基于分数阶 Fourier 的双混沌加密算法

汪乐乐 李国东

(新疆财经大学应用数学学院 乌鲁木齐 830012)

摘 要 图像加密在生活中有着重要地位。针对传统的自然混沌系统安全性较低的问题,提出了改进的 H-L 双混沌和分数阶 Fourier 变换的图像加密算法。以穷举法解出的最优解序列的顺序为基础,将混沌映射与分数阶 Fourier 变换结合起来,实现了空间域和频域的置乱,使明文信息得到了隐藏。仿真实验结果表明,通过改进的算法达到了较好的加密效果,其密钥空间大、计算复杂度低、敏感性强,能有效地抵抗统计攻击等,在图形信息安全方面有一定的应用价值。

关键词 离散余弦变换,分数阶 Fourier,背包问题,图像加密,混沌加密

中图法分类号 TP309 **文献标识码** A

Double Chaotic Image Encryption Algorithm Based on Fractional Transform

WANG Le-le LI Guo-dong

(School of Mathematics, Xinjiang University of Finance and Economics, Urumqi 830012, China)

Abstract Image encryption plays an important role in daily life. Aiming at the problem of low security of traditional natural chaos system, an improved image encryption algorithm based on H-L double chaos and fractional Fourier transform was proposed. Based on the order of the optimal solution sequence solved by the exhaustive method, the chaotic map is combined with the fractional Fourier transform. At the same time, it combines with the fractional Fourier transform to realize the scrambling in the spatial and the frequency domains, so that the plain text information is hidden. The simulation results show that the improved algorithm achieves good encryption effect, large key space, low computational complexity, strong sensitivity and effective anti-statistical attack performance. It has certain value in the aspect of graphic information security.

Keywords DCT, Fractional Fourier, Backpack problem, Image encryption, Chaotic encryption

1 引言

现今网络科技迅猛发展,图像作为信息载体,其传递的保密性和安全性得到了密切的关注。但因为某些图像所涵盖的信息涉及个人隐私或为重要机密,甚至牵涉到国家机密,这些信息的泄露会造成经济上的损失甚至更为严重的后果,于是图像信息的保密性更为重要,探索高效、安全的图像加密方法成为热点。广大研究者通过图像的加密技术来解决上述问题,主要原理是利用某种加密过程算法使图像的像素点位置或灰度值发生改变,进而改变图像的整体结构。

混沌系统由于具有初值敏感性、伪随机性等优良的密码学特性,因此国内许多学者在数字图像方面关于混沌加密的文献[2-4]中提到了不同类型的加密设计,常用的经典思想主要分为:像素空间位置置乱、灰度值的扩散变换以及两者的混合。学者对加密进行了研究:从低维到高维的混沌映射、从单一到高维的混沌系统,DNA 码序列的加密等方法成了新的研究热点。DNA 编码将每个像素进行编码 GTCA,可以获得较大的密钥空间,能够抵御常见的攻击。这是生物工程中的计算难题,受实验成本高、计算复杂度高的限制,其实用性不强,并且容易遭到攻击。

黄冬梅等[2]用修正的 Henon 法对遥感图像中每个波段的灰度值进行加密处理,通过检索实验表明该方法的安全性和准确性较好,但存在密文不均的问题,每个波段的加密处理中参数的选择多,较为复杂,需要考虑的因素较多。赵国敏等[3]在以广义 Henon 与 CNN 超混沌系统相结合的基础上用产生的序列进行加密,得出此算法的图像加密抗攻击性强,较为安全。黄清梅等[4]利用细胞神经网络产生的超混沌序列操作图像进行置乱操作,以达到加密的目的,从而得到其置乱度较高、容易实现的结论。谢国波等[5]采用量子 Logistic 混沌与分数阶傅里叶变换解决了传统加密系统简单、伪随机和周期性不好以及易受到攻击等问题。谢国波等[6]采用二维离散 Fourier 变换进行置乱操作,与混沌结合,改善了灰阶直方图不够平滑的缺点。Wang 等[14]提出了一种明文关联的图像加密方案,其使用基本的异或操作处理明文像素点和伪随机序列的值,但这种方案存在大量的迭代循环操作,加密速度慢,其实际应用价值偏低。Ganesan 等[15]于 2014 年提出了明文

本文受国家自然科学基金(11461063),国家社科基金(14BTJ021),新疆维吾尔自治区普通高等学校人文社会科学重点研究基地基金(050315B03),新疆财经大学研究生科研创新项目(XJUFE2017K006,XJGRI2017112),新疆维吾尔自治区自然科学基金(2017D01A24,2017D01A23)资助。

汪乐乐(1993—),女,硕士,主要研究方向为数字分析与图像处理,E-mail:1491658722@qq.com;**李国东**(1976—),男,博士,教授,主要研究方向为数字分析与图像处理,E-mail:lgdzhy@126.com(通信作者)。

关联的图像加密算法，此算法为典型的明文关联，经过循环，可使任意一个明文像素点的信息扩散到整个密文图像中。Cheng 等[16]提出了一种基于混沌映射和 S 盒子的快速图像加密算法，其借助 Tent 映射、循环移位和查找表操作，提升了伪随机序列产生的速度，有效地减少了浮点数运算。

针对当前大多数混沌加密方法是单一混沌系统，被攻击和破译的可能性比较大的问题，文中提出了改进的 H-L 混沌算法。该方法利用 Henon 映射先对图像像素点进行迭代置乱，打乱行和列，再将置乱矩阵与行阵相乘后进行 x 方向的 α 阶 DFRFT 变换，与列阵相乘后进行 y 方向的 β 阶 DFRFT 变换，从而得到加密矩阵，并将其嵌入到 Hilbert 分数阶图像中，以合成密文图像；Logistic 混沌映射对变换后的密文图像进行扩散加密运算，采用穷举法解决背包问题得到的全局最优方案的序列来处理，改进的混沌算法按照最佳方案的序列顺序依次进行运算。该方法克服了一些传统方法只在频域、空间域、和单一的混沌系统作用于某一方案而导致的结构简单、伪随机的产生和参数变量少的问题。仿真实验表明，相比于传统的加密算法，该算法具有更高的安全性和抗攻击性。在混沌映射算法原有优点的基础上，用一种利用穷举法解出背包问题最优解的序列来结合两种混沌映射加密算法，以避免单一化加密算法的不安全、易攻破加密图像的现象。该改进的混沌加密方法计算较为简单，操作易于实现，解密程度较为困难，无论是从理论分析还是计算机仿真方面都可以对其进行验证。

2 本文算法及原理

2.1 加密原理

本文针对传统的自然混沌和单一混沌系统的安全性不高等问题，提出了穷举法最优解序列和分数阶 Fourier 变换混沌的图像加密算法。在穷举法的最优解问题上，将最优解序列应用于改进的 H-L 混沌映射算法，将混沌系统和 Fourier 变换结合起来，置乱效果好，避免了能轻易破解的问题，不但增大了加密图像的解密难度，而且提高了加密信息的安全级别。文中改进的算法先采用 Henon 映射对图像的数字矩阵进行迭代处理以产生两个序列，截取前 M 项序列，并对其进行升序排序，得到行置乱矩阵($ind1$)和列置乱矩阵($ind2$)，打乱原数字矩阵的行和列，得到加密箱矩阵(ea)，然后用加密箱矩阵与行置乱矩阵相乘后进行水平方向上的 α 阶 DFRFT 变换，将变换后的矩阵与列阵相乘后继续竖直方向上的 β 阶 DFRFT 变换，最后将得到的密文图像嵌入 Hilbert 梯度图像，完成改进的 Henon 映射；Logistic 映射对密文图像进行异或运算再加密，最终改进 H-L 算法按照序列的顺序进行加密处理。该方法解决了其安全级别不高和易破解的问题，经过模拟仿真，该方法比传统加密具有更高的安全级别。

2.2 加密实现

加密过程的流程如图 1 和图 2 所示。

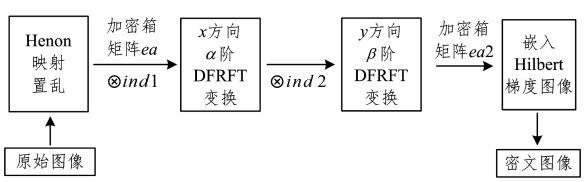


图 1 改进的 Henon 加密流程

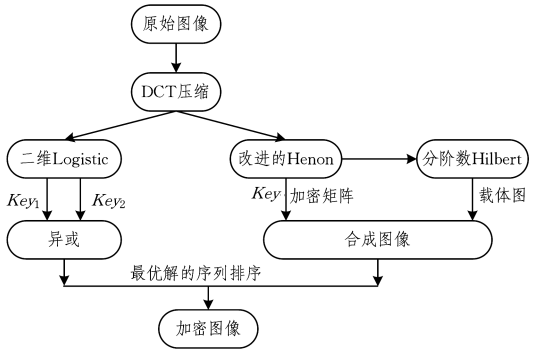


图 2 图像加密流程图

改进算法的主要步骤如下：

(1)像素的提取操作，获取样本图像的像素数字矩阵，提取图片信息；对目标样本图像进行 DCT 变换。

(2)Henon 映射迭代产生混沌序列 $ind1=x_1,x_2,\cdots,x_m$；$ind2=y_1,y_2,\cdots,y_m$，截取 M 项得到序列 $C=\{c_m\mid k=i+1,\cdots,m\}$，$D=\{d_k\mid k=i+1,\cdots,m\}$，打乱明文图像的数字矩阵 ea，得到加密箱矩阵。

(3)将数字矩阵 ea 与置乱后的行阵和列阵相乘得到图像矩阵 R。与行阵相乘后进行 x 方向上的 α 阶 DFRFT 变换，然后与列阵相乘后进行 y 方向上的 β 阶 DFRFT 变换，从而获得加密复数矩阵。通过式(1)得到幅度谱：

$$|F(m,n)=[R^2(m,n)+I^2(m,n)]^{1/2}| \tag{1}$$

其中，$R(m,n)$ 是实数部分，$I(m,n)$ 是虚数部分。然后通过式(2)、式(3)将加密复矩阵逆变换从频域转到空间域。

$$F(m,n)=\sum_{x=0}^{M-1}\sum_{y=0}^{M-1}f(x,y)\mathrm{e}^{-j2\pi(\frac{mx}{M}+\frac{ny}{M})} \tag{2}$$

$$F(m,n)=|F(m,n)|e^{j\varphi(m,n)} \tag{3}$$

其中，$F(m,n)$为频率分布函数，$|F(m,n)|$为其幅度谱。

(4)密文图像经过 Henon 映射嵌入载体图像(Hilbert 梯度图)，从而得到新的加密图像。

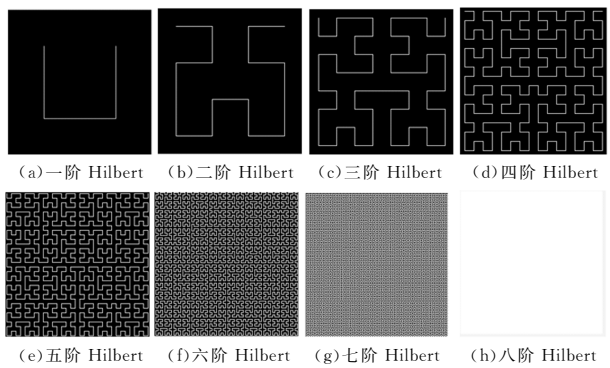
(5)将新的密文图作为新一轮的样本，经过 Logistic 的异或运算，得到二次密文图像。

(6)按照求解出的最优序列的顺序进行加密，最终得到多次加密的最终图像。

(7)解密：加密的逆过程，此处不再赘述。

在 Henon 混沌映射算法中，将 Hilbert 曲线作为载体图像，在进行不同阶段的加密过程时，进行局部加密。因为 Hilbert 的图像在梯度变化时具有遍历性的特性，所以选取 8 幅 Hilbert 图像作为载体图像。

图 3 给出载体图像的 Hilbert 曲线图，在进行 Henon 混沌映射算法的过程时，用不同阶数的 Hilbert 曲线进行图像的融合加密过程，以达到加密的效果。



(a)一阶 Hilbert (b)二阶 Hilbert (c)三阶 Hilbert (d)四阶 Hilbert

(e)五阶 Hilbert (f)六阶 Hilbert (g)七阶 Hilbert (h)八阶 Hilbert

图 3 Hilbert 曲线梯度图

3　改进系统的混沌映射及 Fourier 变换

3.1　DCT 变换

将二维离散余弦变换(Discrete Cosine Transform，DCT)用于图像变换。假设有 $M\times N$ 矩阵，定义为：

$$B_{p,q}=a_p a_q\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}A_{m*n}\cos\frac{\pi(2n+1)p}{2N},0\leqslant p\leqslant M-1,\ 0\leqslant q\leqslant N-1 \tag{4}$$

$$a_p=\begin{cases}\dfrac{1}{\sqrt{M}}, & p=0\\ \sqrt{\dfrac{2}{M}}, & 1\leqslant q\leqslant M-1\end{cases} \tag{5}$$

$$a_q=\begin{cases}\dfrac{1}{\sqrt{N}}, & q=0\\ \sqrt{\dfrac{2}{N}}, & 1\leqslant q\leqslant N-1\end{cases} \tag{6}$$

其中，B 是矩阵 A 的 DCT 系数。在基于快速傅里叶(FFT)上，对图像进行逆离散余弦变换，将 DCT 变换值不大于 20 的系数设为 0，经过逆变换得到重构后的图像。

3.2　Henon 映射(Hilbert 为载体图像)

Henon 映射是一个二维非线性映射系统。Henon 算法利用混沌序列将图像矩阵的行和列打乱，如动力学方程(见式(7))所示：

$$\begin{aligned}x_{n+1}&=1-ax_n^2+y_n\\ y_{n+1}&=bx_n\end{aligned} \tag{7}$$

其中，使 Henon 处于混沌状态时的参数控制为 $a=1.4$，$b=0.3$，Lyapunov 指数等于 0.418，取 Henon 映射的密钥 $k=-0.40001$。使用密钥作为初始值，得到两个混沌序列，然后将明文图像的序列打乱，并截取 X 项，按照冒泡法将序列从小到大排序，得到按照混沌序列加密后的图像。最后将对应阶数的 Hilbert 曲线的图像进行嵌入，从而构成合成图像，将 Hilbert 图像与 11110000=240 逐位运算，将加密后的图像进行相同维数的 240 逐位运算，并把加密后的图像的高 8 位移到低 8 位，再将加密后的图像嵌入载体图像(即 Hilbert 图像)的低 8 位，从而构成合成图像。

Henon 映射分叉的效果如图 4 所示。

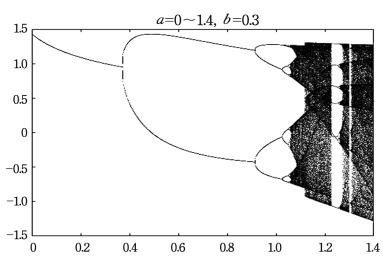


图 4　Henon 映射分叉的效果图

3.3　Logistic 映射

Logistic 映射是一种典型的动力系统，对 Logistic 映射的迭代操作会出现混沌的现象。Logistic 的分立形式方程如下所示：

$$x_{n+1}=ux_n(1-x_n),u\in[0,4],x\in[0,1] \tag{8}$$

Logistic 混沌映射的初值选取为 0.2915826302，映射的参数选取 $u=4.0$，通过异或操作对图像进行混沌加密，并在下一过程中再一次使用异或操作进行解密。

3.4　Fourier 变换

随着分数阶 Fourier 基本理论的完善和发展，“任意”函数通过一定的分解，能够表示为正弦函数的线性组合形式，其已经普遍应用于通信技术、密码学领域。用 FFT 来计算 FRFT，其函数定义如下：

$$X_p=F^p[x(t)]=\int_{-\infty}^{+\infty}x(t)K_p(u,t)\mathrm{d}t \tag{9}$$

其中，分数阶 Fourier 变换的核函数如下：

$$K_p(u,t)=\begin{cases}\sqrt{\dfrac{1-j\cot\alpha}{2\pi}}\exp\left[j\left(\dfrac{u^2+v^2}{2\pi}\cot\alpha-\dfrac{ut}{\sin\alpha}\right)\right], & \alpha\neq n\pi\\ \delta(t-u), & \alpha=2n\pi\\ \delta(t+u), & \alpha=(2n\pm1)\pi\end{cases} \tag{10}$$

其中，α 为变换的角度，p 为参数，当 $p=1$ 时，其为传统 Fourier 变换，$p=0$ 时其是信号自身。在图像处理中，需要转换为离散的形式，二维连续分数阶 Fourier 为：

$$X_{p1,p2}(u,v)=\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}x(s,t)K_{p1,p2}(s,t,u,t)\mathrm{d}s\mathrm{d}t \tag{11}$$

其中，$x(s,t)$ 为原始二维信号，那么二维变换的核方程如下：

$$K_{p1,p2}(s,t,u,t)=\frac{\sqrt{1-j\cot\alpha}\sqrt{1-j\cot\beta}}{2\pi}\times\exp\left[j\left(\frac{s^2+u^2}{2}\cot\alpha-\frac{su}{\sin\alpha}\right)\right]\exp\left[j\left(\frac{t^2+v^2}{2}\cot\beta-\frac{tv}{\sin\beta}\right)\right] \tag{12}$$

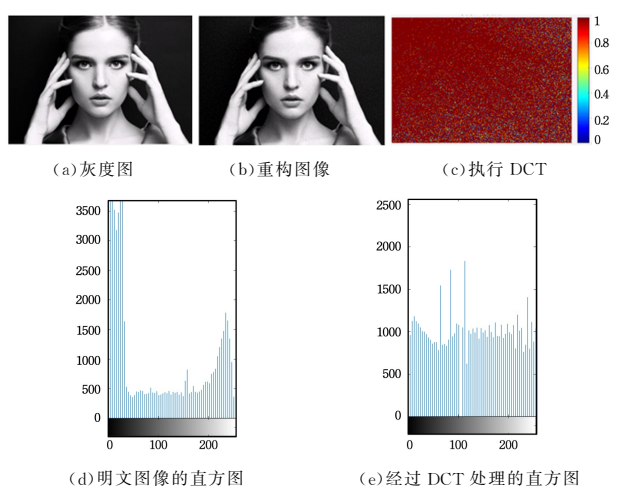
基于分数阶 Fourier 的可分离性，二维 Fourier 变换可分离为两个分别在 x 方向和 y 方向的一维分数阶 Fourier 换阶。

4　仿真实验

4.1　DCT 重构图像

对明文图像进行 DCT 处理，获取对明文图进行重构的图像。

如图 5 所示，图 5(a)为灰度图，运用 DCT 方法处理并行逆变换得到重构图像(见图 5(b))，得到的能量分布 DCT 结果如图 5(c)所示，明文图像和 DCT 处理后的直方图如图 5(d)和图 5(e)所示。纵览直方图，由未经过 DCT 处理的原图的直方图可知，明文图像的能量分布不均匀，主要分布于左上角，并且整体上其前一段和下一段的能量为 0；而经过 DCT 处理后的能量分布是均匀的，这也就说明 DCT 的处理效果是比较好的。



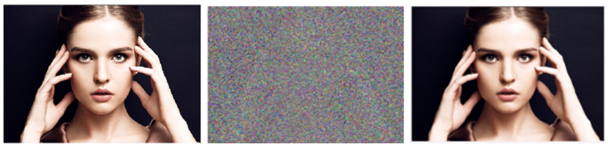
(a)灰度图　(b)重构图像　(c)执行 DCT

(d)明文图像的直方图　(e)经过 DCT 处理的直方图

图 5　DCT 变换的实验结果

4.2 Logistic 混沌的加密操作

采用 Logistic 方法对明文图像进行加密，其中加密次数为 1 次，得到的加密效果如图 6 所示。



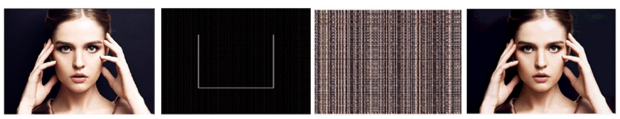
(a)明文原图 (b)加密图 (c)解密图像

图 6 经 Logistic 加密的效果图

利用 Logistic 混沌映射对如图 6(a)所示的明文图像进行加密处理，经过一次 Logistic 混沌加密处理后得到图 6(b)，保密图像中虽然已经很难看出具体的局部信息，但是其总体的外轮廓较为明显，这就需要再一次进行混沌映射处理，以达到很难分析图像的程度。经过一次 Logistic 映射，得到的密文图中已经很难解读要传递的信息。经过 Logistic 混沌映射逆变换得到的解密图像为图 6(c)。

4.3 Henon 混沌的加密图像(载体图像为 1 阶 Hilbert 图像)

Henon 映射对明文图像(见图 7(a))进行加密，其中载体图像是经过 Hilbert 一阶处理后得到的图像(见图 7(b))，经过一次 Henon 映射得到的加密图如图 7(c)所示，一次加密后已经看不出明文的特征，说明加密是相对有效的，经过 Henon 混沌映射的逆过程得到解密后的图像(见图 7(d))。

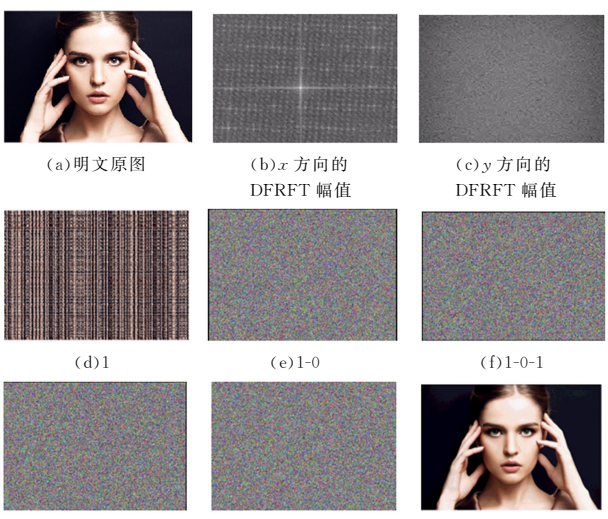


(a)明文原图 (b)一阶 Hilbert 载体图 (c)一次 Henon 加密图 (d)解密图像

图 7 经 Hilbert 加密的效果图

4.4 经过最优解排序的实验仿真

选取人脸图像 Smark(256×256)的彩色图像作为实验测试的仿真对象，图像加密算法是在 Matlab2016a 环境下进行实验仿真的。实验中的密钥数据：Henon 映射初始密 0.100111140001，控制参数 $\alpha=1.4$，$\beta=0.3$，Logistic 的初始值 $x_0=0.2915826302$，$x_0=y_0$，设定 0-logistic，1-henon，采用穷举法解背包问题得到的最优解序列为{1,0,1,1,0,0,0,1}。



(a)明文原图 (b)x 方向的 DFRFT 幅值 (c)y 方向的 DFRFT 幅值

(d)1 (e)1-0 (f)1-0-1

(g)1-0-1-1 (h)最终加密图像 (i)解密图像

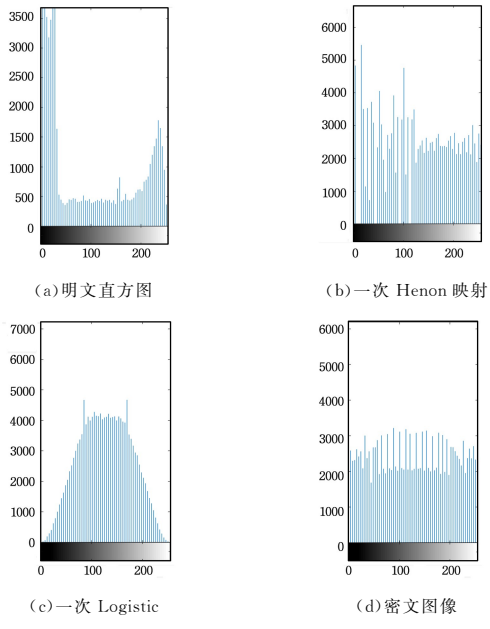
图 8 给定排序后的加密效果图

图 8(a)为明文图像，图 8(b)是 x 方向的 DFRFT 加密幅值，图 8(c)是 y 方向的 DFRFT 加密幅值，图 8(d)是以一阶 Hilbert 梯度为载体的 Henon 加密图像，图 8(e)为 Logistic 对密文的二次加密图像，图 8(f)和图 8(g)为按照最优解排序的密文图像，图 8(f)为二阶 Hilbert 梯度的载体图像进行 Henon 加密得到的图像；图 8(g)是以三阶 Hilbert 梯度图作为载体进行 Henon 加密得到的加密图像；按照排列顺序最终解密图如图 8(h)和图 8(i)所示。在经过多次的加密过程处理后，在加密的最终图像中分辨原图的特征是相当困难的。从进行加密的图像仿真结果来看，加密后的图像完全看不出图像特征，并且按照加密的序列顺序，经过一次加密和二次加密的图像更难辨别图像的识别度，按照序列的最终加密图像已杂乱无章，可见加密的效果较好。

5 结果检验——性能分析

5.1 密文统计特性分析

对于直方图的分析，每一个像素值出现的概率越小，图像的安全性就越稳定；能量分布有很大的不同，灰度值出现的概率有明显的差异，加密后的像素出现的频率基本相同，随着序列次数的增加，密文直方图像素的能量分布越均匀；密文图像的直方图更加平稳，波动程度小，并且分布的均匀程度也有很大的改善，基本掩盖了原始图像的分布规律，更增加了破译的广度和难度，并有效地抵抗攻击。



(a)明文直方图 (b)一次 Henon 映射

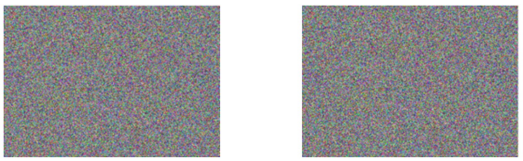
(c)一次 Logistic (d)密文图像

图 9 实验样本图像的直方图

5.2 密钥敏感性分析

(1)Logistic 和 Henon 映射具有复杂的动态性能，其密钥、参数的选择具有敏感性，即使微弱的数字差，也会得到完全不同的密文图像；将 Logistic 的混沌密钥 Key 增加 0.000000000000001，解密将会发生错误，如图 10(a)所示，并且 Logistic 混沌映射的异或操作也容易导致解密错误。

(2)基于最优解序列顺序的选取也大大地增加了不确定性，提升了破译的难度，增强了图像的安全程度。同时，在解密时，若没有按照加密时的排列顺序，或者将顺序颠倒，进行了错误的解密顺序，解密时也将会发生错误，如图 10(b)所示。



(a)Logistic 的 Key 发生错误的解密图　(b)序列的逆顺序发生错误的解密图

图 10　发生错误的解密图像

(3)NPCR 与 UACI：NPCR(像素改变率)表示当明文中任意像素值发生微小变化或密钥发生微小的变动时，密文产生显著改变，其像素值发生变化的比率；UACI 为平均改变强度的归一化值。D_1 表示密文，D_2 为明文图像像素值发生改变时的密文，其公式为：

$$NPCR=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)}{M\times N}\times 100\% \tag{13}$$

$$UACI=\frac{1}{M\times N}\times\left[\sum_{i}\sum_{j}\frac{|D_1(i,j)-D_2(i,j)|}{256}\right]\times 100\% \tag{14}$$

任取明文图像的一点坐标，对其进行微小的转化，如将像素点(7,125)转化为(7,136)，由式(13)和式(14)可知，此时 $NPCR=98.78\%$，$UACI=32.99\%$。综上，改进算法对明文具有很强的敏感性和抗差分攻击能力。

表 1　NPCR 与 UACI

	本文算法	文献[5]算法	文献[6]算法
$NPCR$	0.99895363	0.99893162	0.9964
$UACI$	0.337869893	0.334836967	0.3378

5.3　信息熵分析

信息熵分析用于描述信息的不确定性。图像灰度值分布得越均匀，信息熵就越大。信息熵的计算公式如下所示：

$$H(m)=-\sum_{i=0}^{255}p(m_i)\log_2 p(m_i) \tag{15}$$

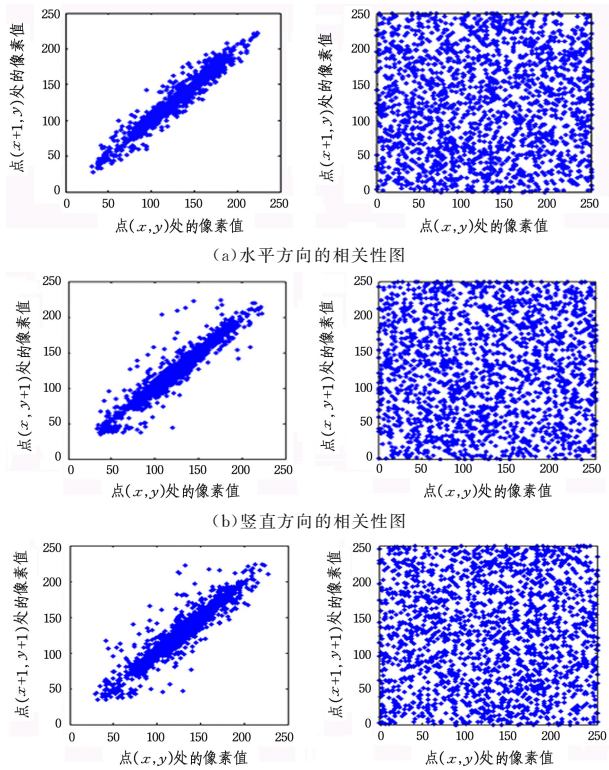
其中，$p(m_i)$是灰度值为 m_i 出现的概率，此时有$\sum_{i=0}^{255}p(m_i)=1$，信息熵越接近于 8，说明它的抗攻击性越好，表述的是每个像素值出现的概率越接近，则灰度值分布越均匀，进而说明抗统计攻击性越好。信息熵是表示所有灰度值出现的概率相等时出现的最大值，最大值为 8。在改进的加密算法上的信息熵 $H=7.8892$，加密前的信息熵 $H=7.2639$，可以看出加密后的信息熵更接近 8，说明改进算法能够较好地抵抗统计攻击。

5.4　相邻像素的相关系数

相邻像素的相关系数是用来反映像素的扩散程度。密文的相关系数越接近于 0，说明效果越好，密文图像越安全。为了验证明文图和密文图相邻像素的相关性，在两幅图中随机选取 1000 对在水平、垂直和对角方向上的像素对，测试其相关系数。图 11 表示明文与密文中相邻像素值在水平、竖直、对角方向的相关性关系。从图中看出，明文有明显的线性关系，密文图像相邻点之间几乎没有任何关系。

$$R_{AB}=\frac{\sum_{m}\sum_{n}(A_{mn}-\overline{A})(B_{mn}-\overline{B})}{\sqrt{(\sum_{m}\sum_{n}(A_{mn}-\overline{A})^2)(\sum_{m}\sum_{n}(B_{mn}-\overline{B})^2)}} \tag{16}$$

表 2 列出了明文图与密文图相邻像素之间的相关系数，像素对随机选取。从这些数据可以看出，原图的相关性很高，接近于 1，而密文相关系数接近于 0，表明该算法将明文中相邻像素点之间的相关性已完全打乱，基本不相关，像素点几乎是随机分布的；密文的相关系数远小于明文，说明改进算法的抗统计能力很强，按照此方法加密的效果比较好。



(a)水平方向的相关性图

(b)竖直方向的相关性图

(c)对角方向的相关性图

图 11　明文与密文的相邻像素相关性散点图

表 2　相关系数

方向	原图	加密图像	文献[5]算法	文献[6]算法
水平	0.9903	−0.0221	0.0009	0.0012
垂直	0.9933	−0.0074	−0.0013	−0.0026
对角	0.9888	0.0075	−0.0026	0.0035

5.5　密钥空间分析

在此算法中，密钥为双精度型，采用了双混沌映射的初值及参数作为初始条件的密钥，参数选择至少达到 10^{64}，为算法提供了较大的密钥空间，很难破解此密文图像。

5.6　经典攻击类型分析

在进行加密的过程中，密码攻击者对密钥或密码进行破译。其中，在对图像进行破解的过程中获得了其加密算法，此称之为 Kerckhoff 假设。其攻击对象如下：

(1)唯密文攻击，即攻击者对密文信息具有一定的了解，而对明文一无所知。

(2)已知明文攻击，即攻击者了解密文和部分明文与密文的对应关系。

(3)选择明文攻击，即攻击者了解加密算法，可以选择明文并得到相应明文对应的密文信息。

(4)选择密文攻击，即攻击者了解加密算法，可以选择密文并得到对应的明文。

显然，选择明文攻击是有效的攻击方法，加入加密算法能够有效地抵制这种方法的攻击，也就能有效地抵制其他方法的攻击。然而其对文中算法是不适用的，本文算法通过明文图像产生，想要通过二维图像中像素值为 0 的矩阵进行破译基本上是不成立的；并且，本文算法中对于密钥的敏感性是极高的，当其出现了 10^{-10} 的微小差别时，便无法对密文图像进行破解。综上所述，本文的加密算法能够有效地抵制选择明文攻击。

结束语　文中提出的加密算法是基于 Windows 10 操作

(下转第 401 页)

[3] PAGE L. The PageRank citation ranking: Bringing order to the web[J]. Stanford Digital Libraries Working Paper, 1998, 9(1): 1-14.

[4] HAVELIWALA T H. Topic-Sensitive PageRank: A Context-Sensitive Ranking Algorithm for Web Search[J]. IEEE Educational Activities Department, 2003, 15(4): 784-796.

[5] TONG H H, FALOUTSOS C, PAN J Y. Fast Random Walk with Restart and Its Applications[C]// Proceedings of the Sixth International Conference on Data Mining (ICDM 06). IEEE Computer Society, 2006: 613-622.

[6] HERLOCKER J L, KONSTAN J A, TERVEEN L G, et al. Evaluating collaborative filtering recommender systems [J]. 2004, 22(1): 5-53.

[7] BOBADILLA J, SERRADILLA F. A new collaborative filtering metric that improves the behavior of recommender systems [J]. Knowledge-Based Systems, 2010, 23(6): 520-528.

[8] 王成，朱志刚，张玉侠，等. 基于用户的协同过滤算法的推荐效率和个性化改进[J]. 小型微型计算机系统，2016，37(3)：428-432.

[9] VINODHINI S, RAJALAKSHMI V, GOVINDARAJULU B. Building Personalised Recommendation System With Big Data and Hadoop Mapreduce [J]. Metabolism Clinical & Experimental, 2009, 58(1): 38-46.

[10] RODRIGUES C M, RATHI S, PATIL G. An efficient system using item & user-based CF techniques to improve recommendation[J]. International Conference on Next Generation Computing Technologies, 2017, 10(1): 569-574.

[11] LIAO C L, LEE S J. A clustering based approach to improving the efficiency of collaborative filtering recommendation [J]. Electronic Commerce Research & Applications, 2016, 18: 1-9.

[12] FERNÁNDEZ P. Google's pagerank and beyond: The science of search engine rankings [J]. Mathematical Intelligencer, 2008, 30(1): 68-69.

[13] BRIN S, PAGE L. The anatomy of a large-scale hypertextual Web search engine[J]. International Conference on World Wide Web, 1998, 56(18): 107-117.

[14] ANDERSON R, FAN C, LANG K. Local Graph Partitioning using PageRank Vectors[J]. IEEE Symposium on Foundations of Computer Science, 2006, 47(5): 475-486.

[15] SPIELMAN D, TENG S H. Nearly-linear time algorithms for graph partitioning, graphsparsification, and solving linear systems[J]. Data Structures and Algorithms, 2004, 2(3): 81-90.

[16] FERRAGINA P. A personalized search engine based on web-snippet hierarchical clustering[J]. Software Practice & Experience, 2010, 38(2): 189-225.

[17] VERMA D, MEILA M. A comparison of spectral clustering algorithms[D]. Washington: University of Washington, 1997.

[18] SHI J, MALIK J. Normalized cuts and image segmentation[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2000, 22(8): 888-905.

[19] KANNAN R, VEMPALA S, VETA A. On clusterings-good, bad and spectral[C]// Proceedings of the IEEE Symposium on Foundations of Computer Science. 2000: 367-377.

(上接第 397 页)

系统，主要借助 Matlab R2016a 作为实验平台，利用了改进的双混沌算法，结合了分数阶 Fourier 变换将时域和空间域特性连接的最优解序列的分数阶 Fourier 的双混沌算法。改进算法先采用 Henon 混沌对像素点进行迭代，通过置乱操作得到加密箱，加密箱与行阵进行矩阵乘法后对 x 方向进行 α 阶 DFRFT 变换，再与列阵相乘后进行 y 方向上的 β 阶 DFRFT 变换，得到的图像与 Hilbert 梯度图像进行 Henon 映射，从而得到加密图像。Logistic 映射通过异或运算得到加密图像，Hilbert 梯度图的选取是利用穷举法解背包问题的最优解的排序，文中序列为给定的已得的最优解。该算法解决了传统的自然系统在单一领域内使用某一方法而削减了参量导致系统结构简单、易被攻击、安全性的问题。改进算法的密钥空间变大、计算冗乱度较低、敏感性强、安全性级别高，在图像传输方面具有先进性。综上，该算法不仅有很好的加密效果，而且有非常强的抗破译能力。

参 考 文 献

[1] ADLEMAN L M. Molecular Computation of Solutions to Combinatorial Problems [J]. Science, 1994, 266(5187): 1021-1024.

[2] 黄冬梅，耿霞，魏立斐. 基于 Henon 映射的加密遥感图像的安全检索方案 [J]. 软件学报，2016，27(7)：1729-1740.

[3] 赵国敏，李国东. 基于广义 Henon 映射以及 CNN 超混沌系统图像加密方案 [J]. 信阳师范学院学报自然科学版，2015，15(1)：141-145.

[4] 黄清梅，李国东. 基于 CNN 超混沌特性对图像加密技术的应用研究 [J]. 绵阳师范学院学报，2017，2(2)：60-66.

[5] 谢国波，杨彬. 基于比特置乱的量子混沌图像加密算法[J]. 计算机工程，2017，43(7)：182-186.

[6] 谢国波，王添. 基于像素置乱和比特替换的混沌图像加密算法[J]. 微电子学与计算机，2016，33(3)：80-85.

[7] 徐兵，袁立. 基于改进 Logistic 混沌映射的数字图像加密算法研究[J]. 计算机测量与控制，2014，22(7)：165-167.

[8] 郭伟创，叶瑞松. 一种基于猫映射和伯努利移位映射的图像加密算法[J]. 汕头大学学报(自然科学版)，2015，30(1)：13-23.

[9] 张雪锋，范九伦. 一种改进的基于混沌系统的数字图像加密算法[J]. 计算机应用研究，2007，24(4)：184-186.

[10] 郑凡，田小建，范文华，等. 基于 Henon 映射的数字图像加密[J]. 北京邮电大学学报，2008，31(1)：66-70.

[11] 韩风英，李云. 利用复合混沌系统的图像加密方案研究与设计[J]. 电脑知识与技术，2010，6(13)：3450-3452.

[12] 李凯佳，俞锐刚，袁凌云. 基于 DNA-记忆元胞自动机与 Hash 函数的图像加密算法 [J]. 计算机工程与设计，2017，38(2)：470-477.

[13] 廖春成，周小平，廖春龙，等. 像素位置与比特双重置乱的混沌图像加密算法 [J]. 中国科技论文，2014(1)：112-116.

[14] WANG X Y, WANG T. A novel algorithm for image encryption based on couple chaotic systems [J]. International Journal of Modern Physics B, 2012, 26(30): 395.

[15] GANESAN K, MURALI K. Image encryption using eight dimensional chaotic cat map [J]. European Physical Journal Special Topics, 2014, 223(8): 1611-1622.

[16] CHENG P, YANG H, WEI P, et al. A fast image encryption algorithm based on chaotic map and lookup table [J]. Nonlinear Dynamics, 2014, 79(3): 2121-2131.

[17] LI G D, WANG L L. Double chaotic image encryption algorithm based on optimal sequence solution and fractional transform[J]. Visual Computer, 2018, 1(1): 1-11.