文章编号:1671-4598(2018)07-0251-05 DOI:10.16526/j.cnki.11—4762/tp.2018.07.056 中图分类号:TP391 文献标识码:A

基于混沌 Gyrator 变换与压缩感知的光学图像加密算法

杨 鹏
(陕西机电职业技术学院,陕西 宝鸡 721001)

摘要:为了增强光学加密技术的安全性与降低密文的数据容量,文章提出了基于混沌 Gyrator 变换与压缩感知的光学图像加密算法;首先,引入 Logistic 映射,利用明文特性来生成其初值,利用其输出的混沌序列来生成压缩感知的测量矩阵;随后,基于压缩感知理论,对明文进行预处理,获取中间密文;最后,利用 logistic 映射的随机序列来计算 Gyrator 变换的旋转角度,联合随机相位掩码,利用 Gyrator 变换方法对中间密文完成光学调制,得到最终密文;实验结果显示:与当前光学加密技术相比,所提算法具有更高的安全性与抗明文攻击能力。

关键词:光学图像加密;Logistic 映射;Gyrator 变换;压缩感知;随机相位掩码

An Optical Image Encryption Algorithm Based on Chaotic Gyrator Transform and Compressed Sensing

Yang Peng
(Shanxi institute of meshatronic technology, Shanxi 721001, China)

Abstract: In order to enhance the security of optical encryption technology and reduce the data capacity of cipher, an optical image encryption algorithm based on chaotic Gyrator transform and compressive sensing was proposed in this paper. Firstly, the plaintext characteristics were introduced to generate the initial value of Logistic map, and the output of chaotic sequences was used to generate two measurement matrices for compressed sensing. Then, based on compressed sensing theory, the intermediate cipher was got by using the compressed sensing theory to process the plaint. Finally, the rotation angle of Gyrator transformation was calculated by using the random sequence of logistic map. Finally, the intermediate cipher was fished optical modulation by jointing random phase mask to get the final cipher. The experimental results show that the proposed algorithm has higher security and anti plaintext attack capability compared with the current optical encryption technology.

Keywords: optical image encryption; logistic mapping; gyrator transform; compressed sensing; random phase mask

0 引言

随着各国之间的交流日益频繁,信息安全已成为当前各国的关注焦点,特别是随着计算机科学技术与互联网技术的快速发展,使得信息被窃取变得越来越容易[1]。而数字图像含有很多用户想要表达的隐秘信息,是当前用户进行交流的常用介质[2]。但是,当图像在开放的互联网中传输时,易被未知攻击干扰,导致图像内容被外泄,带给用户诸多安全隐患[3]。为了防止数字图像信息在互联网中遭遇攻击,保证其真实性,研究人员提出了图像加密技术,根据当前的研究成果可知,图像加密方法主要集中为 2 类较,一种是基于混沌理论的加密技术[4-6],另外一个是利用光学理论来加密[7-8]。如李春虎等人[4]为了扩大加密算法的密钥空间,设计了基于斜帐篷混沌映射和 Arnold 变换的图像加密方案,首先根据明文生成密钥,然后利用斜帐篷混沌映射和 Arnold 变换对图像进行加密,该算法引入混沌映射大大增加了密钥空间,使密文随机性和抗攻击性更强。吕群等人[5]为了解决现有的一些图像加密算法中,存在无法抵御选择明文攻击以及加密程度低、效率低等问题,设计了基于混沌系统和动态 S—盒的图像加密算法,依靠图像本身进行二维映射变换来改变像素点的位置,完成图像的置乱,并根据混沌序列对置乱后的图像进行分组,再联合 S 盒,完成图像的扩散。Ye 等人[6]为了增强密文的安全性与抵御攻击能力,通过联合波线置换和块扩散方法,提出了一种新的鲁棒加密方案,根据波浪特性,设计了波线置换技术,并通过二维 Arnold 变换,从多个不同的方向来完成像素的置乱,并基于 Arnold 变换的输出序列,设计一种新的像素扩散函数,实现置乱图像的加密,实验结果验证了其算法的安全性。虽然基于混沌理论的加密算法能够改善密文的安全性,在互联网中抵御一定的攻击能力,但是,不管是低维的混沌映射,还是高维的混沌系统,二者均存在迭代周期性,使得密文的安全性不佳[7]。

为了克服基于混沌理论的加密方案存在的不足,学者

收稿日期:2018-04-09; **修回日期**:2018-05-07。

作者简介:杨 鹏(1981-),男,讲师,陕西西安人,主要从事图像处理、信息安全、计算机信息管理方向的研究。

们又提出了光学加密方法，如肖宁等人[1]为了消除密文的轮廓显示问题，设计了基于圆谐分量展开与 Gyrator 变换域相位检索的光学图像加密算法，基于离轴圆谐分量展开机制，将 Gyrator 变换频谱分割为零阶圆谐分量与非零阶圆谐分量，并利用球面相位因子来调制零阶圆谐分量，输出加密密文，随后，引入迭代相位检索 Gyrator 变换算法，对非零阶圆谐分量完成编码，输出最终的密文，实验结果验证了其算法的合理性。杨建新等人[7]为了解决当前基于干涉原理的光学图像加密算法因存在轮廓显现导致其安全性不高的问题，设计了双光束叠加与差异模的光学图像加密算法，基于 Gyrator 变换，将明文变成一个 Gyrator 频域的复杂函数，随后引入矢量分解方法，将 Gyrator 频域复杂函数进行差异分解，输出幅度与相位不均等的 2 个矢量成分，利用 2 个相位掩码对矢量成分进行调制，将其从频域变为空域，将其相位部分视为私密，而幅度部分视为最终加密密文。Wang 等人[8]为了增强密文的安全性，消除对称加密方法的不足，提出了基于改进的幅度－相位恢复机制的非对称光学图像加密技术，通过利用不同的初始条件迭代 Logistic 映射，输出 2 个混沌掩码，将二者作为公共密钥，随后，对幅度－相位检索方法进行改进，完成图像的加密，获取一个实值密文，便于存储与管理，测试数据表明了其加密方法的可靠性。

但是，上述光学加密技术均忽略了明文自身的特性，使其低于明文攻击能力不佳，对此，本文基于混沌 Gyrator 变换与压缩感知的光学图像加密算法。为了增强算法与明文的联系，本文利用明文像素来迭代 Logistic 映射，利用其输出的混沌序列来生成压缩感知的测量矩阵；同时，为了降低密文的数据容量，引入压缩感知理论，对明文进行数据降维处理，得到一个紧凑的中间密文；最后，根据明文像素迭代 logistic 映射的数组来计算 Gyrator 变换的旋转角度，并结合随机相位掩码，利用 Gyrator 变换方法对中间密文完成光学调制，得到最终密文。租后，测试了所提光学加密技术的安全性。

1 压缩感知[9-10]

随着信息时代的到来，人们对信息需求量越来越大，使得信号采样率、传输和存储实现的压力越来越大[9]。而压缩感知 CS（Compressed Sensing）在采样方面有独特的优势，它可以利用比 Nyquist 采样理论更少的样本来重建信号。为了确保重建成功，信号应该是稀疏的或可压缩的[10]，对于一维信号 $x \in R^N$，其可以表示为：

$$x = \sum_{i=1}^{N} \xi_i \varphi_i = \varphi\xi \tag{1}$$

其中：ξ 代表 $N \times 1$ 维向量的加权系数；φ 是一个正交变换矩阵；φ_i 是 φ 的正交基。

在式（1）中，若 ξ 只存在 $K(K << N)$ 个非零系数，那么 x 可视为 K 的系数信号。在信号的 CS 过程中，直接替代计算 x，可观测到一个 $M \times N$ 维的线性矩阵：

$$y = \varphi\varphi\xi = \Theta\xi \tag{2}$$

其中：φ 是一个 $M \times N$ 维的测量矩阵，它与 φ 无关。

为了正确恢复 ξ，重构矩阵 Θ 应满足 K 的严格等距性质：

$$(1-\delta_K)\|\xi\|_2^2 \leqslant \|\Theta\xi\|_2^2 \leqslant (1+\delta_K)\|\xi\|_2^2 \tag{3}$$

其中：$\delta_K \in [0 \quad 1]$ 是等距常量。

最后，通过求解以下非凸优化问题，可以以较高的概率恢复原始信号：

$$\min\|\xi\|_0 \quad \text{s.t.} \quad y = \Theta\xi \tag{4}$$

取信号商都 512，稀疏度为 25%，测量长度为 5×5，且频域稀疏为零时，信号的重构效果见图 1。依图可知，CS 的信号恢复准确度较为理想，与初始信号曲线的拟合度较高。

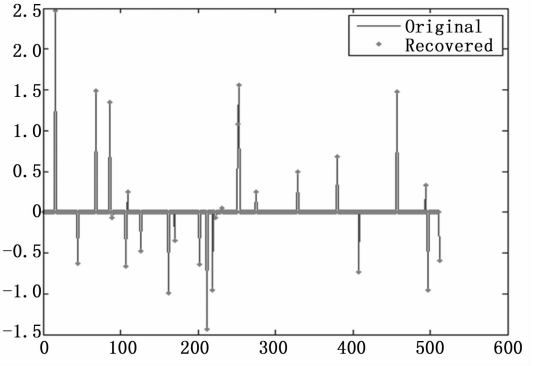


图 1 CS 的信号恢复测试

2 Gyrator 变换

积分变换[1]由于其含有变换参数，可以被视为加密钥，有效扩大密钥空间，在图像加密中得到广泛应用。若变换角度为 α，则图像 $f_i(x_i, y_i)$ 的 Gyrator 变换为[1]：

$$O(x_0, y_0) = G^{\alpha}[f_i(x_i, y_i)](x_0, y_0) = \frac{1}{|\sin\alpha|}\iint f_i(x_i, y_i) \times \exp\left(i2\pi \frac{(x_0y_0 + x_iy_i)\cos\alpha - (x_iy_0 + x_0y_i)}{\sin\alpha}\right)\mathrm{d}x_i\mathrm{d}y_i \tag{5}$$

式中，$g^{\alpha}()$ 是 Gyrator 变换算子；(x, y) 为输入坐标；(u, v) 为输出坐标；$o(x, y)$ 是复杂场函数。

另外，$g^{\alpha}()$ 的逆变换 $|o_0|$ 为：

$$g^{-\alpha}(o(x, y)) = g^{2\pi-\alpha}(o(x, y)) \tag{6}$$

所提技术就是借助 Gyrator 变换的广义透镜所对应的级联结构来编码图像，如图 2 所示。在图 2 中的左边代表的是 Gyrator 变换的 Gyrator 变换，由三个透镜构成；且任意两个透镜之间的距离是相等的[1]，均为 Z。透镜 L_1、L_3 的焦距均是 Z；而 L_2 的焦距为 $\frac{Z}{2}$。P_1，P_2 是输入、输出平面。图 2 中的右边代表具体的透镜结构；α_1，α_2 都是旋转角度，二者满足：

$$\alpha_1 = -\alpha; \alpha_2 = \alpha - \frac{\pi}{2} \tag{7}$$

初始图像经过 P_1 与 GT 系统后，输出的编码结果在 P_2 中：

$$O(u,v)=\frac{1}{|2\lambda\sin\alpha_2|}\times\iint o(x,y)\exp\left\{j2\pi\frac{(uv+xy)(2\sin2\alpha_1\sin2\alpha_2-1)-\frac{(xv+yu)}{2\lambda z\sin2\alpha_2}}{\sin\alpha}\right\}\mathrm{d}x\mathrm{d}y \tag{8}$$

其中：λ 是光波波长。

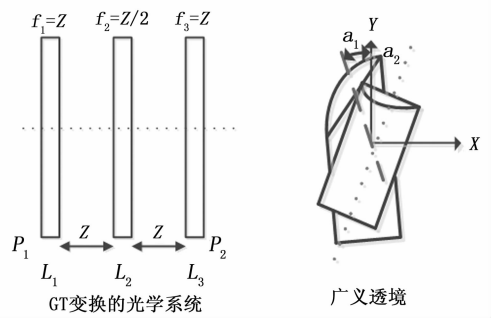


图 2　Gyrator 变换的光学系统

3　本文光学图像加密算法

所提的基于混沌 Gyrator 变换与压缩感知的光学图像加密算法主要包括 3 个过程：(1) 利用 Logistic 映射来形成测量矩阵；(2) 基于压缩感知的明文预处理；(3) 基于混沌 Gyrator 变换的图像加密。具体过程如下：

1) 令初始明文图像为 $f(x,y)$，其尺寸为 $h\times l$；随后，引入 Logistic 映射，对其迭代，以形成随机序列 $x=\{x_1,x_2,\ldots x_{h\times l}\}$：

$$x_{n+1}=\mu x_n(1-x_n) \tag{9}$$

其中：$\mu\in[0,4]$ 是混沌行为控制参数；$x_n\in[0,1]$、x_0 分别是输出值与初始值。

为了增强密文的抗明文攻击能力，本文利用明文像素来计算 Logistic 映射的 x_0：

$$x_0=\frac{T}{10^6} \tag{10}$$

其中：T 是明文的像素数量。

2) 根据 x_0 与 μ_1，对式 (9) 完成迭代，形成随机序列 $x=\{x_1,x_2,\ldots x_{h\times l}\}$。并将 $x=\{x_1,x_2,\ldots x_{h\times l}\}$ 排列为一个矩阵，将其作为测量矩阵 $\boldsymbol{\varphi}$：

$$\boldsymbol{\varphi}=\begin{bmatrix} x_1, & x_2 & \cdots\cdots & x_h \\ x_{h+1}, & x_{h+2} & \cdots\cdots & x_{2h} \\ \vdots & \vdots & & \vdots \\ x_{h\times l-h}, & \cdots\cdots & \cdots\cdots & x_{h\times l} \end{bmatrix} \tag{11}$$

3) 根据式 (11) 的测量矩阵 $\boldsymbol{\varphi}$，基于“1 压缩感知”，对图像 $f(x,y)$ 进行压缩，获取预处理图像 $f_{CS}(x,y)$；

4) 经典的 Gyrator 变换加密方法中的旋转角度 α 为一个定值，对明文缺乏敏感性，也就是对不同的明文实施加密，其采用的 α 都是相同的，从而削弱了算法的抗攻击能力[11-12]。对此，为了改善密文的抗明文攻击能力，充分消除加密方法的线性特征，本文借助两级 Gyrator 变换来实现这个目的。首先，从随机序列 $x=\{x_1,x_2,\ldots x_{h\times l}\}$ 中国分别提取奇数元素与偶数元素，形成了两个子序列 $S_{odd}=\{s_n\}$，$Z_{even}=\{z_m\}$，$n=m=\frac{h\times l}{2}$。其中，S_{odd} 是由所有奇数元素构成的序列；S_{even} 是由所有偶数元素构成的序列。再依据 $S=\{s_n\}$，$Z=\{z_m\}$ 计算 Gyrator 变换的参数 α_1，α_2：

$$\begin{cases}\alpha_1=\sum_{n=1}^{m}\frac{s_i}{2\pi n}\\ \alpha_2=\sum_{n=1}^{n}\frac{z_i}{2\pi n}\end{cases} \tag{12}$$

5) 根据式 (10) 计算的初值 x_0，再设置 μ_2，$\mu_2\neq u_1$，再次迭代式 (9)，获取一个新序列 $y=\{y_1,y_2,\ldots y_{h\times l}\}$。再将序列 $x=\{x_i\}$、$y=\{y_i\}$ 转换为两个不同的矩阵 $\boldsymbol{S}'=\{\|x(i,j)|,i=1,2..h,j=1,2..l\}$、$\boldsymbol{Z}'=\{\|z(i,j)|,i=1,2..h,j=1,2..l\}$。根据矩阵 $\boldsymbol{S}'$ 与 $\boldsymbol{Z}'$，获取对应的混沌掩码 $RPM1$、$RPM2$：

$$\begin{cases}RPM1=\exp(is(i,j))\\ RPM2=\exp(iz(i,j))\end{cases} \tag{13}$$

6) 根据参数 α_1，α_2，以及混沌掩码 $RPM1$、$RPM2$，根据图 3 所示的光电混合装置，对预处理图像 $f_{CS}(x,y)$ 完成 2 级 Gyrator 变换，输出密文 $C(x',y')$：

$$C(x',y')=G^{\alpha_1}\{G^{\alpha_2}\{f_{CS}(x,y)\times RPM1\}\times RPM2\} \tag{14}$$

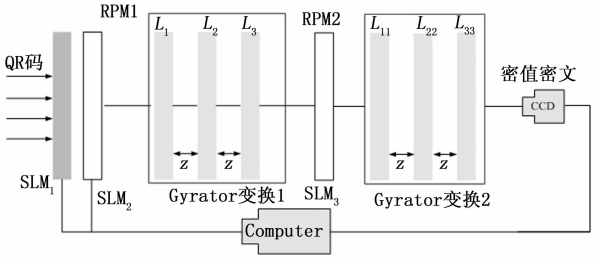


图 3　所提算法的光电混合结构

4　实验结果与分析

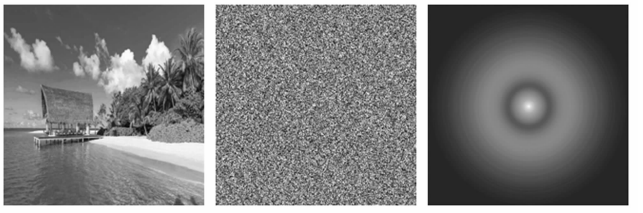
为了测试本文加密方法的安全性与抗明文攻击能力，借助 Matlab 6.5 软件完成实验，同时，将当前较为先进的光学加密方案作为对照组：文献 [1] 与文献 [7]，以突出所提技术的优势。进行实验的参数为：光学波长 $\lambda=623.8$ nm，混沌参数 $u_1=3.68$，$u_2=3.95$，焦距 $z=0.5$ m。

4.1　光学图像加密效果

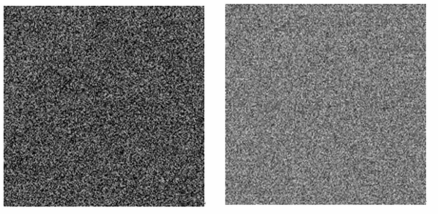
将图 4 (a) 视为本次实验的对象，其尺寸为 256×256，随后，基于所提技术、文献 [1] 以及文献 [7] 对其完成光学加密，结果见图 4 (b) ～4 (e)。依据测试结果可知，文献 [1] 的输出结果与所提算法、文献 [7] 不同，其输出 2 个密文，而本文算法与文献 [7] 均为一个密文；而且三种技术的加密效果都比较好，明文信息得到了很好的隐藏，非法用户难以从中直接获取相关线索。

主观评估难以具体量化三者的优劣，为此，本文引入信息熵值[1]来评估，测试数据见表 1。根据表中数据可知，文献 [1] 的密熵值最高，分别为 7.995 2、7.996 7，而本文算法密文熵值略低于文献 [1]，约为 7.996 1，文献 [7]

的密文熵值最低，约为 7.993 7。原因是文献［1］利用了离轴圆谐分量展开机制将 Gyrator 变换频谱分割为零阶、非零阶圆谐分量，并利用球面相位因子，对零阶圆谐分量进行调制，形成相应的密文，充分破坏了加密系统的线性关系，将两个密文分发给两个不同的用户，使其安全性最高。而本文算法则是利用明文像素来计算 Gyrator 变换的旋转角度以及相应的相位掩码，对明文进行二级 Gyrator 变换加密，显著增强了密文与明文的关系，充分消除了加密系统的线性特征，使其具备较高的安全性。而文献［7］则是利用矢量分解方法将 Gyrtor 频谱分割为两个不同的成分，通过 2 个相位掩码对矢量成分进行调制，从而完成加密，虽然矢量分解能够破坏系统的线性关系，但是其结果仅保留在一个纯 POS 掩码中，使其安全性较低。



(a)初始明文 (b)本文算法 (c)文献[1]的第一个密文



(d)文献[1]的第二个密文 (e)文献[7]的密文

图 4 不同算法的光学加密结果

表 1 密文熵值的测试果

名称	本文算法	文献[1]的第一个密文	文献[1]的第二个密文	文献[7]
熵值	7.996 1	7.995 2	7.996 7	7.993 7

4.2 抗选择明文攻击能力测试

选择明文攻击是是当前互联网中较为常见的攻击类型，对密文安全威胁较大，因此，优异的加密技术应可充分抵御选择明文攻击[2]。根据当前的研究成果可知，NPCR、UACI 曲线[2]是衡量加密技术的抗选择明文攻击能力的经典指标。由文献［2］可知，NPCR，UACI 函数为：

$$\mathrm{NPCR}=\frac{\sum_{i=1}^{W}\sum_{j=1}^{H}Difp(I(i,j),I'(i,j))}{W\times H}\times 100\% \quad (15)$$

$$\mathrm{UACI}=\frac{1}{W\times H}\left[\sum_{ij}\frac{|I(i,j)-I'(i,j)|}{255}\right]\times 100\% \quad (16)$$

$$\mathrm{Difp}(I(i,j),I'(i,j))=\begin{cases}0, & I(i,j)=I'(i,j)\\ 1, & I(i,j)\neq I'(i,j)\end{cases} \quad (17)$$

式中，W,H 分别是初始图像的高度与宽度；I,I' 分别代表两个明文经加密处理后的两个密文，且这两个明文都只存在一个相异灰度值[2]。

以图 4（a）为对象，将其（126，12）处的像素值 212 改为 21，剩余像素不变，并通过本文算法，文献［1］和文献［7］对篡改前后的明文完成加密，根据式（15）～式（16），形成 3 种方案的 NPCR、UACI 曲线，结果见图 5。按照输出的测试数据可知，本文光学加密算法的的抗明文攻击能力最强，其稳定的密文 NPCR、UACI 值都是最大的，分别为 99.81%，35.79%，而文献［1］、文献［7］两种技术的抗选择明文攻击能力较弱，对应的 NPCR、UACI 值均要小于本文算法。主要是因为本文光学加密过程均与明文紧密相连，使其对于不同的初始图像，会得到不同的加密密钥，导致其难以获取正确密钥，无法对密文进行破译，本文方案利用初始图像的像素来迭代 Logistic 映射，根据去输出的随机序列来压缩初始图像，已经计算二级 Gyrator 变换的两个旋转角度，当攻击者利用其它图像来攻击时，因着明文的不同，使得攻击者得到的密钥均为错误的。而文献［1］、文献［7］两种技术的加密过程均没有考虑明文自身特性，使其加密密钥对明文不敏感。

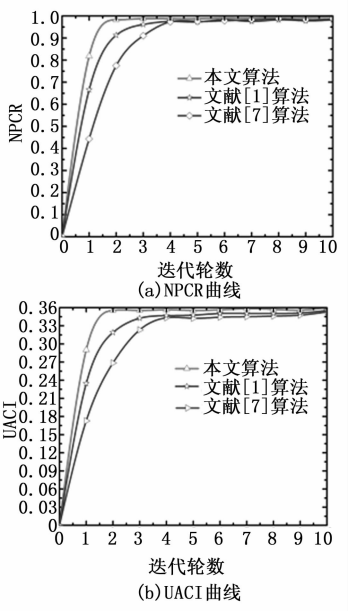


图 5 三种算法的抗选择明文攻击能力测试

4.3 密钥敏感性测试

良好的加密算法应满足严格的“雪崩效应”，即使密钥发生极其微小的变化，攻击者也是无法得到正确的解密图像[1]。对此，本文验证了混沌控制参数 $u_2=3.95$ 的敏感性，通过一个偏差 $\Delta t=10^{-16}$ 对 $u_2=3.95$ 进行修改，形成两个错误的密钥 $u_2=3.95-10^{-16}$ 和 $u_2=3.95+10^{-16}$，剩余的密钥均不变。再借助正确密钥以及两组错误密钥来复原图 4（b），输出结果和对应的 MSE 曲线如图 6 所示。根据测试数据可知，即使 $u_2=3.95$ 发生了 10^{-16} 这样极其微小的修改，仍然是不能对密文进行破译。只有当密钥没有偏差时，才能正确破译密文，此时的 MSE 曲线出现突变，其值接近零。这说明所提光学加密技术具备强烈的密钥敏感性。

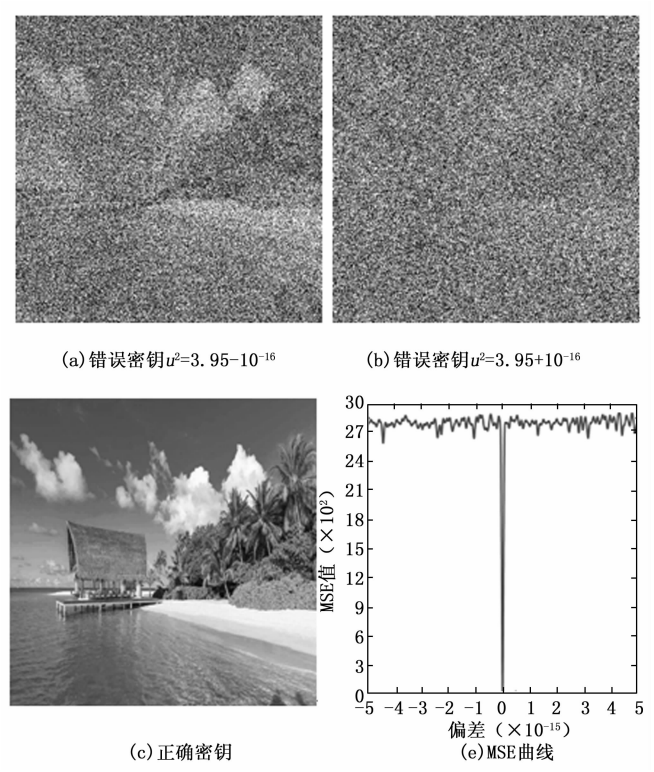


图 6　所提算法的密钥敏感性测试

4.4　加密算法的实际应用

医学图像对于医生判断病情至关重要，若图像在网络传输中遭受攻击，则会严重影响图像的质量，对于病情的判断不利。为此，本文以 B 超图像为例，其尺寸为 256×256，见图 7（a）；根据式（10）可计算初值 $x_0=0.65$；设置 $u_1=3.68$，$u_2=3.95$，根据算法过程，可得到 Gyrator 变换的两个旋转角度 $\alpha_1=0.51°$，$\alpha_2=0.63°$。依据式（13），得到的两个随机掩码分别见图 7（b）和图 7（c）。再设置光学变换参数：光学波长 $\lambda=623.8$ nm，混沌参数 $u_1=3.68$，$u_2=3.95$，焦距 $z=0.5$ m。根据式（14），获取相应的密文，见图 7（d）。

若图 7（a）在网络中遭遇噪声与模糊攻击，见图 7（e）和图 7（f），严重降低了图像质量，给医生的准确判断病情带来不利影响。但是，若本文算法的密文遇到噪声与模糊攻击后，根据所以算法的密钥，对其复原，结果见图 7（g）和图 7（h）。由图可知，所提算法充分混淆了医学图像信息，即使其在网络中遇到噪声与模糊攻击，其影响的也只是加密密文而已，只要用户利用正确的密钥对其解密，既可获得清晰完整的图像。

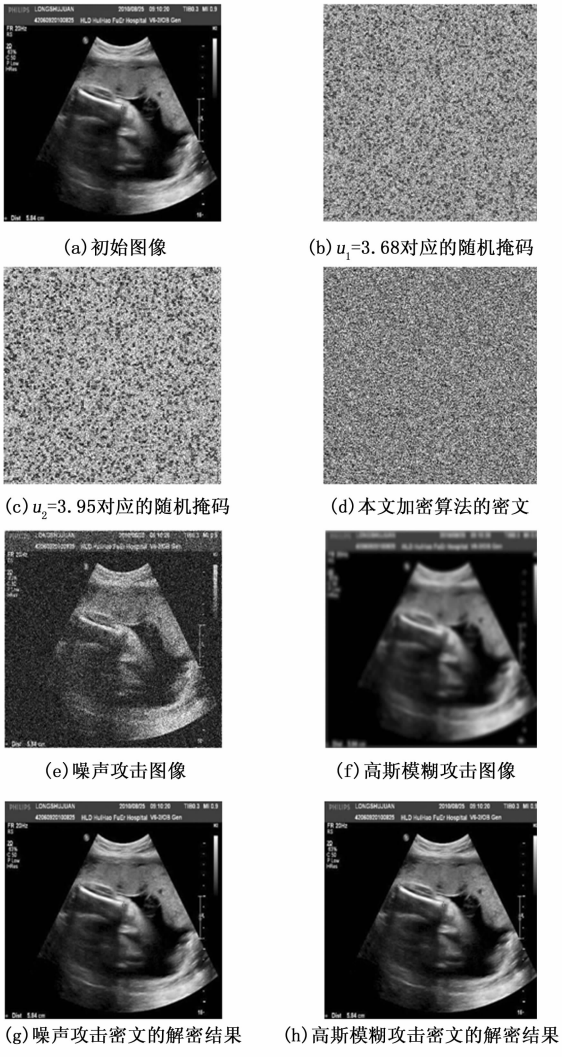


图 7　所提算法的实际应用测试

5　结论

为了提高加密算法对初始明文的敏感性，增强密文的抗选择明文攻击能力，本文设计了混沌 Gyrator 变换耦合压缩感知的光学图像加密算法。通过明文像素来迭代 Logistic 映射，利用其输出的混沌序列来生成压缩感知的测量矩阵；并根据测量矩阵，利用压缩感知技术对明文进行预处理，增强算法与明文的关系，有效降低密文的数据容量；最后，利用两个不同的随机序列来计算 Gyrator 变换的两个旋转角度，结合相位掩码，对预处理结果完成二级光学调制，完成图像的加密。所提算法不仅有效破坏了整个密文的线性特性，而且对明文十分敏感。测试结果验证了所提光学加密技术的安全性。

参考文献：

[1] 肖　宁，李爱军. 基于圆谐分量展开与 Gyrator 变换域相位检索的光学图像加密算法 [J]. 电子测量与仪器学报，2017，31（6）：876－884.

[2] 王涛涛，张　超. 基于 Diophantus 模型与动态 S 盒的图像加密算法 [J]. 计算机工程与设计，2017，38（10）：2678－2685.

[3] Abdelkader Moumen，Hocine Sissaoui. Images Encryption Method using Steganographic LSB Method，AES and RSA algorithm [J]. Nonlinear Engineering ，2017，6（1）：53－59.

（下转第 261 页）