·安全技术·　　文章编号：1000-3428(2019)01-0121-08　　文献标志码：A　　中图分类号：TP309

基于快速响应码约束的光学图像加密算法

曹　蕾

（西华师范大学 教育学院，四川 南充 637000）

摘　要：为提高光学图像加密算法的安全性与解密质量，方便密钥的存储、管理与传输，提出一种基于快速响应(QR)码约束与混沌 Gyrator 变换的图像加密算法。引入二维耦合混沌系统，利用明文像素对其进行迭代后输出 2 个随机相位掩码。通过 2 个混沌序列来计算 2 个 Gyrator 变换的旋转角度，然后利用明文生成相应的 QR 码，并将其置于 2 个随机相位掩码结构的输入平面，通过两级 Gyrator 变换输出一个实值密文。同时，借助 QR 码的支撑约束条件对传统的相位检索技术进行改进，最终从密文中检索到初始的 QR 码后解密图像。实验结果表明，与借助圆谐分量展开与 Gyrator 变换实现光学图像加密的算法相比，该算法具有较高的安全性与解密质量，在噪声攻击下，其复原图像的失真度较低。

关键词：光学图像加密；快速响应码；二维耦合混沌系统；随机相位掩码；Gyrator 变换；相位检索技术

中文引用格式：曹蕾. 基于快速响应码约束的光学图像加密算法[J]. 计算机工程，2019，45(1)：121-128.

英文引用格式：CAO Lei. Optical image encryption algorithm based on quick response code constraint[J]. Computer Engineering，2019，45(1)：121-128.

Optical Image Encryption Algorithm Based on Quick Response Code Constraint

CAO Lei

(School of Education，China West Normal University，Nanchong，Sichuan 637000，China)

【Abstract】 In order to improve the security and decryption quality of optical image encryption algorithm and facilitate key storage，management and transmission，an image encryption algorithm based on Quick Response(QR) code constraint and chaotic Gyrator transform is proposed. A two-dimensional coupled chaotic system is introduced，and two random phase masks are output after iteration using plaintext pixels. Two chaotic sequences are used to calculate the rotation angles of the two Gyrator transforms，and then the corresponding fast response codes are generated by plaintext. The codes are placed on the input plane of two random phase masks and a real ciphertext is output by two-stage Gyrator transforms. At the same time，the traditional phase retrieval technology is improved by using the support constraints of the QR code，and the original QR code is retrieved from the ciphertext and the decrypted image is decrypted. Experimental results show that the proposed algorithm has higher security and decryption quality than the optical image encryption algorithm based on circular harmonic component expansion and Gyrator transform，under noise attack，the distortion of restored image is lower.

【Key words】 optical image encryption；Quick Response(QR) code；two-dimensional coupled chaotic system；random phase mask；Gyrator transform；phase retrieval technology

DOI：10.19678/j.issn.1000-3428.0049571

0　概述

图像是多媒体技术中较常用的介质，在医疗与模式识别等领域得到广泛应用[1-2]。如何确保图像信息在网络中安全传输，已成为当前国内外学者的研究焦点[3]。

目前，较主流的图像加密技术分为混沌加密与光学加密 2 种。混沌加密技术[4]主要利用混沌系统的复杂轨迹、相空间等特性置乱与扩散图像像素。文献[3]利用改进 Lorenz 混沌系统的混沌序列来加密图像。文献[4]设计基于混沌系统与动态密钥选择机制的图像加密技术，其利用置乱方法与动态密钥选择机制来完成像素加密。文献[5]设计基于混沌系统与动态 S 盒的图像加密算法，该算法根据混沌系统来生成一个动态 S 盒，以实现图像加密。但是混沌加密技术主要是在空域上来完成像素置乱，

基金项目：四川省自然科学基金(201412673501)；四川省科技计划项目(2014GZX0003)；西华师范大学博士科研启动项目(412/412506)。

作者简介：曹　蕾(1982—)，女，副教授、博士，主研方向为网络信息安全、计算机图像、多媒体技术。

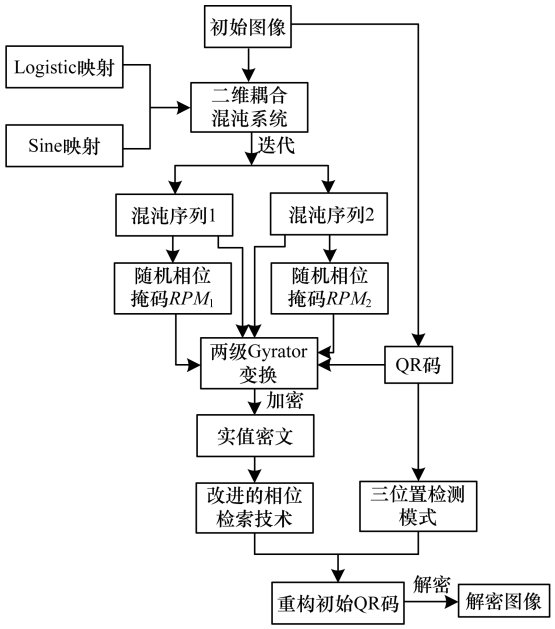
收稿日期：2017-12-05　　**修回日期：**2018-01-05　**E-mail：**caolei1982xdt@sina.com

且混沌系统在多次迭代期间存在周期性,从而导致该技术的安全性较低[6]。近年来,诸多学者提出相应的光学图像加密技术。文献[7]提出基于双随机相位编码的光学图像加密方法,实验结果验证了其安全性。但是,该算法的密文是一个复数函数,不方便私钥的管理与传输。文献[8]设计基于压缩感知与分数阶 Fourier 域的光学加密算法,仿真结果表明该技术具备良好的安全性与加密效率。但是其随机相位掩码(Random Phase Mask,RPM)的重构较困难,若 RPM 在重构阶段遭遇到破坏或者丢失,则用户难以正确复原图像。文献[9]提出基于多光束干涉与矢量分解的光学图像加密算法,并验证了其技术的有效性与优越性。但是该技术是将纯相位掩码作为私钥,不便于密钥的管理与传输,且其需要多个分光元器件,这增加了光学装置的复杂性。

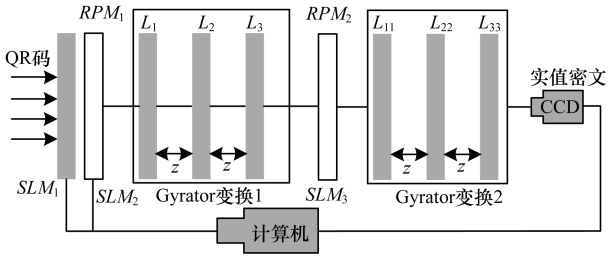
为将明文以实值函数形式输出并提高密文的安全性与解密质量,本文提出基于快速响应(Quick Response,QR)码约束与混沌 Gyrator 变换的图像加密算法。将二维耦合混沌系统的参数视为私钥,以降低传输容量,通过混沌随机序列来计算 Gyrator 变换的 2 个角度,再将明文转换为相应的 QR 码后通过只记录其两级 Gyrator 变换的强度分布,输出一个实值密文,以方便密钥的存储、管理与传输。同时,将 QR 码的三位置检测模式作为信息支撑约束条件,改进相位检索技术并从密文中检索初始 QR 码。

1 基于 QR 码的光学图像加密算法

本文图像加密算法的过程如图 1(a)所示,其相应的光学加密装置如图 1(b)所示。其中,RPM_1、RPM_2 为随机相位掩码,SLM_1、SLM_2、SLM_3 为空间光调制器,L_1、L_2、L_3 为第 1 个 Gyrator 变换的透镜,相应的焦距为 z,L_{11}、L_{22}、L_{33} 为第 2 个 Gyrator 变换的透镜,相应的焦距也为 z。由图 1 可知,该技术分为 3 个过程:1)基于二维耦合混沌系统的随机相位掩码生成;2)基于两级 Gyrator 变换的 QR 码加密;3)基于改进相位检索技术的密文复原。根据二维耦合混沌系统的输出序列获取 2 个不同的随机相位掩码,分别置于空域与频域平面上,以兼顾算法的效率与安全性。再利用混沌序列来计算2 个不同的 Gyrator 变换角度,联合随机相位掩码完成图像加密。最后借助 QR 码的三位置检测模式来改进相位检索技术,重构初始 QR 码后实现密文的准确解密。



(a)算法流程



(b)光学加密装置结构

图 1 基于 QR 码的光学图像加密算法

1.1 基于二维耦合混沌系统的随机相位掩码生成

低维(维数 <3)混沌映射具有加密效率高的特点,但是,其混沌序列的自相关性较高,导致其密文的安全性较低。为此,本文引入二维耦合混沌系统[10],该系统融合 Logistic 映射[11]与 Sine 映射[12]的优势来实现加密。其中,Logistic 映射[11]函数如下:

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

其中,$\mu\in[0,4]$ 是混沌参数,x_n、$x_0\in[0,1]$ 分别代表输出值与初始值。

Sine 映射[12]函数为:

$$x_{i+1}=\frac{\alpha\sin(\pi x_i)}{4} \tag{2}$$

其中,$\alpha\in[0,1]$ 为混沌参数。

依据文献[10]可知,利用非线性耦合方法可得到二维耦合混沌系统:

$$\begin{cases}x_{i+1}=\alpha\left(\dfrac{\sin(\pi y_i)}{4}+\delta\right)x_i(1-x_i)\\ y_{i+1}=\alpha\left(\dfrac{\sin(\pi x_{i+1})}{4}\right)y_i(1-y_i)\end{cases} \tag{3}$$

其中,$\delta\in[0,3]$ 为混沌参数。

为突出式(3)的融合优势,取测试步长为 4 000,在 TestU01[13] 中测试 Logistic 映射、Sine 映射与

式(3)的混沌序列的自相关性,结果如图 2 所示。由图 2 可以看出,式(3)所输出的混沌序列具有较高的伪随机性,其对应的自相关性系数最低,基本都接近 0,而 Logistic 映射、Sine 映射的混沌序列自相关性均较高。

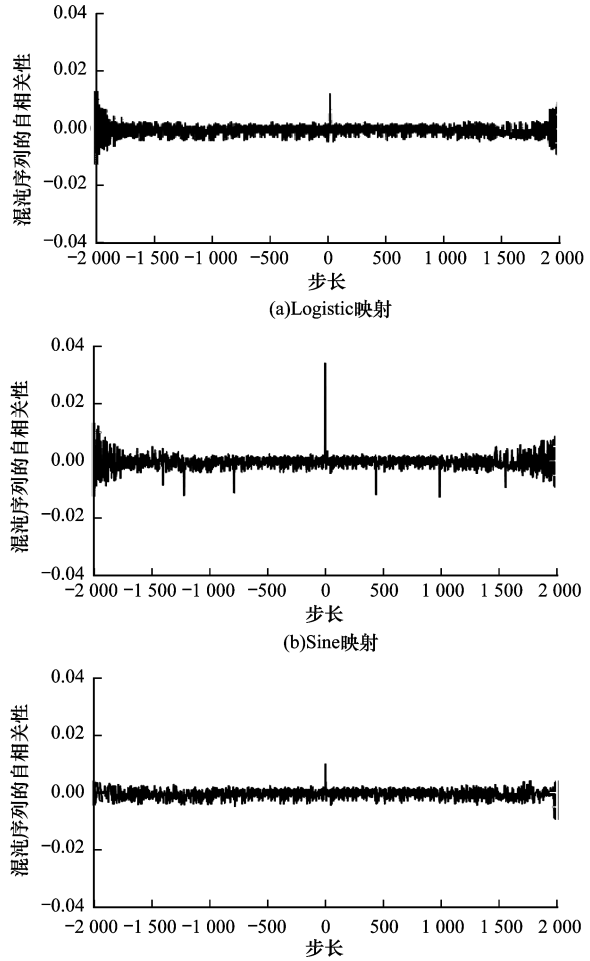


图 2　不同混沌映射的混沌性能测试结果

为增强算法抵御明文攻击的能力,本文借助初始图像的像素数量来估算二维耦合混沌映射的初始值 x_0、y_0:

$$\begin{cases} x_0 = \dfrac{T}{2\times 10^7} \\ y_0 = 1 - x_0 \end{cases} \tag{4}$$

根据 x_0、y_0 与混沌参数 α、δ,先迭代式(3)K 次,舍弃所有的输出值,以降低瞬态效应。再对式(3)迭代 $M\times N$ 次,此时可输出 2 个混沌序列 $\boldsymbol{X}=\{x_1, x_2,\cdots,x_{M\times N+K}\}$、$\boldsymbol{Y}=\{y_1,y_2,\cdots,y_{M\times N+K}\}$。为获取相应的随机相位掩码,对向量序列 $\boldsymbol{X}$、$\boldsymbol{Y}$ 进行变换,得到 2 个新向量序列 $\boldsymbol{S}=\{s_n\}$,$\boldsymbol{Z}=\{z_n\}$:

$$\begin{cases} s_n = 2\pi\times((abs(x_n)-floor(abs(x_n)))\times \\ \qquad 10^{14}\bmod(256))/255 \\ z_n = 2\pi\times((abs(y_n)-floor(abs(y_n)))\times \\ \qquad 10^{14}\bmod(256))/255 \end{cases} \tag{5}$$

其中,$abs(\cdot)$表示取绝对值运算,$floor(\cdot)$表示向下取整运算。

通过对序列 $\boldsymbol{S}=\{s_n\}$、$\boldsymbol{Z}=\{z_n\}$ 进行重排,形成 2 个二维矩阵 $\boldsymbol{S}'=\{s(n,m)\,|\,n=1,2,\cdots,M,m=1,2,\cdots,N\}$、$\boldsymbol{Z}'=\{z(n,m)\,|\,n=1,2,\cdots,M,m=1,2,\cdots,N\}$。再依据矩阵 $\boldsymbol{S}'$、$\boldsymbol{Z}'$ 计算相应的随机相位掩码 RPM_1、RPM_2:

$$\begin{cases} RPM_1 = \exp(is(n,m)) \\ RPM_2 = \exp(iz(n,m)) \end{cases} \tag{6}$$

若明文尺寸为 512×512 像素,依据式(4)可得 $x_0=0.133$、$y_0=0.867$,并取 $\alpha=0.45$,$\delta=3.8$,对式(3)进行 512×512 次迭代。基于式(5)、式(6)获取的 RPM_1、RPM_2 如图 3 所示。

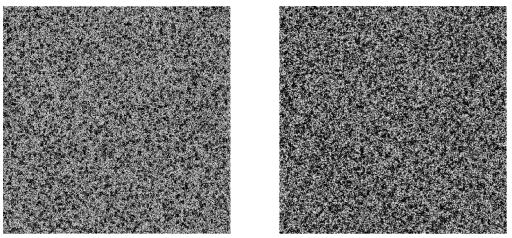


图 3　2 个随机相位掩码

1.2　基于两级 Gyrator 变换的 QR 码加密

联合 RPM_1、RPM_2,基于 Gyrator 变换来实现对图像的光学加密。Gyrator 操作[13]是处理二维信号的常用方法,令旋转角度为 β,则图像 $f_i(x_i,y_i)$ 的 Gyrator 变换为[13]:

$$O(x_0,y_0)=G^{\beta}[f_i(x_i,y_i)](x_0,y_0)= \frac{1}{|\sin\beta|}\iint f_i(x_i,y_i)\times \exp\left(\mathrm{i}2\pi\frac{(x_0y_0+x_iy_i)\cos\beta-(x_iy_0+x_0y_i)}{\sin\beta}\right)\mathrm{d}x_i\mathrm{d}y_i \tag{7}$$

其中,$G^{\beta}[\cdot]$是 Gyrator 变换,(x_i,y_i)、(x_0,y_0)分别代表输入、输出坐标,$O(x_0,y_0)$是复杂场函数。且 $G^{\beta}[\cdot]$的可逆变换 $|O_0|$ 如下:

$$G^{-\beta}(O(x_i,y_i))=G^{2\pi-\beta}(O(x_i,y_i)) \tag{8}$$

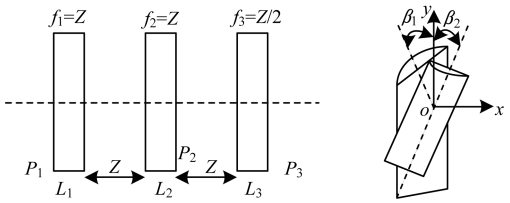
其中,$G^{-\beta}$是旋转角度为 β 的 Gyrator 逆变换。

在本文光学加密技术中,主要借助 Gyrator 操作中透镜的级联结构来完成信息加密。Gyrator 变换的光学系统结构如图 4 所示。其中,图 4(a)是 Gyrator 变换的光学结构,包含 3 个透镜 L_1、L_2、L_3,且 L_1 与 L_2、L_2 与 L_3 间的距离均是 Z。另外,L_1 与 L_2 的焦距是 Z,L_3 的焦距是 $Z/2$,P_1、P_2 分别是输入、输出平面。图 4(b)是 Gyrator 操作的透镜结构,其中,β_1、β_2 为旋转角度:

$$\beta_1=-\beta,\beta_2=\beta-\pi/2 \tag{9}$$

二维信号由 P_1 平面进入,被相应的光学系统调制后,密文信息将记录在 P_2 上:

$$O(x_0,y_0)=\frac{1}{|2\lambda\sin\beta|}\times\iint f_i(x_i,y_i)\times\exp\left(\mathrm{i}2\pi\frac{(x_0y_0+x_iy_i)(2\sin2\beta_1\sin2\beta_2-1)-\dfrac{(x_iy_0+x_0y_i)}{2\lambda\sin2\beta_2}}{\sin\beta}\right)\mathrm{d}x_i\mathrm{d}y_i \tag{10}$$



(a)Gyrator变换的光学结构 (b)广义透镜

图 4 Gyrator 变换的光学系统

在传统的 Gyrator 变换域加密技术中,旋转角度 β 固定,缺乏动态性,导致该技术加密密文的安全性较低。为增强算法的安全性,破坏加密系统的线性关系,本文使用两级 Gyrator 变换并根据式(3)输出的 2 个混沌序列 $\boldsymbol{S}=\{s_n\}$、$\boldsymbol{Z}=\{z_n\}$ 来计算旋转角度 β_1、β_2。分别从序列 $\boldsymbol{S}=\{s_n\}$、$\boldsymbol{Z}=\{z_n\}$ 中随机选择 N 个元素值,形成 2 个对应的过渡数组 $\boldsymbol{V}=\{v_1,v_2,\cdots,v_N\}$,$\boldsymbol{Q}=\{q_1,q_2,\cdots,q_N\}$,则旋转角度 β_1、β_2 为:

$$\begin{cases}\beta_1=\sum_{n=1}^{N}\dfrac{v_i}{2\pi N}\\ \beta_2=\sum_{n=1}^{N}\dfrac{q_i}{2\pi N}\end{cases} \tag{11}$$

利用 β_1、β_2 对 QR 码进行两级 Gyrator 变换,将变换结果的强度分布视为密文 $C(x'',y'')$:

$$C(x'',y'')=G^{\beta_1}\{G^{\beta_2}\{f(x,y)\times RPM_1\}\times RPM_2\} \tag{12}$$

其中,$f(x,y)$ 是明文对应的 QR 码,G^{β_1}、G^{β_2} 分别是旋转角度为 β_1、β_2 的 Gyrator 变换。

以图 5(a)为明文,利用成熟的免费软件(https://cli.im/)来生成其相应的 QR 码,如图 5(b)所示。通过上述加密过程,输出的密文如图 5(c)所示。由图 5 可以看出,明文图像经过本文加密算法处理后,其信息被高度隐藏,最终呈现一幅白噪声分布的图像。

(a)明文 (b)QR码 (c)加密密文

图 5 基于两级 Gyrator 变换的图像加密过程

1.3 基于改进相位检索技术的密文复原

由于本文光学加密技术没有任何相位信息,因此引入相位检索技术[14]来解密图像。在本文算法中,由于只有一个强度数据 $C(x'',y'')$ 可以利用,因此传统的相位检索技术会大幅降低收敛速度。为解决该问题,本文利用 QR 码的三位置检测模式(左上角、右上角、左下角)作为支撑约束条件,以解决停滞问题。具体步骤如下:

步骤 1 假设初始 QR 码的估计值为 $f_0(x,y)$,其大小与明文尺寸相等,含有 $M\times N$ 个元素。

步骤 2 对于第 k 轮迭代,利用相干平行光束照射初始 QR 码的估计模型 $f_k(x,y)$。随后,基于两级 Gyrator 变换,利用 2 个混沌相位掩码 RPM_1、RPM_2 对 $f_k(x,y)$ 进行调制:

$$g_k(x'',y'')=G^{\beta_1}\{G^{\beta_2}\{f_k(x,y)\times RPM_1\}\times RPM_2\} \tag{13}$$

步骤 3 用强度数据 $C(x'',y'')$ 替代临时函数 $g_k(x'',y'')$ 的幅度部分,且保持其相位部分不变。则光照分布函数变为:

$$\hat{g}_k(x'',y'')=|C(x'',y'')|^{\frac{1}{2}}\times\arg(g_k(x'',y'')) \tag{14}$$

其中,arg(·)为相位提取操作。

步骤 4 依据式(14)修改的光照分布函数,执行式(13)的逆过程,利用旋转角度为 $-\beta_1$、$-\beta_2$ 的两级 Gyrator 变换,可得:

$$\hat{f}_k(x,y)=G^{-\beta_1}\{G^{-\beta_2}\{\hat{g}_k(x'',y'')\times conj(RPM_1)\}\times conj(RPM_2)\} \tag{15}$$

其中,$conj$ 为共轭运算。

步骤 5 在进行 $k+1$ 轮迭代时,利用支撑约束条件 $P(x,y)$ 来更新初始 QR 码的估计值 $f_{k+1}(x,y)$:

$$f_{k+1}(x,y)=\frac{\varepsilon\times P(x,y)\times(|\hat{f}_k(x,y)|+f_k(x,y)\times P(x,y))}{P(x,y)+\gamma} \tag{16}$$

其中,ε、γ 均为调整参数,且为常量,ε 用于调整迭代过程的收敛速度,γ 用于确保式(16)结果不为零。

步骤 6 为确定迭代停止时间,利用 $|f_k(x,y)|$ 与初始 QR 码 $f(x,y)$ 间的相关系数 CC(Correlation Coefficient)作为收敛标准:

$$CC=\frac{E\{[f-E(f)][|f_k|-E(|f_k|)]\}}{\sqrt{E\{[f-E(f)]^2\}}\sqrt{E\{[|f_k|-E(|f_k|)]^2\}}} \tag{17}$$

其中,$E(\cdot)$ 代表求期望值运算。当相关系数 CC 达到用户预设值(与 1 接近)时,则可获得最佳的迭代结果。

步骤 7 反复执行步骤 1 ~ 步骤 5,直到相关系数 CC 达到预设值,其最后的更新结果 $f_{k+1}(x,y)$ 即为解密 QR 码,通过相应的解码软件可以获取初始明文。

以图 5(c)为解密对象,初始 QR 码的三位置检测模式如图 6(a)所示,经过上述相位检索算法得到的解密 QR 码如图 6(b)所示,最终复原的图像如图 6(c)所示。

(a)三位置检测模式　(b)解密QR码　(c)解密图像

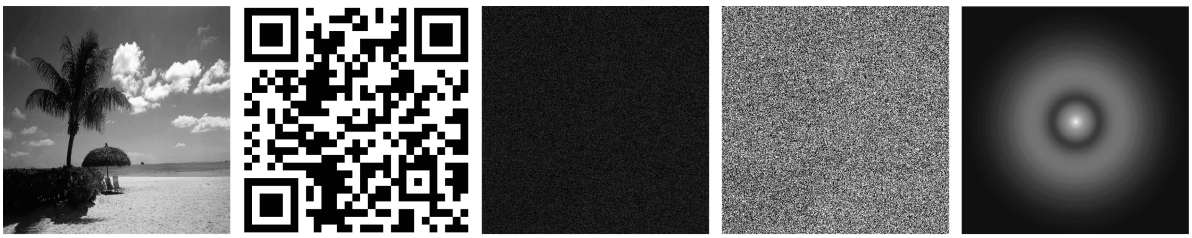
图 6　密文的解密结果

2　实验结果与分析

本次实验借助 Matlab7.0 工具来测试本文光学加密算法的合理性与安全性。另外,为体现该加密算法的优越性,将文献[9,15]算法与本文算法进行对比分析。其中,文献[15]算法借助圆谐分量展开与 Gyrator 变换来完成图像的光学加密,其能够显著增强密文的安全性。测试实验所需的部分参数为:混沌参数 $\alpha=0.45$, $\delta=3.8$, $K=2\ 000$,调整参数 $\varepsilon=0.09$, $\gamma=0.001$,焦距 $z=0.06$ m,波长为 632.8 mm,式(17)的收敛预设值为 0.999。

2.1　光学图像加密效果

将 512×512 像素的图 7(a)作为测试对象,利用本文算法、文献[9]算法、文献[15]算法进行光学图像加密,输出结果如图 7(b)~图 7(e)所示。其中,明文对应的 QR 码如图 7(b)。



(a)初始明文　(b)明文对应的QR码　(c)本文算法结果　(d)文献[9]算法结果　(e) 文献[15]算法结果

图 7　不同光学图像加密算法输出的密文对比

由图 7 可以看出,3 种加密技术都具备较高的安全性,明文的内容信息均得到了高度混淆,结果都为一幅高斯噪声分布图像,且没有轮廓显示问题,非授权用户不能直接从这些密文中获取有用信息。为有效区分这 3 种光学加密机制的安全性差异,本文引入信息熵[15]来进行量化,测试结果如表 1 所示。由表 1 可以看出,3 种算法的密文熵值均与理论值 8 接近,但是本文算法的密文熵值要略大于文献[9]算法和文献[15]算法,这表明本文光学加密算法具有更高的安全性。造成该现象的原因是本文加密算法利用二维耦合混沌系统来生成混沌相位掩码,增加了密文的敏感性,且 Gyrator 变换的参数均根据混沌序列来生成,而非固定,这能够显著增加密文的伪随机性,此外,通过两级 Gyrator 变换对明文的相应 QR 码进行调制,能够充分破坏系统的线性关系,从而使得本文算法输出的密文具有较高的安全性。文献[15]算法的 Gyrator 变换参数固定,缺乏敏感性,不能有效破坏系统的线性关系,导致其密文安全性较低。文献[9]算法主要借助多路光束的干涉原理与矢量分解技术来完成图像的加密,其算法的密钥空间较小,且多路光束的对准问题影响了其密文的安全性。

表 1　3 种算法信息熵值测试结果

算法	密文熵值
本文算法	7.998 3
文献[9]算法	7.988 2
文献[15]算法	7.993 6

2.2　抗选择明文攻击能力测试

根据文献[1]可知,*NPCR*、*UACI* 曲线是衡量加密技术抗选择明文攻击性能的常用指标。*NPCR*、*UACI* 的计算公式为[1]:

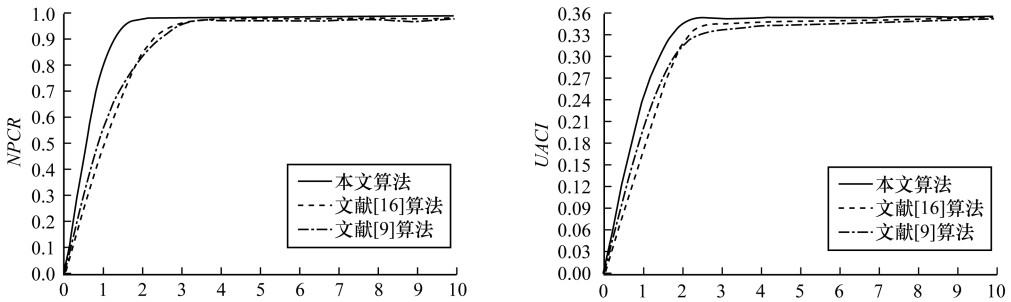
$$NPCR=\frac{\sum_{i=1}^{W}\sum_{j=1}^{H}Difp(I(i,j),I'(i,j))}{W\times H}\times 100\% \quad (18)$$

$$UACI=\frac{1}{W\times H}\left[\sum_{ij}\frac{|I(i,j)-I'(i,j)|}{255}\right]\times 100\% \quad (19)$$

$$Difp(I(i,j),I'(i,j))=\begin{cases}0, I(i,j)=I'(i,j)\\ 1, I(i,j)\neq I'(i,j)\end{cases} \quad (20)$$

其中,W、H 分别是明文的高度、宽度,I、I'分别是2 个明文经加密处理后的 2 个密文,且这 2 个明文都只存在一个相异灰度值。

以图 7(a)作为测试对象,将其位于(65,103)处的像素值 102 修改成 39,从而构成新的图像。利用本文算法、文献[9]算法、文献[15]算法对修改前后的图像进行加密,并基于式(18)~式(20)形成 3 种算法对应的 *NPCR*、*UACI* 曲线,如图 8 所示。由图 8 可以看出,本文算法的抗明文攻击能力最强,其 *NPCR*、*UACI* 值分别为 99.87%、35.94%,均大于文献[9]算法和文献[15]算法。造成该结果的原因是本文光学加密算法的 2 个随机相位掩码均是利用明文像素迭代混沌系统所输出的随机序列来生成,且两级 Gyrator 变换的参数均与明文相关,从而使得整个加密过程都与明文紧密相关,提高了加密密文对明文的敏感性,若非授权用户通过其他明文来解密本文算法的密文,因明文的变换,导致其得到的密钥与正确密钥存在巨大差异,最终无法对密文进行复原。而文献[9]算法与文献[15]算法的加密过程都忽略了明文,导致两者对明文的敏感性较低。



(a)*NPCR*测试结果 (b)*UACI*测试结果

图 8 3 种算法抗选择明文攻击性能测试结果

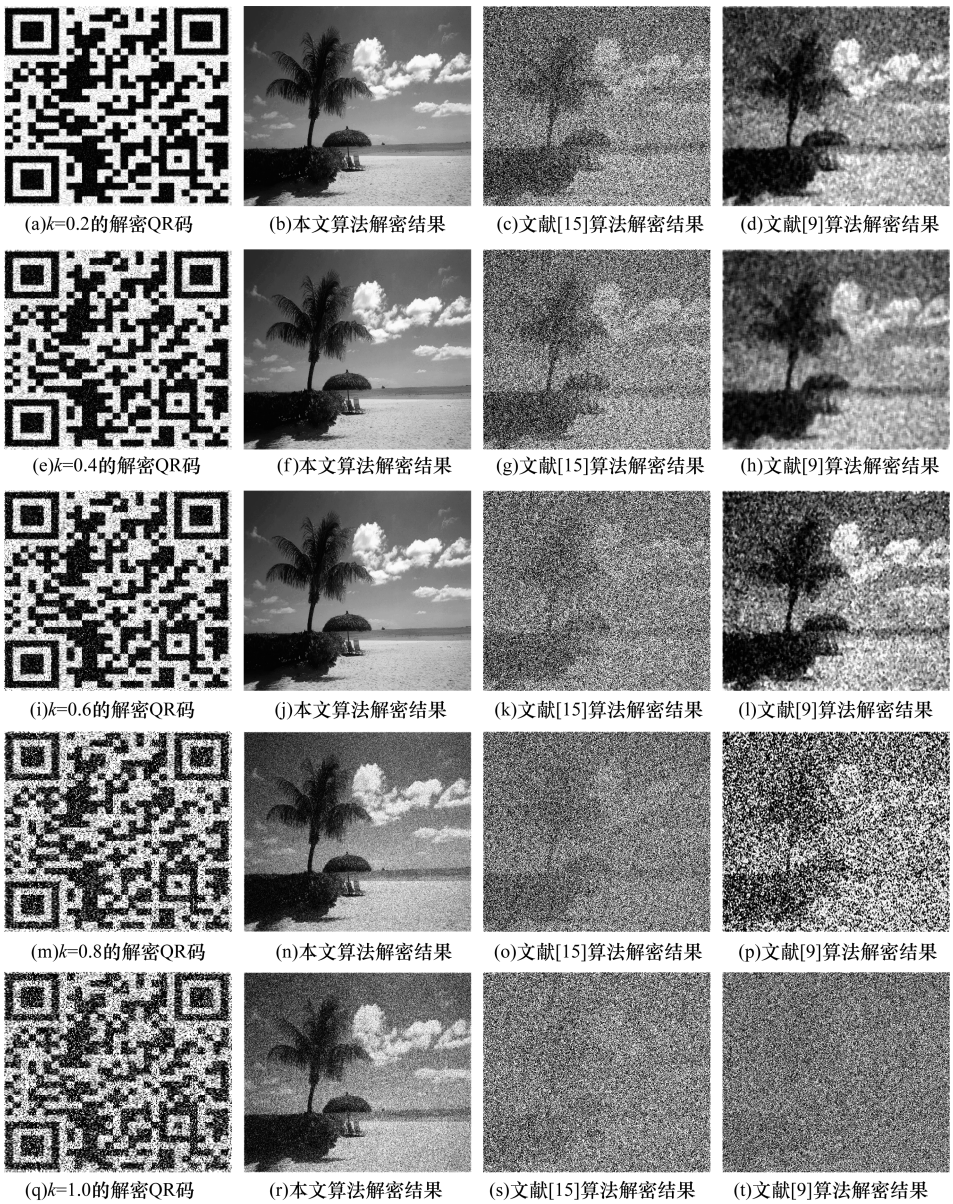
2.3 噪声攻击下的解密效果测试

图像的处理和传输过程都会受到噪声的影响，故加密技术应具备较高的抗噪声攻击能力[15]。本文算法的输出密文为 $C(x'',y'')$，其经过高斯噪声干扰后形成的噪声图像为：

$$C'(x'',y'')=C(x'',y'')[1+kG(x'',y'')] \tag{21}$$

其中，$C'(x'',y'')$是噪声破坏密文，k 是噪声强度系数，$G(x'',y'')$是高斯噪声。

不同 k 值的噪声攻击密文的解密结果如图 9 所示。



(a)k=0.2的解密QR码 (b)本文算法解密结果 (c)文献[15]算法解密结果 (d)文献[9]算法解密结果

(e)k=0.4的解密QR码 (f)本文算法解密结果 (g)文献[15]算法解密结果 (h)文献[9]算法解密结果

(i)k=0.6的解密QR码 (j)本文算法解密结果 (k)文献[15]算法解密结果 (l)文献[9]算法解密结果

(m)k=0.8的解密QR码 (n)本文算法解密结果 (o)文献[15]算法解密结果 (p)文献[9]算法解密结果

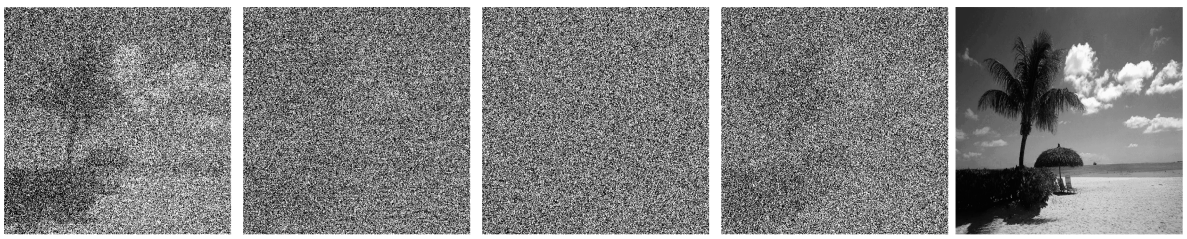
(q)k=1.0的解密QR码 (r)本文算法解密结果 (s)文献[15]算法解密结果 (t)文献[9]算法解密结果

图 9 3 种算法在不同噪声下的解密结果

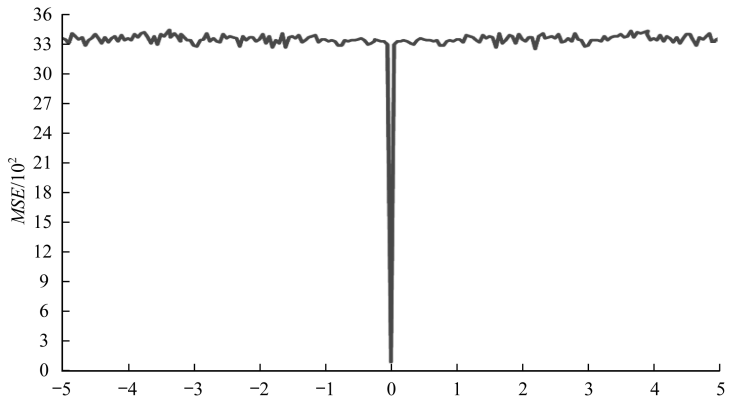
由图 9 可以看出,随着噪声强度的增加,文献[9]算法、文献[15]算法的解密质量逐步下降,均无法得到正确的明文,而本文算法在不同 k 值的噪声攻击下,均可获取可接受的解密质量。在 $k=0.2$、0.4、0.6 时,由于 QR 码具有较强的纠错能力,使本文算法复原图像不受噪声影响,当 k 值继续增大时,虽然复原质量有所下降,但是解密图像视觉质量仍然较好。在 $k=0.8$、1.0 时,文献[9]算法、文献[15]算法解密失败,复原图像质量最差,无法看清图像轮廓,而本文算法的复原图像信息与细节仍然可以接受,这主要归功于 QR 码优越的纠错能力。

2.4　算法敏感性测试

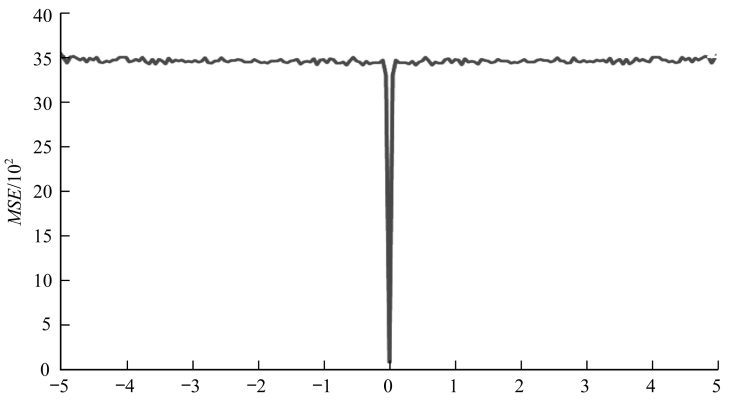
密钥敏感性是评估加密技术安全性的重要指标[2]。为此,本文验证混沌参数 $\alpha=0.45$ 与 $\delta=3.8$时算法的敏感性。先利用篡改因子 $\Delta=10^{-16}$来修改 δ 与 α,得到($\delta-\Delta$)、($\delta+\Delta$)以及($\alpha-\Delta$)、($\alpha+\Delta$),其余密钥保持不变,从而形成 4 组错误密钥。随后,借助正确密钥和这 4 组错误密钥对图 7(c)进行解密,得到 δ、α 的 *MSE* 曲线,结果如图 10 所示。由图 10 可以看出,非授权用户利用 4 组错误密钥对图 7(c)解密时,均不能将其复原,*MSE* 值接近3 500。只有所有密钥完全正确时,才能得到初始明文,如图 10(e)所示,其 *MSE* 曲线出现巨大变化,正确密钥对应的 *MSE* 值趋于 0,如图 10(f)、图 10(g)所示,这表明本文算法具有较强的敏感性,满足严格的“雪崩效应”。



(a)错误密钥($\delta-\Delta$)　(b)错误密钥($\delta+\Delta$)　(c)错误密钥($\alpha-\Delta$)　(d)错误密钥($\alpha+\Delta$)　(e)正确密钥



(f)密钥δ的*MSE*曲线



(g)密钥α的*MSE*曲线

图 10　本文算法敏感性能测试结果

3 结束语

本文利用 QR 码约束与混沌 Gyrator 变换,提出一种新的图像加密算法。在加密过程中,将包含明文所有信息的 QR 码置于 2 个随机相位掩码的输入平面,通过利用由二维耦合混沌映射生成的 2 个随机相位掩码以及 2 个旋转角度,基于两级 Gyrator 变换,将其强度分布视为最终密文,以方便密钥的管理与传输。在解密过程中,将初始 QR 码的三位置检测模式作为支撑约束条件,改进相位检索算法,提高其收敛速度并从密文中重构 QR 码,充分利用 QR 码的纠错能力来提高密文在外来攻击下的解密质量。实验结果验证了本文算法的合理性与优越性。下一步将引入图像融合技术对本文算法进行改进,以实现多图像同步加密并降低传输载荷。

参考文献

[1] NOROUZI B, MIRZAKUCHAKI S. An image encryption algorithm based on DNA sequence operations and cellular neural network[J]. Multimedia Tools and Applications, 2016, 76(11): 13681-13701.

[2] 宋鑫超,苏庆堂,赵永升. 内联时延混沌映射耦合 Lorenz 系统的图像加密算法[J]. 计算机工程与设计, 2016, 37(7): 1757-1761.

[3] 汪彦,涂立. 基于改进 Lorenz 混沌系统的图像加密新算法[J]. 中南大学学报(自然科学版), 2017, 48(10): 2678-2685.

[4] CHAI X, YANG K, GAN Z. A new chaos-based image encryption algorithm with dynamic key selection mechanisms[J]. Multimedia Tools and Applications, 2016, 76(7): 9907-9927.

[5] ÜNAL ÇAVU OĞLU, KAÇAR S, PEHLIVAN I, et al. Secure image encryption algorithm design using a novel chaos based S-Box[J]. Chaos Solitons and Fractals, 2017, 95: 92-101.

[6] 冯雪娇. 基于小波变换的图像加密算法的研究[D]. 哈尔滨:哈尔滨理工大学, 2015.

[7] 宋利. 基于双随机相位编码的光学图像加密方法研究[D]. 成都:电子科技大学, 2016.

[8] LIU X, MEI W, DU H. Optical image encryption based on compressive sensing and chaos in the fractional Fourier domain[J]. Journal of Modern Optics, 2014, 61(19): 1570-1577.

[9] CHEN L, LIU J, WEN J, et al. A new optical image encryption method based on multi-beams interference and vector composition[J]. Optics and Laser Technology, 2015, 69(18): 80-86.

[10] LIU W, LIU Z, LIU S. A symmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm[J]. Optics Letters, 2013, 38(10): 1651-1653.

[11] LIU L F, MIAO S X. A new image encryption algorithm based on logistic chaotic map with varying parameter[J]. SpringerPlus, 2016, 5(1): 1-12.

[12] 彭英杰,陈豪颉. 多特征检测耦合混沌映射的红外图像加密算法[J]. 计算机工程与设计, 2017, 38(11): 3099-3105.

[13] L'ECUYER P, SIMARD R. TestU01: a C library for empirical testing of random number generators[J]. ACM Transactions on Mathematical Software, 2007, 33(4): 22-28.

[14] ZHAO T, RAN Q, YUAN L, et al. Optical image encryption using password key based on phase retrieval algorithm[J]. Journal of Modern Optics, 2016, 63(8): 771-776.

[15] 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.

编辑 吴云芳

(上接第 120 页)

[12] 葛永. 若干安全多方数值计算基础协议的设计[D]. 合肥:安徽大学, 2017.

[13] ARDEHALI M. Quantum oblivious transfer and bit commitment protocols based on two non-orthogonal states coding[J]. Computer Science, 2017, 41(12): 2445-2454.

[14] ZHANG G, LIU L, LIU Y. An attribute-based encryption scheme secure against malicious KGC[C]//Proceedings of the 11th International Conference on Trust, Security and Privacy in Computing and Communications. Washington D. C., USA: IEEE Press, 2012: 1376-1380.

[15] HUR J, KOO D, HWANG S O, et al. Removing escrow from ciphertext policy attribute-based encryption[J]. Computers and Mathematics with Applications, 2013, 65(9): 1310-1317.

[16] 赵圣楠,蒋瀚,魏晓超,等. 一个单服务器辅助的高效 n 取 k 茫然传输协议[J]. 计算机研究与发展, 2017, 54(10): 2215-2223.

编辑 司森森