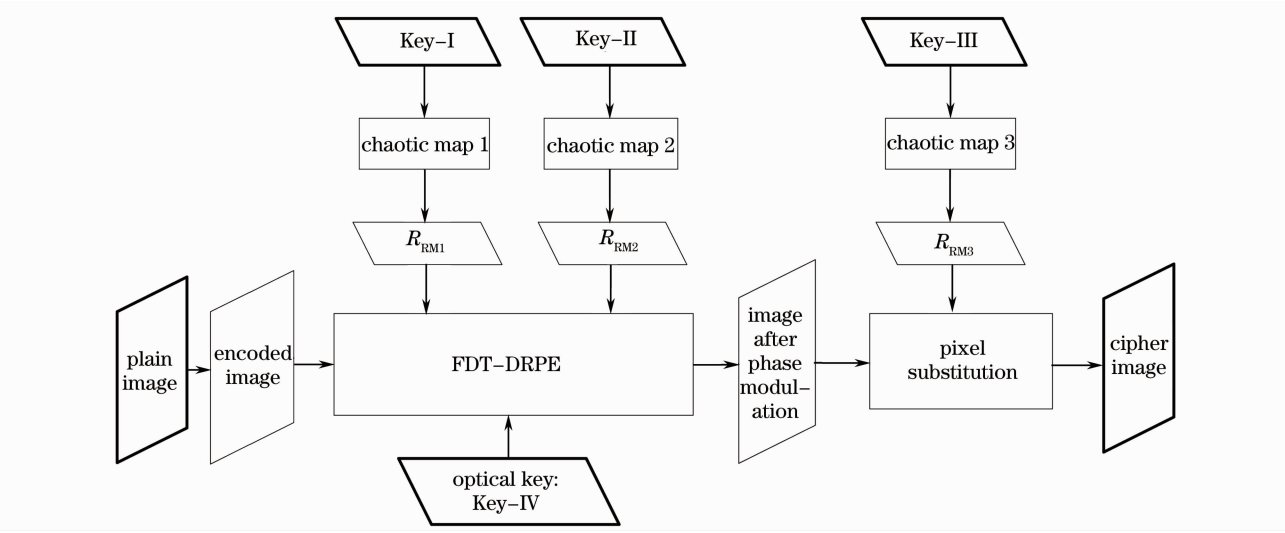

图 2　改进加密系统的算法框图

Fig. 2　Scheme of proposed system

4.2　算法描述

分别采用 Logistic 映射和 Chen 系统构造两块随机相位模板(R_{RM1}，R_{RM2})，采用时空混沌映射来构造像素值替代模板 R_{RM3}，R_{RM1} 和 R_{RM2} 是[0，2π]上均匀分布的噪声矩阵，R_{RM3} 是[0，1]上均匀分布的随机矩阵。由于经过 FDT-DRPE 模块后的图像 U_1 是复值图像，不能采用对实值图像的按位“异或”方法进行像素值替代。在这里对 U_1 提取其振幅和相位，分别进行替代操作，并且在振幅替代过程中采用的非线性操作有助于抵御选择明文攻击。具体加密算法如下所述：

输入：待加密图像 U_0；多维密钥：(Key-Ⅰ；Key-Ⅱ；Key-Ⅲ；Key-Ⅳ)＝(μ_1，I_{01}；x_0，y_0，z_0，c；I_{02}，μ_2，ε；λ，d_1，d_2)。

输出：加密后图像 U_2。

1) 将 U_0 进行相位编码：$U_0'=\exp(\mathrm{j}U_0)$；

2) 根据密钥 Key-Ⅰ和 logistic 混沌映射构建随机相位模板 R_{RM1}；

3) 根据密钥 Key-Ⅱ和 Chen 混沌系统构建随机相位模板 R_{RM2}；

4) 根据 R_{RM1}、R_{RM2} 和 Key-Ⅳ计算 U'_0 经过 FDT-DRPE 加密后的图像 U_1；

5) 根据密钥 Key-Ⅲ和时空混沌系统构造随机替代矩阵 R_{RM3}；

6) 提取复值图像 U_1 的归一化振幅 M_1 及相位 P_1，根据 R_{RM3} 进行振幅和相位替代操作，得到新的振幅和相位：

$$M_1'=[M_1\times 255+(R_{RM3}\times 255)^2]\bmod 255, \tag{8}$$

$$P_1'=P_1+R_{RM3}\times 2\pi. \tag{9}$$

7) 输出加密后图像为 $U_2=M_1'\exp(\mathrm{j}P_1')$。

解密是加密的逆过程，其具体解密算法描述如下：

输入：密文图像 U_2；多维密钥：(Key-Ⅰ；Key-Ⅱ；Key-Ⅲ；Key-Ⅳ)＝(μ_1，I_{01}；x_0，y_0，z_0，c；I_{02}，μ_2，ε；λ，d_1，d_2)。

输出：解密后图像 U_4。

1) 根据密钥 Key-Ⅲ和时空混沌系统生成随机振幅替代矩阵 R_{RM3}；

2) 提取密文图像 U_2 的振幅和相位，根据 R_{RM3} 恢复替代前的振幅 M' 和相位 P'；

3) 恢复经随机相位编码后的图像为 $U_3=M'\exp(\mathrm{j}P')$；

4) 根据密钥 Key-Ⅰ和 Logistic 混沌映射构建随机相位模板 R_{RM1}；

5) 根据密钥 Key-Ⅱ和 Chen 混沌系统构建随机相位模板 R_{RM2}；

6) 根据 U_3、R_{RM1}、R_{RM2} 和密钥 Key-Ⅳ经过逆菲涅耳变换恢复编码后的原图像为 $U'_4=F_{\mathrm{FDT}\text{-}d_1}\cdot[F_{\mathrm{FDT}\text{-}d_2}(U_3)R^*_{RM2}]R^*_{RM1}$；

7) 获得解密图像 U_4 为 $U_4=\arccos[\mathrm{Re}(U'_4)]$。

5　仿真及安全性分析

使用 Matlab2010 来进行系统仿真，测试图像共有 6 幅标准灰度图，分别为 lena. png，twodim. png，peppers. tiff，camera. tiff，plane. tiff 和 mandrill. tiff。加密系统的多维密钥参数对应为

$$(\mu_1, x_{01}; x_0, y_0, z_0, c; x_{02}, \mu_2, \varepsilon; \lambda, d_1, d_2) = (3.999, 0.5372; 0, 1, 0.28; 0.3875, 4, 0.001; 633\times10^{-9}, 4, 3). \tag{10}$$

对 Chen 系统的数值求解采用四阶古典 Runge-Kutta 方法，步长 $h=0.001$。

5.1　加解密算法有效性分析

图 3 显示了分别由 Logistic 映射、Chen 系统和时空混沌映射所构建的三个随机模板以及它们的直方图。可以看出生成的两块相位模板是相互独立的[0,2π]上均匀分布的噪声序列。振幅相位替代模板是[0,1]上均匀分布的随机噪声序列。

图 4 以二维码和 Lena 图为例展示了算法的加解密效果。从图4(b)和(e)可以看出加密图像类似

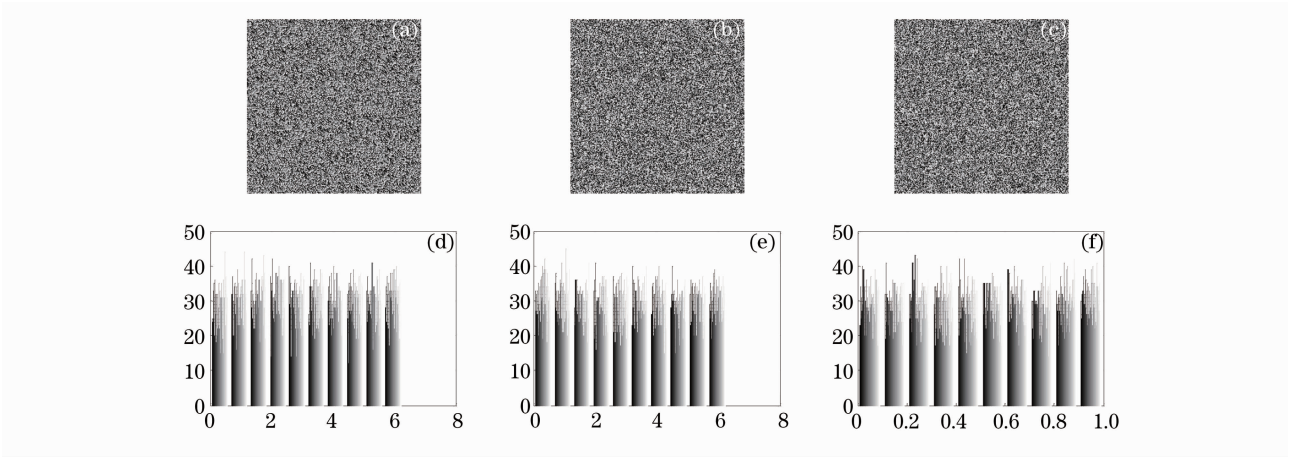

图 3　随机相位调制模板和振幅替代模板。(a)模板 R_{RM1}；(b)模板 R_{RM2}；(c)模板 R_{RM3}；(d) R_{RM1} 的直方图；(e) R_{RM2} 的直方图；(f) R_{RM3} 的直方图

Fig. 3　Random phase masks, substitution mask and histograms. (a) R_{RM1}; (b) R_{RM2}; (c) R_{RM3}; (d) histogram of R_{RM1}; (e) histogram of R_{RM2}; (f) histogram of R_{RM3}

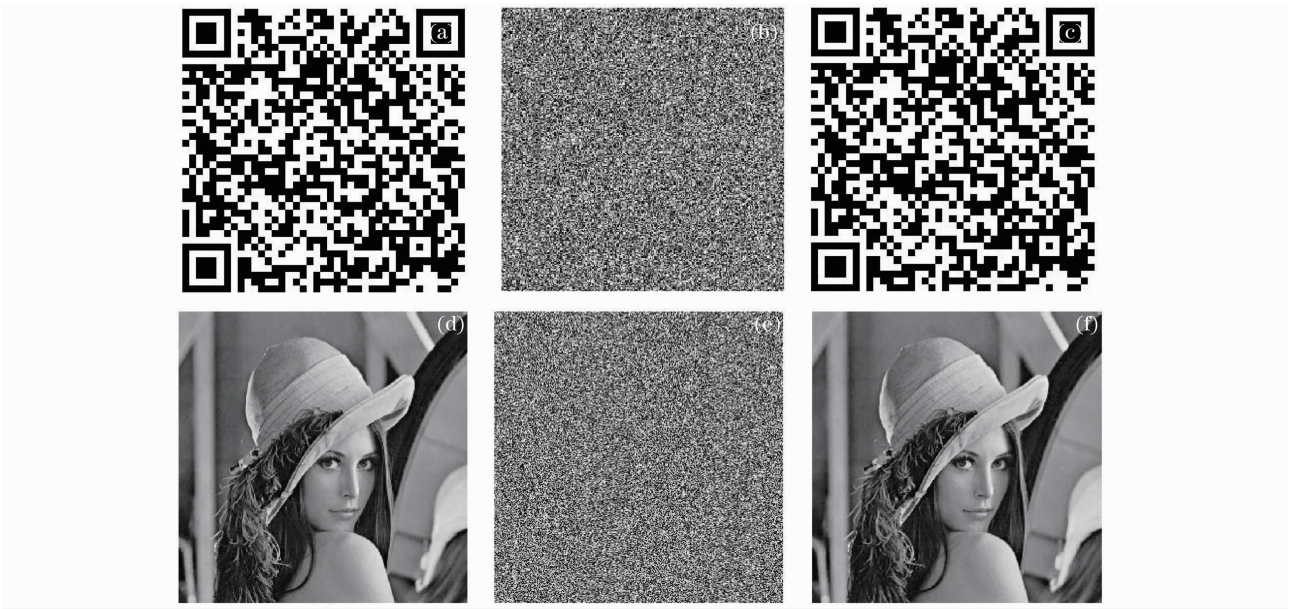

图 4　算法加解密效果图。(a)和(d)为二维码和 Lena 原图；(b)和(e)为相应的加密图像；(c)和(f)为相应的解密图像

Fig. 4　Performance of the proposed system. (a) Original twodim; (b) cipher image of Fig. 4(a); (c) decrypted image of Fig. 4(b); (d) original Lena; (e) cipher image of Fig. 4(d); (f) decrypted image of fig. 4(e)

噪声，完全看不出原图信息，图 4(c)和(f)则说明解密算法可以正确恢复原图像。

5.1.1　均方误差和相关系数

解密图像和原图像的均方误差 f_{MSE} 及相关系数 C 常被用来客观评价图像解密效果，其定义为

$$f_{\mathrm{MSE}}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(A_{ij}-B_{ij})^2, \tag{11}$$

$$C=\frac{\left|\sum_{i=1}^{M}\sum_{j=1}^{N}(A_{ij}-\overline{A})(B_{ij}-\overline{B})\right|}{\sqrt{\left[\sum_{i=1}^{M}\sum_{j=1}^{N}(A_{ij}-\overline{A})^2\right]\left[\sum_{i=1}^{M}\sum_{j=1}^{N}(B_{ij}-\overline{B})^2\right]}}, \tag{12}$$

式中 $\boldsymbol{A}$，$\boldsymbol{B}$ 分别表示大小为 $M\times N$ 的原图像和解密图像矩阵，A_{ij}，B_{ij} 代表对应 (i,j) 位置处的像素值，$\overline{A}$、$\overline{B}$ 表示矩阵 $\boldsymbol{A}$，$\boldsymbol{B}$ 的平均值。

由以上定义可知，均方误差 f_{MSE} 越接近于 0，相关系数 C 越接近 1，$\boldsymbol{A}$ 和 $\boldsymbol{B}$ 的相似度就越大，算法的解密效果越好；反之则说明算法解密效果不好。

表 1 对比了文献[3,17,19]和算法的解密图像与原图的均方误差和相关系数。从中可以看出给出的算法解密效果明显优于文献[3]中的 VOI 加密系统，与文献[17,19]的解密效果相当。

表 1　解密图像与原图的相似性

Table 1　Similarity of decrypted image and original image

Image	Relationship between decrypted image and original image							
	C				f_{MSE}			
	Ref.[3]	Ref.[17]	Ref.[19]	Proposed	Ref.[3]	Ref.[17]	Ref.[19]	Proposed
Camera	0.90590	1.00000	1.00000	0.99999	1.18×10^{-2}	1.94×10^{-4}	2.10×10^{-4}	1.53×10^{-6}
Peppers	0.95758	0.99987	1.00000	1.00000	8.28×10^{-3}	1.15×10^{-5}	4.04×10^{-3}	4.05×10^{-3}
Lena	0.95553	1.00000	1.00000	1.00000	5.86×10^{-3}	2.51×10^{-5}	2.20×10^{-3}	4.10×10^{-7}
Mandrill	0.71891	0.99998	1.00000	1.00000	2.00×10^{-2}	5.68×10^{-3}	8.64×10^{-3}	5.66×10^{-3}
Twodim	0.67802	1.00000	0.99996	1.00000	1.59×10^{-1}	7.64×10^{-6}	3.76×10^{-5}	7.97×10^{-6}
Plane	0.92796	0.99988	1.00000	1.00000	2.14×10^{-2}	1.37×10^{-3}	2.06×10^{-2}	1.53×10^{-2}

5.1.2　稳健性分析

图像加密算法面对数据损失和噪声的稳健性也是加密算法性能的一个重要衡量指标，选取“辣椒”图像对所提算法做了相应的稳健性测试，对部分损失和添加噪声的密文图像进行解密，解密结果如图 5 所示。图 5(a)为密文数据损失左上角 64×64 子块后解密的图像，图 5(b)为添加均值为 0，方差为 1 的高斯噪声后的解密图像，图 5(c)和(d)中添加的分别是浓度分别为 0.02 和 0.2 的椒盐噪声。图 5 显示的解密结果均能分辨出原图的基本轮廓，说明本算法具有一定的稳健性。不难看出，其中密文图像部分损失时解密效果相对较弱，但是本算法对椒盐噪声有着较好的抵抗能力，尤其是当椒盐噪声的浓度达到 0.2 时，解密图像与原图相关系数仍为 0.1822，解密图像可以辨认出原图的轮廓。

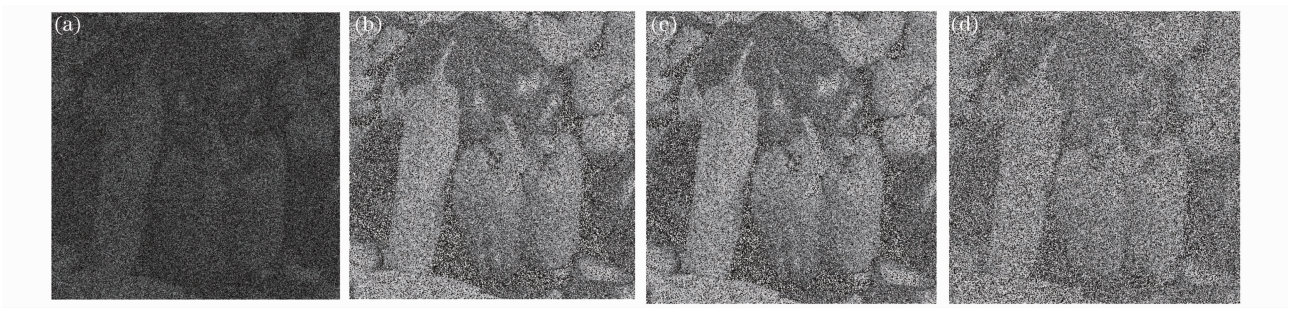

图 5　密文损失和噪声攻击测试。(a)数据损失后恢复的图像；(b)加高斯噪声后恢复的图像；(c)添加浓度为 0.02 椒盐噪声后恢复的图像；(d)添加浓度为 0.2 椒盐噪声后恢复的图像

Fig. 5　Occlusion and noise attack. Recovered images from (a) occlusion; (b) Gaussian noise; (c) salt & pepper noise with density of 0.2 and (d) salt & pepper noise with density of 0.2

5.2　安全性分析

对提出的算法从直方图，相邻像素相关性，信息熵，密钥敏感性，密钥空间等几个方面进行了全面的安全性分析。

5.2.1　直方图

直方图是反映图像灰度值分布统计特性的一个重要形式化指标，加密图像直方图越平坦说明图像像素值分布越均匀，留给密码分析者的分析空间就越小。

图 6 对比了经典的 $4f$ 系统，文献[19]的算法和本文算法的加密结果，可以看出 $4f$ 系统和文献[19]加密后图像像素值分布比原图像更加平坦，但是并不均匀，而本文给出的算法密文图像对应的直方图像素分布最为均匀，在混淆原图像的统计特征方面效果最好。

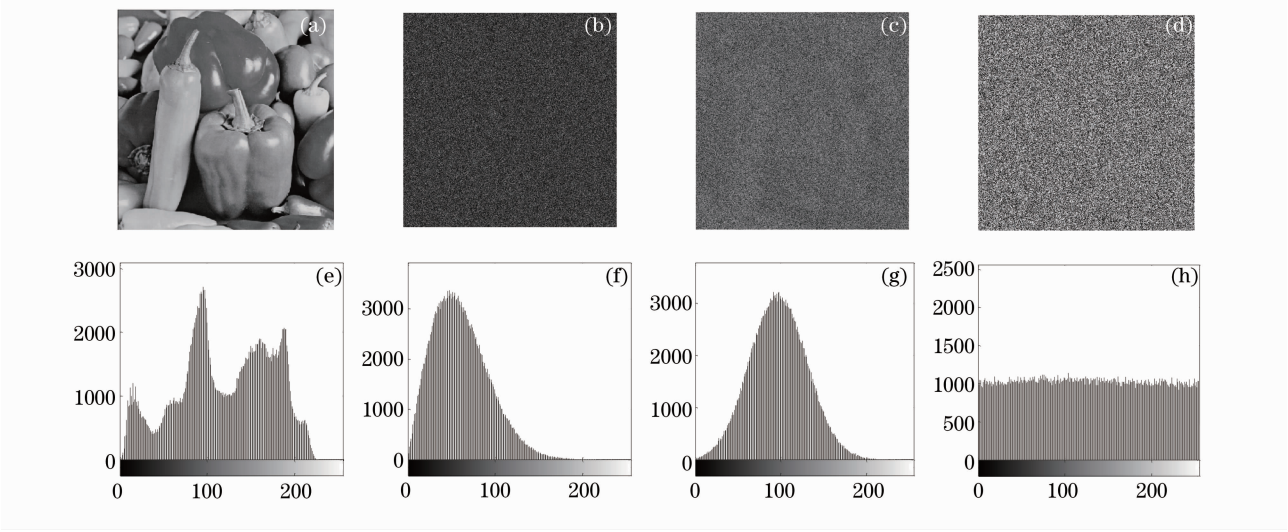

图 6　几种方法的对比。(a) peppers 原图；(b) $4f$ 系统加密图；(c) Ref.[19]加密图；(d)本文加密图；(e)～(h)分别为(a)～(d)的相应的灰度直方图

Fig. 6　Comparison of several methods. (a) Original peppers; (b) cipher image of $4f$; (c) cipher image of Ref.[19]; (d) cipher image of proposed system; (e)～(h) are corresponding histograms of (a)～(d) respectively

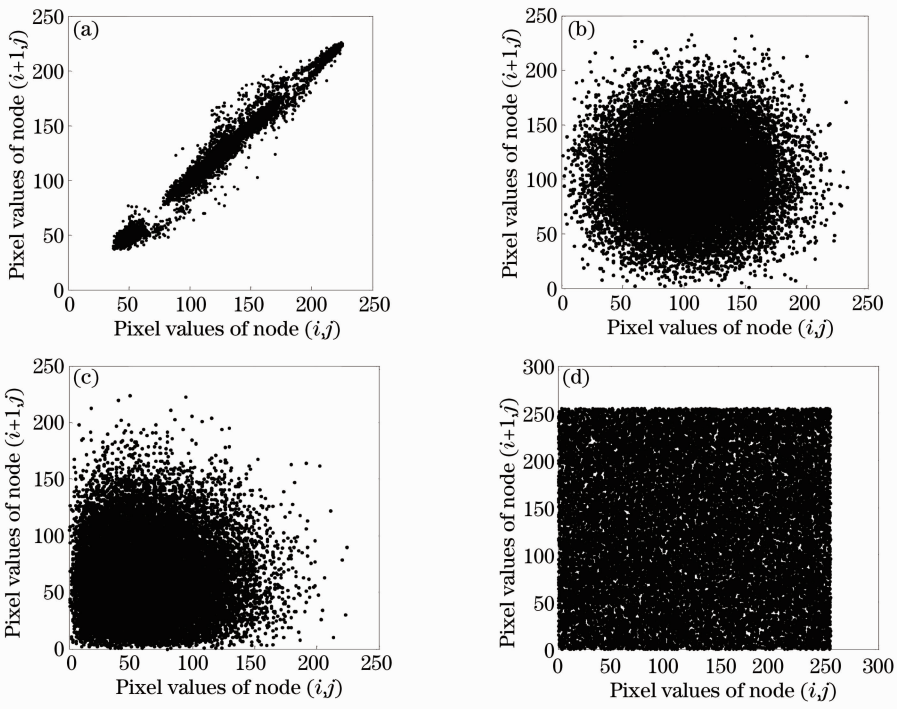

图 7　Lena 图的垂直方向相邻像素分布图.(a)原始 Lana 图；(b) VOI 加密图；(c) FDT-DRPE 加密图；(d)本文提出的系统的加密图

Fig. 7　Gray values distribution of vertically adjacent pixels in plain image and cipher image. (a) Original Lena; (b) cipher Lena of VOI; (c) cipher Lena of FDT-DRPE; (d) cipher Lena of proposed system

5.2.2　相邻像素相关性

数字图像的一个显著特征就是相邻像素的相关性高，因此好的加密算法应该能显著破坏相邻像素的相关性。图 7 以 Lena 图的垂直方向为例直观地显示了加密前后相邻像素点像素值之间关系的转变，图中的点分别以相邻两点的像素值作为横坐标和纵坐标。图 7(a)中的点都集中在坐标面的对角线周围，说明各点的纵、横坐标几乎相等，即原图中相邻点的像素值几乎相等，相关性很强。图 7(b)～(d)中的点均匀散落在坐标面上，各点的纵、横坐标之间没有明显关系，说明加密后图像相邻点像素值相关性低。对比图 7(b)～(d)可以发现，本文算法像素值的分布比 VOI 和 FDT-DRPE 加密系统更加均匀，扩散性更好。

引入相邻像素值向量之间的相关系数来明确图像相邻像素之间的相关程度，其计算方法如下：

$$r_{xy}=\frac{|C_{ov}(\boldsymbol{x},\boldsymbol{y})|}{\sqrt{D(\boldsymbol{x})}\sqrt{D(\boldsymbol{y})}},\tag{13}$$

$$E(\boldsymbol{x})=\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{x}_i,\tag{14}$$

$$D(\boldsymbol{x})=\frac{1}{N}\sum_{i=1}^{N}[\boldsymbol{x}_i-E(\boldsymbol{x})]^2,\tag{15}$$

$$C_{ov}(\boldsymbol{x},\boldsymbol{y})=\frac{1}{N}\sum_{i=1}^{N}[\boldsymbol{x}_i-E(\boldsymbol{x})][\boldsymbol{y}_i-E(\boldsymbol{y})].\tag{16}$$

式中 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 分别表示图像中相邻像素点的像素值所对应的两个向量，r_{xy} 代表 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的相关系数。表 2 所列为原始图像和加密后图像按垂直、水平、对角三个不同方向的相邻像素值向量之间的相关系数，由表 2 可见，原图像的相邻像素相关系数都很高，接近于 1，而加密后图像的相邻像素相关系数都接近于 0，这说明加密算法从垂直，水平，对角三个方向上都有效的破坏了原图的相邻像素相关性，掩盖了原图的统计特性。

5.2.3　信息熵

信息熵是度量信息有序性的一个重要手段，一个系统越是混乱信息熵就越高，对于 8-bit 的灰度图像来说，其计算方法为

$$H(s)=-\sum_{i=0}^{2^8-1}P(s_i)\mathrm{lb}[P(s_i)],\tag{17}$$

式中 $P(s_i)$ 代表灰度值 i 出现的概率。图像像素值分布越均匀，信息熵就越大，最大值为 8。表 3 对比了用几种不同算法加密的 Lena 图像的信息熵，可以看出本文提出的算法信息熵最接近于 8，密文像素值分布最均匀，加密效果最好。

表 2　原始图像与加密图像的相邻像素相关系数

Table 2　Correlation coefficients of adjacent pixels in plain image and cipher image

Image	Correlation coefficients					
	Vertical		Horizontal		Diagonal	
	Plain image	Cipher image	Plain image	Cipher image	Plain image	Cipher image
Camera	0.95922	0.00433	0.93348	0.00051	0.90866	0.00629
Peppers	0.97913	0.00104	0.97669	0.00164	0.96385	0.00235
Lena	0.98498	0.00140	0.97187	0.00010	0.95927	0.00144
Mandrill	0.75870	0.00275	0.86650	0.00139	0.72614	0.00159
Plane	0.96409	0.00027	0.96630	0.00158	0.93700	0.00121

表 3　Lena 加密图像的信息熵

Table 3　Entropy of cipher Lena

Entropy	Algorithms				
	Proposed	Ref.[2]	Ref.[3]	Ref.[19]	Ref.[20]
	7.9973	7.0253	7.0921	7.1327	7.9965

5.2.4　密钥敏感性分析

如图 8(a)所示，原 FDT-DRPE 系统在解密时，若原图为实值图像，即使相位模板 R_{RM1} 错误，经强度探测器，也可解密图像。另外，对衍射距离 d_1 也不敏感，图 8(b)为 d_1 错误时的解密图像。图 8(c)，(d)分别是 R_{RM2} 和 d_2 错误时的解密图像，说明 FDT-DRPE 算法对第一块随机模板和第一段衍射距离不敏感，对第二块模板和第二段衍射距离敏感。好的加密系统要求对密钥敏感，即密钥出现较小偏差时不能正确解密图像。依据这一原则 FDT-DRPE 算法具有安全隐患。

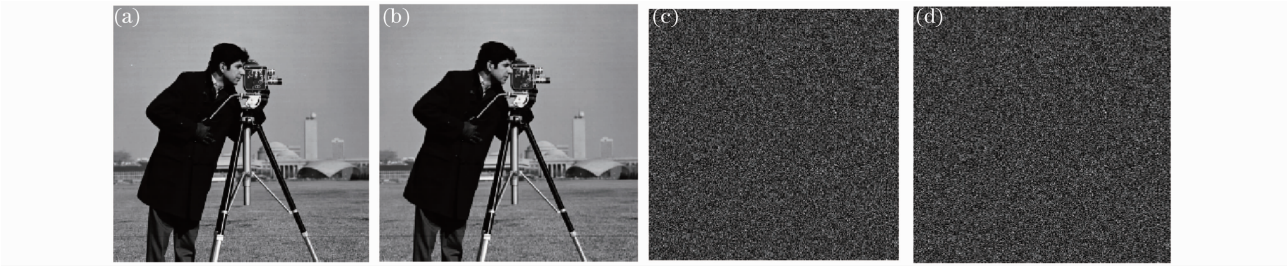

图 8　原 FDT-DRPE 算法的解密图像。(a) R_{RM1} 错误；(b) d_1 错误；(c) R_{RM2} 错误；(d) d_2 错误

Fig. 8　Decrypted images in FDT-DRPE (a) with wrong R_{RM1}; (b) with wrong d_1; (c) with wrong R_{RM2}; (d) with wrong d_2

改进后的混合加密算法对所有密钥参数均具有高度灵敏性。图 9(a),(b)表明构建第一块随机相位模板的 Key-Ⅰ中 Logistic 系统的初值密钥 μ_1 在偏差为 $\Delta\mu_1=10^{-15}$ 时不能正确解密，而偏差 10^{-16} 时能恢复原图像。因此可以说改进算法克服了 FDT-DRPE 系统对第一块随机相位模板不敏感的缺点。图 9(c),(d)表明 Key-Ⅲ中时空混沌系统的耦合系数密钥 ε 在偏差 $\Delta\varepsilon=10^{-18}$ 时仍不能解密图像，直至 $\Delta\varepsilon=10^{-19}$ 时才能正确解密图像。可以认为 x_0 和 ε 的灵敏度分别为 10^{-15} 和 10^{-18}，同理可得三个混沌系统中的其他密钥参数灵敏度均为 10^{-15}。图 10～12 则给出了 Key-Ⅳ中照射光波长 λ 和衍射距离 d_1，d_2 存在偏差时的解密效果图，可以看出波长的灵敏度为 10^{-11}，衍射距离 d_1 的灵敏度也为 10^{-3}，d_2 灵敏度为 10^{-4}。

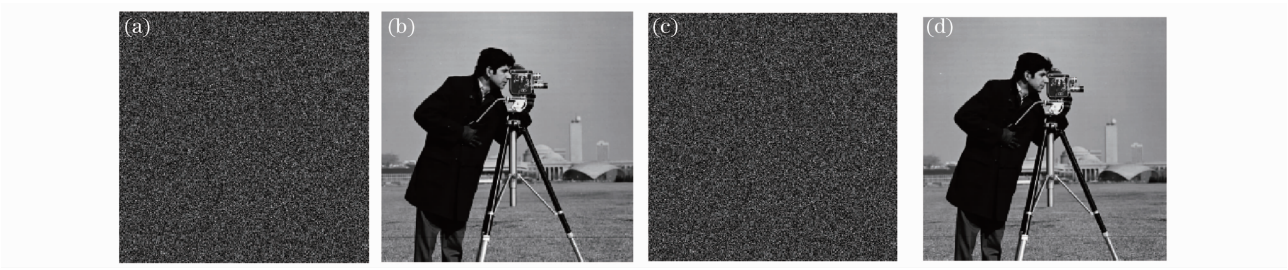

图 9　混沌系统初值偏差时的解密图像。(a) $\Delta\mu_1=10^{-15}$；(b) $\Delta\mu_2=10^{-16}$；(c) $\Delta\varepsilon=10^{-18}$；(d) $\Delta\varepsilon=10^{-19}$

Fig. 9　Decrypted images with deviation in initial values of chaos. (a) $\Delta\mu_1=10^{-15}$; (b) $\Delta\mu_2=10^{-16}$; (c) $\Delta\varepsilon=10^{-18}$; (d) $\Delta\varepsilon=10^{-19}$

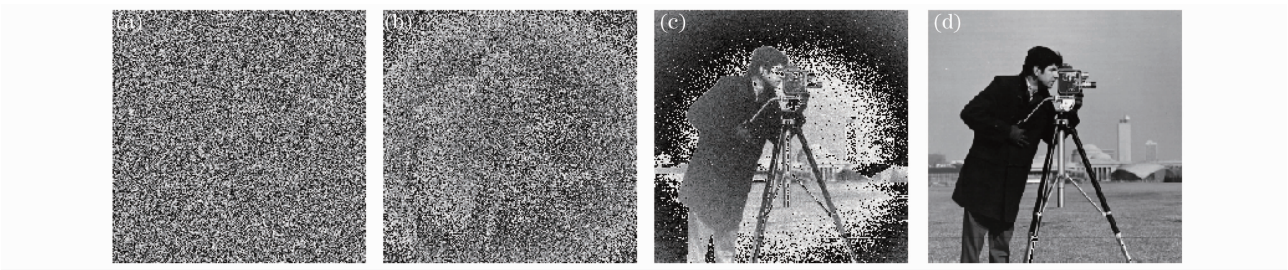

图 10　波长 λ 偏差时的解密图像。(a) $\Delta\lambda=10^{-10}$；(b) $\Delta\lambda=10^{-11}$；(c) $\Delta\lambda=10^{-12}$；(d) $\Delta\lambda=10^{-13}$

Fig. 10　Decrypted images with deviation in wavelength. (a) $\Delta\lambda=10^{-10}$; (b) $\Delta\lambda=10^{-11}$; (c) $\Delta\lambda=10^{-12}$; (d) $\Delta\lambda=10^{-13}$

5.2.5　密钥设计和密钥空间

加密系统的密钥维数多，密钥精度高，必然会产生较大的密钥空间。基于以上密钥敏感性分析，各参数的取值范围和 Matlab 双精度浮点数的有限精度，加密系统中混沌密钥参数 μ_1，x_{01}；x_0，y_0，z_0，c；x_{02}，μ_2，ε 均可以达到浮点数的最高精度 10^{-16}，忽略混沌系统参数整数部分的区分度，密钥空间为中混沌密钥的种类仍可达$(10^{15})^9$。将 λ 设为 $s_1s_2s_3.t_1t_2\times10^{-9}$，$d_1$，$d_2$ 设定为 $p.q_1q_2q_3$，则光学密钥参数 λ，d_1，d_2 的可能取值至少达到$(10^3)^3$ 种，因此整个密钥空间的大小至少达到$(10^{15})^9\times(10^3)^3=10^{144}\approx2^{478}$，相当于 478 位二进制密钥的空间大小。故本算法足以

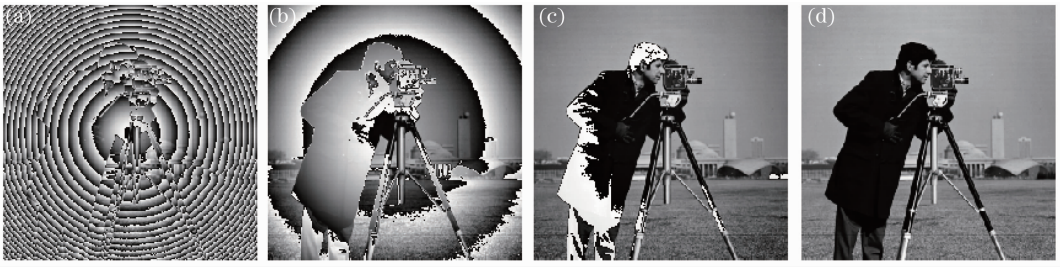

图 11　d_1 偏差时的解密图像。(a) $\Delta d_1=10^{-3}$；(b) $\Delta d_1=10^{-4}$；(c) $\Delta d_1=10^{-5}$；(d) $\Delta d_1=10^{-6}$

Fig. 11　Decrypted images with deviation in d_1. (a) $\Delta d_1=10^{-3}$; (b) $\Delta d_1=10^{-4}$; (c) $\Delta d_1=10^{-5}$; (d) $\Delta d_1=10^{-6}$

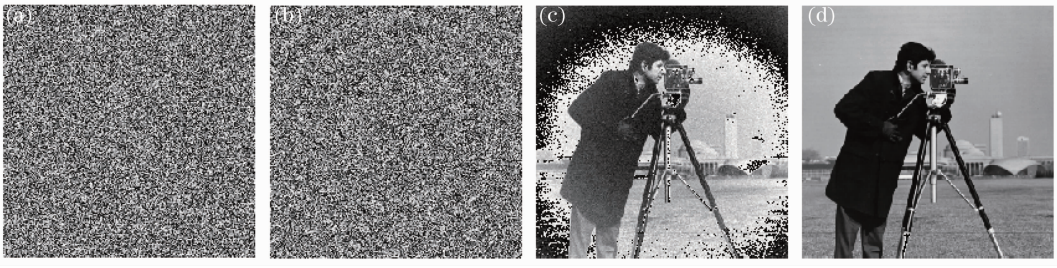

图 12　d_2 偏差时的解密图像。(a) $\Delta d_2=10^{-3}$；(b) $\Delta d_2=10^{-4}$；(c) $\Delta d_2=10^{-5}$；(d) $\Delta d_2=10^{-6}$

Fig. 12　Decrypted images with deviation in d_2. (a) $\Delta d_2=10^{-3}$; (b) $\Delta d_2=10^{-4}$; (c) $\Delta d_2=10^{-5}$; (d) $\Delta d_2=10^{-6}$

抵抗穷举攻击。

6　结　　论

光学信息安全技术和混沌密码学都是信息安全领域的重点研究方向。将两者有效结合，提出的对FDT-DRPE的改进算法可以总结如下：首先，在加密前将原图像进行相位编码得到复值图像，可以增加系统对第一块随机相位模板和衍射距离的敏感性；其次，在FDT-DRPE模块后增加像素值替代模块，使得密文的像素值分布更加均匀，有效抵御统计攻击，并且替代过程中采用的非线性操作有助于抵抗选择明文攻击；最后，改进算法采用三种不同的混沌系统来生成所需要的三块随机模板，借助于混沌系统的非线性性、伪随机性、对初值的高度敏感性，使得算法对多维密钥高度灵敏，密钥体积减小，密钥空间有效增大，加密系统的复杂性提高，破译难度增加。仿真结果显示该方法具有较高的安全性和实用性。

参　考　文　献

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

2 G Situ, J Zhang. Double random-phase encoding in the Fresnel domain [J]. Opt Lett, 2004, 29(14): 1584－1586.

3 X Peng, Z Y Cui, T N Tan. Information encryption with virtual-optics imaging system [J]. Opt Commun, 2002, 212(4): 235－245.

4 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.

5 Peng Xiang, Wei Hengzhen, Zhang Peng. Optical Information Security Introduction [M]. Beijing: Science Press, 2008. 181－219.
彭　翔，位恒政，张　鹏. 光学信息安全导论[M]. 北京：科学出版社，2008. 181－219.

6 Xi Sixing, Sun Xin, Liu Bing, *et al*.. New image encryption technology of image based on computer generated hologram [J]. Laser & Optoelectronics Progress, 2012, 49(4): 040902.
席思星，孙　欣，刘　兵，等. 基于计算全息的双随机相位图像加密技术[J]. 激光与光电子学进展，2012，49(4)：040902.

7 Kong Dezhao, Shen Xueju, Lin Chao, *et al*.. Multi-image encryption based on wavelet transform and fractional Fourier transform [J]. Laser & Optoelectronics Progress, 2013, 50(9): 091002.
孔德照，沈学举，林　超，等. 基于小波变换的分数阶傅里叶变换多图加密技术研究[J]. 激光与光电子学进展，2013，50(9)：091002.

8 M He, Q Tan, L Cao, *et al*.. Security enhanced optical encryption system by random phase key and permutation key [J]. Opt Express, 2009, 17(25): 22462－22473.

9 W Chen, X D Chen. Space-based optical image encryption [J]. Opt Express, 2010, 18(26): 27095－27104.

10 Q Wan, P Xiang. Asymmetric cryptosystem based on phase-truncated Fourier transforms [J]. Opt Lett, 2010, 35(2): 118－120.

11 Z Liu, Q Guo, L Xu, *et al*.. Double image encryption by using iterative random binary encoding in gyrator domains [J]. Opt Express, 2010, 18(11): 12033－12043.

12 Z Liu, Y Zhang, W Liu, *et al*.. Optical color image hiding scheme based on chaotic mapping and Hartley transform [J]. Opt & Lasers in Eng, 2013, 51(8): 967－972.

13 Z Liu, S Li, W Liu, *et al*.. Opto-digital image encryption by using Baker mapping and 1-D fractional Fourier transform [J]. Opt & Lasers in Eng, 2013, 51(3): 224－229.

14 Z S Wang, S X Lü, J C Feng, *et al*.. A digital image watermarking algorithm based on chaos and Fresnel transform [C]. The 4th IEEE International Conference on IHMSC, 2012,

2：144－148.

15 Xu Ning，Chen Xuelian，Yang Geng. Research on the algorithm of multiple-image encryption based on the improved virtual optical imaging [J]. Acta Physica Sinica，2013，62(8)：164－169.
徐　宁，陈雪莲，杨　庚. 基于改进后多维数据加密系统的多图像光学加密算法[J]. 物理学报，2013，62(8)：164－169.

16 X Wang，D Zhao. Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain [J]. Opt Commun，2011，284(1)：148－152.

17 X F Meng，X Peng，L Z Cai，*et al*.. Cryptosystem based on two-step phase-shifting interferometry and the RSA public-key encryption algorithm [J]. J Opt A：Pure & Appl Opt，2009，11(8)：085402.

18 Qin Yi，Lü Xiaodong，Gong Qiong，*et al*.. Additional key rotation multiplexing encryption using joint transform correlation architecrure [J]. Acta Optica Sinica，2013，33(3)：0307002.
秦　怡，吕晓东，巩　琼，等. 利用附加密钥旋转在光学联合相关结构中实现多二值图像加密 [J]. 光学学报，2013，33(3)：0307002.

19 Qin Yi，Zhang Shuai，Gong Qiong，*et al*.. Virtual optical image encryption based on interference [J]. Acta Optica Sinica，2012，32(10)：1007001.
秦　怡，张　帅，巩　琼，等. 基于干涉原理的虚拟光学加密系统[J]. 光学学报，2012，32(10)：1007001.

20 F Sun，Z Lü，S Liu. A new cryptosystem based on spatial chaotic system [J]. Opt Commun，2010，283(10)：2066－2073.

21 Liao Xiaofeng，Xiao Di，Chen Yong，*et al*.. Theory and Applications of Chaotic Cryptography [M]. Beijing：Science Press，2009. 232－259.
廖晓峰，肖　迪，陈　勇，等. 混沌密码学原理及其应用[M]. 北京：科学出版社，2009. 232－259.

22 Liu Jiandong，Fu Xiuli. Spatiotemporal chaotic one-way Hash function construction based on coupled tent maps [J]. Journal on Communications，2007，28 (6)：30－38.
刘建东，付秀丽. 基于耦合帐篷映像的时空混沌单向 Hash 函数构造[J]. 通信学报，2007，28(6)：30－38.

23 G R Chen，T Ueta. Yet another chaotic attractor [J]. Int J Bifurcation and Chaos，1999，9(7)：1465－1466.

24 W Zhu，G Yang，J Xu，*et al*.. Information encryption based on virtual optical imaging system and Chen′s chaos [C]. Proceedings of the 2012 International Conference on Web Information Systems and Mining，2012，7529：206－213.

栏目编辑：何卓铭