基于不可逆分数阶离散映射的图像加密算法

刘晓君,王普,鲁晨浩

(西安邮电大学 理学院,西安 710121)

摘 要:基于分数阶离散映射系统的混沌特性,提出了一种基于分数阶循环移位彩色图像加密算法.该算法首先通过利用伪随机发生器产生随机的二进制序列与原彩色图像关联,产成各层随机的初始值参数,其次利用分数阶离散映射产生混沌序列,对彩色图像的红、绿、蓝通道分别进行循环移位置乱加密和扩散运算,最后利用产生的伪随机二进制序列和混沌序列控制对各层的加密矩阵进行矩阵变换,得到加密图像.仿真结果表明,相邻像素的相关性系数近似为 0,信息熵、像素变化率和归一化像素灰度值平均改变强度的平均值分别为 7.997 8、99.609%和 33.442%.该算法具有良好的可靠性和抗攻击能力,能够有效地提高图像的安全性.

关键词:分数阶离散映射;图像加密;循环移位加密;矩阵变换

中图分类号:TP309.7 **文献标志码**:A **文章编号**:1000-2367(2024)05-0117-09

在信息安全领域中,混沌图像加密算法一直是混沌密码学的研究热点之一.自 1997 年 FRIDRICH 将混沌引入图像加密以来[1],大量基于混沌图像的加密算法不断涌现.在图像加密技术的初期阶段,许多基于整数阶混沌映射的加密算法被提出,例如经典的 Logistic 映射和 Hénon 映射[2-5].随后,许多学者还提出了基于整数阶多维连续系统的加密算法[6-7].与整数阶混沌系统相比,分数阶非线性系统有着更大的参数取值空间,该特性增大了密钥空间,从而提高了加密系统的安全性[8-9].因此,将分数阶系统引入到图像加密中已经逐渐成为信息安全领域的研究热点.

文献[10]提出了一种基于分数阶 Chen 系统的图像加密算法,该算法主要利用混沌置乱和混沌掩盖的技术对图像进行加密,得到了较好的加密效果.文献[11]研究了一种基于分数阶 Rössler 混沌系统的图像加密算法,该算法主要依靠混沌系统的阶数和参数来实现加密,该方法在很大程度上提高了密钥空间.在文献[12]中,作者提出了利用变形分数阶 Lorenz 系统对原图像进行滤波处理,然后利用安全 Hash 算法产生置乱和扩散的密钥,将密钥与明文图像联系起来优化了抵御选择明文攻击的能力.文献[13]提出基于 4 维超混沌系统的彩色图像加密算法,首先利用反向传播神经网络相结合产生随机序列,对彩色图像像素置乱和扩散实现加密.以上这些文献都是基于分数阶连续系统进行了图像加密研究.

作为分数阶系统的重要组成部分,分数阶离散映射系统是 21 世纪初才逐渐被人们所重视的分数阶系统,其形式简单,动力学行为丰富.基于此,本文提出了一种基于分数阶离散混沌系统的图像加密算法.该算法首先利用伪随机器产生随机的二进制序列,将其与原彩色图像关联,生成各层随机的系统初始值.在此基础上,利用分数阶离散混沌系统产生的混沌序列,将原彩色图像像素点矩阵 3 层通道各自进行行列循环加密和扩散处理.最后,利用产生二进制随机序列和混沌序列,随机选取不同的矩阵组合方式进行矩阵变换,实现

收稿日期:2023-10-09;**修回日期**:2023-11-22.

基金项目:国家自然科学基金(11702194);陕西省自然科学基金(2023-JC-YB-075).

作者简介(通信作者):刘晓君(1980—),女,黑龙江齐齐哈尔人,西安邮电大学副教授,主要研究方向为非线性系统的图像加密,E-mail:flybett3952@126.com.

引用本文:刘晓君,王普,鲁晨浩.基于不可逆分数阶离散映射的图像加密算法[J].河南师范大学学报(自然科学版),2024,52(5):117-125.(Liu Xiaojun,Wang Pu,Lu Chenhao.An image encryption algorithm based on a fractional-order discrete noninvertible map[J].Journal of Henan Normal University(Natural Science Edition),2024,52(5):117-125.DOI:10.16366/j.cnki.1000-2367.2023.10.09.0002.)

彩色图像加密.该方法通过随机的系统初值,增强了抵抗差分攻击的能力且接近理想值,具有良好的安全性能.

1 系统描述

本文利用文献[14]中提出了一个分数阶不可逆离散系统,其形式如下

$$\begin{cases} {}_a^C\Delta_a^{\upsilon}x(t)=y(t-1+\upsilon)-x(t-1+\upsilon), \\ {}_a^C\Delta_a^{\upsilon}y(t)=b(-x^3(t-1+\upsilon)+x(t-1+\upsilon))+c(-y^3(t-1+\upsilon)+ \\ \qquad y(t-1+\upsilon))-y(t-1+\upsilon), \end{cases} \tag{1}$$

其中,$0<\upsilon\leq 1$ 表示系统的阶数,系统的数值解可表示为

$$\begin{cases} x(n)=x(a)+\dfrac{1}{\Gamma(\upsilon)}\displaystyle\sum_{j=1}^{n}\frac{\Gamma(n-j+\upsilon)}{\Gamma(n-j+1)}(y(j-1)-x(j-1)), \\ y(n)=y(a)+\dfrac{1}{\Gamma(\upsilon)}\displaystyle\sum_{j=1}^{n}\frac{\Gamma(n-j+\upsilon)}{\Gamma(n-j+1)}(b(-x^3(j-1)+x(j-1))+c(-y^3(j-1)+y(j-1))-y(j-1)). \end{cases}$$

在下文,积分下限 a 设定为 0.系统参数取 $b=2.2,c=0.95$,当分数阶数取 $\upsilon=0.84,\upsilon=0.95,\upsilon=0.98$ 时,系统(1)的混沌吸引子见附录图 S1.当系统参数分别变化,分数阶数 $\upsilon=0.98$ 时,系统(1)的分岔图见附录图 S2.

利用美国国家标准与技术研究院(National Institute of Standards and Technology,NIST)对映射(1)的产生的序列值进行随机性测试,结果见表 1.测试结果显示,映射(1)生成的随机数性能优异,适合用于密码系统的随机密钥流生成.

表 1 NIST 测试结果

Tab. 1 NIST test results

测试项目	映射(1)测试结果	测试项目	映射(1)测试结果	测试项目	映射(1)测试结果
单比特频率	0.771 105	二进制矩阵阶	0.617 370	近似熵	0.366 209
块内频率	0.022 785	离散傅里叶变换	0.309 788	随机偏离	0.243 975
累积和	0.900 481	非重叠模板匹配	0.135 553	随机偏离变量	0.350 413
游程	0.196 977	重叠模板匹配	0.243 975	串行	0.217 160
块内最长 1 游程	0.252 935	通用统计	0.075 719	线性复杂度	0.124 202

2 算法设计

本文提出的彩色图像加密算法为对称加密体制,其解密过程是加密的逆过程,其中 R(红),G(绿),B(蓝)通道的置乱扩散过程与各自的参数有关.首先,该算法通过使用伪随机发生器产生随机的二进制序列,并生成各层随机的映射(1)迭代的初始值.其次,利用映射(1)产生的混沌序列,对原彩色图像的像素点矩阵的 3 个通道进行循环加密、扩散加密以及矩阵变换,从而实现彩色图像的加密.该算法加密流程见图 1.

2.1 密钥生成与混沌系统初值

设原始图像为彩色图像,其大小为 $M\times N$.将该彩色图像进行 R,G,B 分层,分别得到图像 $\boldsymbol{P}_{\mathrm{R}}$,图像 $\boldsymbol{P}_{\mathrm{G}}$,图像 $\boldsymbol{P}_{\mathrm{B}}$.

利用伪随机发生器生成的 256 bit 的二进制序列 $\boldsymbol{Q}$,将二进制序列 $\boldsymbol{Q}$ 进行分组,每 16 位为一组,并将其转换为十进制序列得到序列 $\boldsymbol{Q}^1$,将该十进制序列首尾相加.并将得到的序列分成两行分别为记为 $\boldsymbol{Q}^2$ 和 $\boldsymbol{Q}^3$.

通过计算 $\begin{cases} S=\mathrm{sum}(\boldsymbol{Q}^2) \\ S'=\mathrm{sum}(\boldsymbol{Q}^3) \end{cases}$,得到系统的初始值 $\begin{cases} x_n=\dfrac{Q_n^2}{S}-\lfloor\dfrac{Q_n^2}{S}\rfloor, x_n'=\dfrac{Q_n^3}{S'}-\lfloor\dfrac{Q_n^3}{S'}\rfloor, \\ y_n=\dfrac{Q_n^2}{S}-\lfloor\dfrac{Q_n^2}{S}\rfloor, y_n'=\dfrac{Q_n^3}{S'}-\lfloor\dfrac{Q_n^3}{S'}\rfloor, \end{cases}$ $n=1,2,3,4$. 其中,sum(·)表示求和,$\lfloor\cdot\rfloor$表示取整. $x_n,x_n',y_n,y_n',n=1,2,3$,用于对彩色图像各层进行循环加密和扩散加密,$x_4,y_4$ 用于矩阵变换环节.

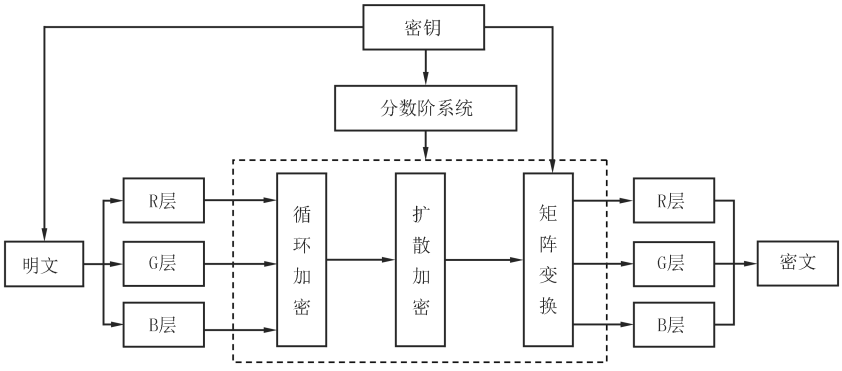


图1　图像加密流程

Fig.1　Image encryption process

2.2　循环加密及扩散加密

将初值 $x_n,y_n(n=1,2,3)$ 代入映射(1)迭代 T_n+M+N 次,其中 T_n 为预迭代值,由此产生各层的混沌序列 $\boldsymbol{o}_n,\boldsymbol{s}_n$. 对各层分别进行循环加密,具体的算法步骤如下.

步骤 1　利用下式分别计算得到用于行循环和列循环的混沌序列

$$\begin{cases}x_n^r=\lfloor \mathrm{mod}(\boldsymbol{o}_n(T_n+1:M)\times 10^4,255)\rfloor+1,\\ x_n^c=\lfloor \mathrm{mod}(\boldsymbol{o}_n(T_n+M+1:T_n+M+N)\times 10^4,255)\rfloor+1,\\ y_n^r=\lfloor \mathrm{mod}(\boldsymbol{s}_n(T_n+1:M)\times 10^4,255)\rfloor+1,\\ y_n^c=\lfloor \mathrm{mod}(\boldsymbol{s}_n(T_n+M+1:T_n+M+N)\times 10^4,255)\rfloor+1.\end{cases}$$

步骤 2　将像素点向右移动 x_n^r 步

$$\begin{cases}\boldsymbol{C}_r=\boldsymbol{P}_{\mathrm{R,G,B}}(i,1:N-x_n^r),\\ \boldsymbol{P}_{\mathrm{R,G,B}}(i,1:x_n^r)=\boldsymbol{P}_{\mathrm{R,G,B}}(i,N-x_n^r+1:N),\\ \boldsymbol{P}_{\mathrm{R,G,B}}(i,x_n^r+1:N)=\boldsymbol{C}_r.\end{cases}$$

再对图像各通道的第 i 行像素灰度值进行行替代加密 $\boldsymbol{P}_{\mathrm{R,G,B}}(i,:)=\boldsymbol{P}_{\mathrm{R,G,B}}(i,:)\oplus y_n^r$.

步骤 3　将像素点向上移动 x_n^c 步

$$\begin{cases}\boldsymbol{C}_r=\boldsymbol{P}_{\mathrm{R,G,B}}(1:M-x_n^c,j)\\ \boldsymbol{P}_{\mathrm{R,G,B}}(1:x_n^c,j)=\boldsymbol{P}_{\mathrm{R,G,B}}(M-x_n^c+1:M,j),\\ \boldsymbol{P}_{\mathrm{R,G,B}}(x_n^c+1:M,j)=\boldsymbol{C}_r.\end{cases}$$

再对图像各通道的第 j 列像素灰度值进行列替代加密 $\boldsymbol{P}_{\mathrm{R,G,B}}(:,j)=\boldsymbol{P}_{\mathrm{R,G,B}}(:,j)\oplus y_n^c$.

步骤 4　利用随机产生的系统初值 $x_n',y_n'(n=1,2,3)$,迭代产生各层的混沌序列 $\boldsymbol{o}_n',\boldsymbol{s}_n'$,对各层分别进行扩散加密.将映射(1)迭代次 $T_n'+M+N$,其中 T_n' 为预迭代值,将产生的迭代值进行如下处理

$$\begin{cases}\boldsymbol{X}_n^r=\lfloor \mathrm{mod}(\boldsymbol{o}_n'(T_n'+1:M)\times 10^4,255)\rfloor+1,\\ \boldsymbol{X}_n^c=\lfloor \mathrm{mod}(\boldsymbol{o}_n'(T_n'+M+1:T_n'+M+N)\times 10^4,255)\rfloor+1,\\ \boldsymbol{Y}_n^r=\lfloor \mathrm{mod}(\boldsymbol{s}_n'(T_n'+1:M)\times 10^4,255)\rfloor+1,\\ \boldsymbol{Y}_n^c=\lfloor \mathrm{mod}(\boldsymbol{s}_n'(T_n'+M+1:T_n'+M+N)\times 10^4,255)\rfloor+1.\end{cases}$$

其中,$\boldsymbol{X}_n^r,\boldsymbol{Y}_n^r$ 表示用于行扩散的混沌序列;$\boldsymbol{X}_n^c,\boldsymbol{Y}_n^c$ 表示用于列扩散的混沌序列.

步骤 5　对图像 $\boldsymbol{P}_{\mathrm{R,G,B}}$ 的第 i 行 $\boldsymbol{P}_{\mathrm{R,G,B}}(i,:)$ 和第 j 列 $\boldsymbol{P}_{\mathrm{R,G,B}}(:,j)$ 按照 $\boldsymbol{P}_{\mathrm{R,G,B}}(i,:)=\boldsymbol{P}_{\mathrm{R,G,B}}(i,:)\oplus\boldsymbol{X}_n^r\oplus\boldsymbol{Y}_n^r,\boldsymbol{P}_{\mathrm{R,G,B}}(:,j)=\boldsymbol{P}_{\mathrm{R,G,B}}(:,j)\oplus\boldsymbol{X}_n^c\oplus\boldsymbol{Y}_n^c$ 进行行和列扩散加密.

在上述步骤中,将原始图像进行分层,对每层图像的像素点分别进行循环和扩散处理,以实现加密的效果.

2.3　矩阵变换

本小节主要阐述算法中的矩阵变换部分.首先从 $\boldsymbol{Q}$ 中随机选取 5 个序列值求和得到 δ.根据 δ 的不同大

小,将彩色图像的 3 层矩阵进行不同组合.利用混沌序列对矩阵进行变换,然后将其分割成 3 个矩阵.最后合并这 3 个矩阵,生成最终的加密矩阵 $\boldsymbol{F}$. 算法步骤如下.

步骤 1 根据 δ 的不同大小,对零矩阵 $\boldsymbol{C},\boldsymbol{V}_1,\boldsymbol{V}_2$ 矩阵进行赋值,其中 $\boldsymbol{C}$ 矩阵的大小为 $M\times 2N$,$\boldsymbol{V}_1$ 和 $\boldsymbol{V}_2$ 大小 $M\times(N/2)$,$\boldsymbol{V}_1=P_B(:,1{:}N/2)$ 表示 $\boldsymbol{P}_B$ 矩阵中 1 到 $N/2$ 的所有数值.

若 $\delta=0$,$\boldsymbol{C}=[\boldsymbol{P}_{\mathrm{R}},\boldsymbol{P}_{\mathrm{G}}]$,$\boldsymbol{V}_1=\boldsymbol{P}_{\mathrm{B}}(:,1{:}N/2)$,$\boldsymbol{V}_2=\boldsymbol{P}_{\mathrm{B}}(:,N/2+1{:}N)$;

若 $\delta=1$,$\boldsymbol{C}=[\boldsymbol{P}_{\mathrm{R}},\boldsymbol{P}_{\mathrm{B}}]$,$\boldsymbol{V}_1=\boldsymbol{P}_{\mathrm{G}}(:,1{:}N/2)$,$\boldsymbol{V}_2=\boldsymbol{P}_{\mathrm{G}}(:,N/2+1{:}N)$;

若 $\delta=2$,$\boldsymbol{C}=[\boldsymbol{P}_{\mathrm{G}},\boldsymbol{P}_{\mathrm{R}}]$,$\boldsymbol{V}_1=\boldsymbol{P}_{\mathrm{B}}(:,1{:}N/2)$,$\boldsymbol{V}_2=\boldsymbol{P}_{\mathrm{B}}(:,N/2+1{:}N)$;

若 $\delta=3$,$\boldsymbol{C}=[\boldsymbol{P}_{\mathrm{G}},\boldsymbol{P}_{\mathrm{B}}]$,$\boldsymbol{V}_1=\boldsymbol{P}_{\mathrm{R}}(:,1{:}N/2)$,$\boldsymbol{V}_2=\boldsymbol{P}_{\mathrm{R}}(:,N/2+1{:}N)$;

若 $\delta=4$,$\boldsymbol{C}=[\boldsymbol{P}_{\mathrm{B}},\boldsymbol{P}_{\mathrm{R}}]$,$\boldsymbol{V}_1=\boldsymbol{P}_{\mathrm{G}}(:,1{:}N/2)$,$\boldsymbol{V}_2=\boldsymbol{P}_{\mathrm{G}}(:,N/2+1{:}N)$;

若 $\delta=5$,$\boldsymbol{C}=[\boldsymbol{P}_{\mathrm{B}},\boldsymbol{P}_{\mathrm{G}}]$,$\boldsymbol{V}_1=\boldsymbol{P}_{\mathrm{R}}(:,1{:}N/2)$,$\boldsymbol{V}_2=\boldsymbol{P}_{\mathrm{R}}(:,N/2+1{:}N)$.

步骤 2 将初值 x_4,y_4 带入映射(1)产生长度为 $M+N$ 的混沌序列 $\boldsymbol{o}_4$ 和 $\boldsymbol{s}_4$.再将将混沌序列前 M 个值赋给 $\boldsymbol{x}^r$ 和 $\boldsymbol{y}^r$,将后 N 个值赋给 $\boldsymbol{x}^c$ 和 $\boldsymbol{y}^c$.对 $\boldsymbol{x}^r,\boldsymbol{y}^r,\boldsymbol{x}^c,\boldsymbol{y}^c$ 进行索引和处理.其中,$\boldsymbol{x}^r,\boldsymbol{y}^r$ 用于矩阵行变换,$\boldsymbol{x}^c,\boldsymbol{y}^c$ 用于矩阵列变换.

步骤 3 将后 $N/2$ 个混沌序列值 $\boldsymbol{o}_4$ 的平均值 κ 作为判断条件.

若 $\boldsymbol{o}_4(i)\geq\kappa$,$\boldsymbol{L}=[\boldsymbol{V}_1(:,i),\boldsymbol{C},\boldsymbol{V}_2(:,i)]$,若 $\boldsymbol{o}_4(i)<\kappa$,$\boldsymbol{L}=[\boldsymbol{V}_2(:,i),\boldsymbol{C},\boldsymbol{V}_1(:,i)]$.将得到的 $\boldsymbol{L}$ 矩阵的第 i 行像素与 $\boldsymbol{x}^r$ 进行替代加密并向右移动 $\boldsymbol{y}^r$ 步.再将转置后的 $\boldsymbol{L}$ 矩阵第 j 列像素与 $\boldsymbol{x}^c$ 进行替代加密并向上移动 $\boldsymbol{y}^c$ 步.得到变换后的矩阵 $\boldsymbol{L}$.

步骤 4 将 $\boldsymbol{L}$ 矩阵进行分割,得到 $\boldsymbol{P}'_{\mathrm{R}},\boldsymbol{P}'_{\mathrm{G}},\boldsymbol{P}'_{\mathrm{B}}$ 矩阵,得到最终的加密矩阵 $\boldsymbol{F}$.

解密算法步骤是加密的算法步骤的逆过程.对密文图像依次进行矩阵逆变换,逆向扩散,逆向循环移位即可得到解密后的图像.

3 性能分析

3.1 数值仿真

本实验中采用的彩色图像 Erna 作为原始图像,其来源于作者创作,为了丰富图像内容,将 4 张图片进行组合拼接为一张.为了进一步验证该加密方法的正确性,从 USC-SIPI 图像数据库(https://sipi.usc.edu/database/)中选择了几幅图像进行图像加密.为了减少随机误差的影响,提高实验结果的可靠性和准确性,本文中对相邻像素的相关性系数、像素变化率(number of pixels change rate,NPCR,R_{n})和归一化像素灰度值平均改变强度(unified average changing intensity,UACI,I_{u})以及信息熵的计算均基于 5 000 次测试结果的平均值.

加密和解密结果见图 2.其中 Erna 图像和 Black 图像大小为 256 像素×256 像素,Peppers 图像和 Lena 图像大小为 512 像素×512 像素.加密图像类似于噪声.

3.2 直方图分析

直方图反映了图像最基本的统计特征.在图 3 中显示了本实验中 Erna 原始图像和加密图像的分布直方图.加密图像的像素灰度值分布平坦且均匀.这表明所提出的加密方案能够有效抵御常见的统计攻击.与文献[15]中加密图像的直方图对比,本文中所提出的方法像素灰度值分布具有同样效果.

3.3 效率分析

在本节分析了该算法的效率,由于分数阶微积分算子的全局特性,使得计算量较整数阶系统稍大.尤其是在处理大尺寸图像时,系统需要处理更多的像素点和数据量,进而增加了算法运行时间.将不同尺寸的 Erna 图像作为测试图像,并与基于整数阶系统设计的文献[16－19]的加密算法进行比较,其中文献[16]是利用图像分层置乱彩色图像,文献[17]是利用行列组合交叉循环移位置乱加密图像,文献[18]是利用图像像素分割方案加密图像,文献[19]是利用自适应扩散策略得到加密图像,得到的测试结果如表 2 所示.

3.4 相关性分析

由于原始图像具有一定的相关性,降低图像的相邻像素之间的相关性才能抵抗攻击.相邻像素之间的相

关性越小说明加密效果越好.相邻相关系数值的大小直接表明像素间相邻相关性的强弱.

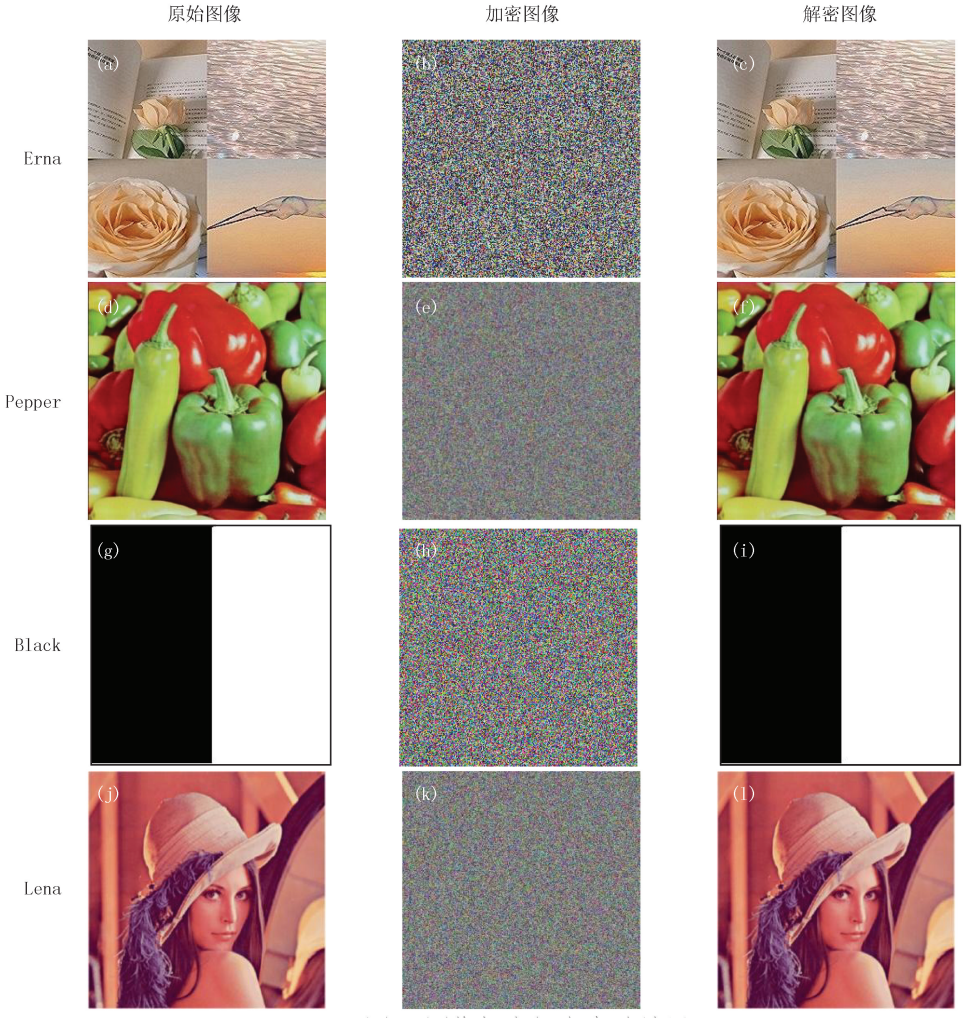


图2　图像加密解密实验结果

Fig. 2　Experimental results of image encryption and decryption

表 2　对不同尺寸图像的执行时间分析

Tab. 2　Execution time analysis for images of different sizes　　s

图像大小	本文	文献[16]	文献[17]	文献[18]	文献[19]
256 像素×256 像素×3 通道	0.862 3	0.054 2	0.471 5	0.745 0	0.533 5
512 像素×512 像素×3 通道	2.556 1	0.333 5	1.841 9	1.878 2	1.796 4
1 024 像素×1 024 像素×3 通道	3.641 2	0.938 4	2.945 6	3.275 6	3.144 7

相邻像素的相关性系数 $R_{\boldsymbol{h}\boldsymbol{h}'}=\mathrm{cov}(\boldsymbol{h},\boldsymbol{h}')/\sqrt{D(\boldsymbol{h})D(\boldsymbol{h}')}$,其中,$\boldsymbol{h}=\{h_k,k=1,2,\cdots,m\}$ 为图像矩阵中随机挑选的 m 个像素的灰度值,$\boldsymbol{h}'$ 为 $\boldsymbol{h}$ 的 m 个相邻像素;协方差 $\mathrm{cov}(\boldsymbol{h},\boldsymbol{h}')=\frac{1}{m}\sum_{i=1}^{m}[h_i-E(\boldsymbol{h})][h'_i-E(\boldsymbol{h}')]$;方差 $D(\boldsymbol{h})=\frac{1}{m}\sum_{i=1}^{m}[h_i-E(\boldsymbol{h})]^2$;$E$ 为期望.

为了比较原始图像和加密图像中相邻像素的相关性,本文计算了这些像素在水平、垂直和对角方向上的相邻像素的相关性系数.具体的计算结果见表 3.根据表 3 的结果可以看出,本文算法产生的加密图像的相关性系数明显降低,表明本文提出的算法能够有效地抵抗统计性分析.

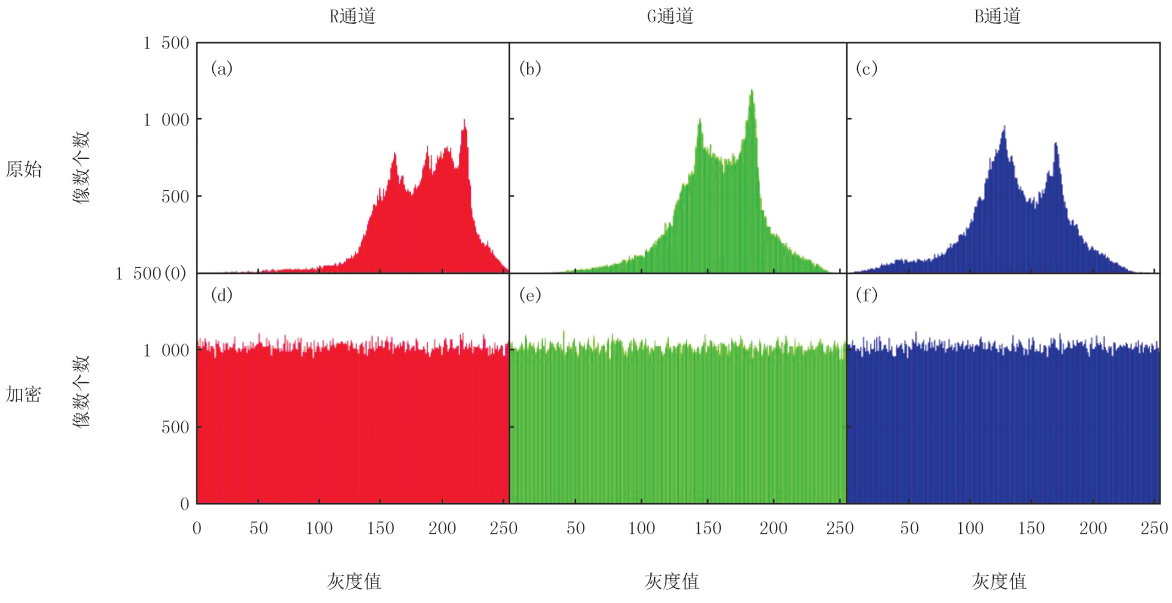


图3 Erna图像及其加密图像的直方图

Fig.3 Histogram of Erna images and their encrypted images

表 3 加密图像的相邻像素的相关性系数

Tab. 3 Correlation coefficient of adjacent pixels of the encrypted images

算法	图像	水平方向相关性系数			垂直方向相关性系数			对角方向相关性系数		
		R 通道	G 通道	B 通道	R 通道	G 通道	B 通道	R 通道	G 通道	B 通道
本文	Lena	−0.001 7	−0.001 7	0.001 1	0.001 9	−0.002 3	−0.006 4	0.003 0	0.004 5	0.007 7
本文	Peppers	−0.002 6	−0.001 6	−0.000 5	−0.002 3	0.004 4	0.000 7	0.001 1	−0.005 2	0.002 9
文献[20]	Lena	−0.002 2	−0.002 5	0.002 5	0.002 1	−0.004 8	−0.006 3	0.001 8	0.006 9	0.007 1
文献[21]	Lena	−0.005 0	−0.005 0	−0.002 0	0.005 6	−0.006 2	0.001 0	0.003 6	−0.001 2	−0.001 2
文献[22]	Peppers	0.002 7	0.001 1	−0.003 6	−0.001 7	−0.008 5	0.007 0	0.000 4	0.000 7	0.000 5
文献[23]	Peppers	0.001 6	0.003 6	−0.001 6	−0.005 5	0.004 5	−0.006 8	0.005 5	−0.003 6	0.006 4

3.5 差分攻击分析

对于一种有效的加密方案,即使原始图像存在微小的差异,也会导致加密图像发生巨大的变化.在差分攻击分析中,采用 R_n 和 I_u

$$R_n(U_1,U_2)=\frac{1}{MN}\sum_{i,j}^{M,N}D(i,j),$$

$$I_u(U_1,U_2)=\frac{1}{MN}\sum_{i}^{M}\sum_{j}^{N}\left|\frac{U_1(i,j)-U_2(i,j)}{255}\right|,$$

$$D(i,j)=\begin{cases}0, & U_1(i,j)=U_2(i,j),\\ 1, & U_1(i,j)\neq U_2(i,j),\end{cases}$$

来分析抵御选择明文攻击的能力,其中,U_1 和 U_2 是两幅待比较的加密图像.理想状态下 $R_n\approx 99.609\%$,$I_u\approx 33.463\%$.

先使用本文中的加密算法对原始图像进行加密并生成加密图像 U_1,接着从原始图像中随机选取 3 000 个像素,将其灰度值加 1,再对图像进行加密,得到加密图像 U_2.最后通过比较 U_1 和 U_2,计算它们的 R_n 和 I_u,结果如表 4 所示.同时从原始图像中随机抽取 100 个像素,并将其像素灰度值随机加 1 或减 1,再对图像进行加密,计算 R_n 和 I_u,结果如表 5 所示.

表 4　两幅加密图像之间的 R_n 和 I_u

Tab. 4　R_n and I_u of two encrypted images　　%

图像	R_n			I_u		
	R 通道	G 通道	B 通道	R 通道	G 通道	B 通道
Erna	99.605	99.609	99.606	33.449	33.453	33.436
Lena	99.608	99.610	99.609	33.452	33.425	33.408
Peppers	99.608	99.610	99.612	33.462	33.420	33.476

由表 4 和表 5 可知,本文算法的加密结果与理论值接近,表现出了良好的抵抗差分攻击的性能.

表 5　两幅加密图像之间的 R_n 和 I_u

Tab. 5　R_n and I_u of two encrypted images　　%

算法	图像	R_n			I_u		
		R 通道	G 通道	B 通道	R 通道	G 通道	B 通道
本文	Lena	99.611	99.611	99.612	33.474	33.464	33.461
本文	Peppers	99.614	99.613	99.604	33.456	33.444	33.456
文献[15]	Lena	99.648	99.658	99.629	33.439	33.479	33.483
文献[20]	Lena	99.629	99.617	99.647	33.603	33.499	33.552
文献[21]	Lena	99.619	99.638	99.600	33.429	33.455	33.428
文献[22]	Peppers	99.582	99.596	99.643	33.462	33.623	33.404
文献[23]	Peppers	99.605	99.605	99.619	33.454	33.418	33.466

将 3 通道的全白和全黑图像,按照本文的加密算法进行加密,得到加密结果和直方图(附录图 S3).结果证明本文的加密算法能够对全白和全黑图像进行加密,说明该加密算法具有抵抗差分攻击的能力.

3.6　信息熵分析

信息熵反映了图像信息的不确定性,信息熵越大,不确定性就越大,可视信息就越少.信息熵

$$H=-\sum_{h}^{l}P(h)\log_2 P(h),$$

其中,l 为图像的灰度等级数,$P(h)$表示灰度值 h 出现的概率.在本文中,将彩色图像进行分层后,对 3 层分量分别进行信息熵分析,得到的结果如表 6 所示.

表 6　原始图像和加密图像的信息熵

Tab. 6　Information entropy of the original image and encrypted image

加密算法	图像	加密图像			加密算法	图像	加密图像		
		R 通道	G 通道	B 通道			R 通道	G 通道	B 通道
本文	Lena	7.998 8	7.998 9	7.997 0	文献[21]	Lena	7.991 2	7.991 4	7.991 5
本文	Peppers	7.997 4	7.997 4	7.997 0	文献[22]	Peppers	7.997 2	7.997 4	7.997 3
文献[15]	Lena	7.999 4	7.999 3	7.999 4	文献[23]	Peppers	7.997 2	7.997 5	7.997 4
文献[20]	Lena	7.999 4	7.999 3	7.999 2					

由表 6 可知,加密图像的各层信息熵均接近于理论值 8,而原始图像的各层信息熵与理论值有明显差别,所以本文的加密算法具有良好的安全性.

4　结　语

本文提出了一种基于不可逆分数阶离散映射的彩色图像加密算法.该算法利用伪随机器产生的二进制序列与原始图像的各个层进行关联,产生每层各自的系统初值,利用不可逆分数阶离散映射对每层的图像进行循环移位置乱和扩散加密.再利用产生的二进制序列和混沌序列,控制对 R、G 和 B 通道的加密矩阵进行矩阵变换,从而生成加密图像.实验结果和性能分析表明,该算法的 R_n、I_u 和加密图像的信息熵分别约为

99.609%、33.463%和 8,具有良好的安全性和可靠性,能够有效抵抗外部差分攻击和熵攻击.

附录见电子版(DOI:10.16366/j.cnki.1000-2367.2023.10.09.0002).

参 考 文 献

[1] FRIDRICH J.Image encryption based on chaotic maps[C]//IEEE International Conference on Systems,Man,and Cybernetics.Computational Cybernetics and Simulation.Piscataway:IEEE Press,1997:1105-1110.

[2] 王勇,杨锦,王瑛.改进 Hénon 超混沌系统与 AES 结合的图像加密算法[J].计算机工程与应用,2019,55(22):180-186.
WANG Y,YANG J,WANG Y.Image encryption algorithm based on improved henon hyperchaotic system combined with AES algorithm [J].Computer Engineering and Applications,2019,55(22):180-186.

[3] 王红涛,冯连强,王志超,等.基于 Hénon 映射置换的彩色图像加密算法[J].重型机械,2020(1):16-20.
WANG H T,FENG L Q,WANG Z C,et al.Color image encryption algorithm based on Hénon mapping permutation[J].Heavy Machinery,2020(1):16-20.

[4] 曾祥秋,叶瑞松.基于改进 Logistic 映射的混沌图像加密算法[J].计算机工程,2021,47(11):158-165.
ZENG X Q,YE R S.Chaotic image encryption algorithm based on improved logistic map[J].Computer Engineering,2021,47(11):158-165.

[5] 纪元法,李菊,孙希延,等.基于改进二维混沌映射的彩色图像加密算法[J].计算机仿真,2023,40(4):180-185.
JI Y F,LI J,SUN X Y,et al.A color image encryption algorithm based on improved 2D chaotic map[J].Computer Simulation,2023,40(4):180-185.

[6] WANG T,SONG L W,WANG M H,et al.A novel image encryption algorithm based on parameter-control scroll chaotic attractors[J].IEEE Access,2020,8:36281-36292.

[7] 庄志本,李军,刘静漪,等.基于新的五维多环多翼超混沌系统的图像加密算法[J].物理学报,2020,69(4):50-63.
ZHUANG Z B,LI J,LIU J Y,et al.Image encryption algorithm based on new five-dimensional multi-ring multi-wing hyperchaotic system [J].Acta Physica Sinica,2020,69(4):50-63.

[8] LYUBOMUDROV O,EDELMAN M,ZASLAVSKY G M.Pseudochaotic systems and their fractional kinetics[J].International Journal of Modern Physics B,2003,17(22/23/24):4149-4167.

[9] 王丰,邵珠宏,王云飞,等.gyrator 变换域的高鲁棒多图像加密算法[J].中国图象图形学报,2020,25(7):1366-1379.
WANG F,SHAO Z H,WANG Y F,et al.Multiple image encryption of high robustness in gyrator transform domain[J].Journal of Image and Graphics,2020,25(7):1366-1379.

[10] 王雅庆,周尚波.基于分数阶陈氏混沌系统的图像加密算法[J].计算机应用,2013,33(4):1043-1046.
WANG Y Q,ZHOU S B.Image encryption algorithm based on fractional-order Chen chaotic system[J].Journal of Computer Applications,2013,33(4):1043-1046.

[11] 张毅,王波.基于分数阶 Rossler 混沌序列的图像加密[J].计算机与现代化,2019(12):119-122.
ZHANG Y,WANG B.Image encryption based on fractional rossler chaotic sequence[J].Computer and Modernization,2019(12):119-122.

[12] 马英杰,陈棱峣,赵耿,等.基于变形分数阶 Lorenz 混沌系统的图像加密算法[J].计算机应用与软件,2023,40(2):308-313.
MA Y J,CHEN D Y,ZHAO G,et al.Image encryption algorithm based on deformed fractional Lorenz chaotic system[J].Computer Applications and Software,2023,40(2):308-313.

[13] 方鹏飞,黄陆光,娄苗苗,等.基于四维超混沌系统的彩色图像加密算法[J].计算机工程与设计,2022,43(2):361-369.
FANG P F,HUANG L G,LOU M M,et al.Color image encryption algorithm based on four dimensional hyper chaotic system[J].Computer Engineering and Design,2022,43(2):361-369.

[14] LIU X J,HONG L,YANG L X,et al.A fractional-order discrete noninvertible map of cubic type:dynamics,control,and synchronization [J].Complexity,2020,2020:2935192.

[15] HUA Z Y,ZHU Z H,YI S,et al.Cross-plane colour image encryption using a two-dimensional logistic tent modular map[J].Information Sciences,2021,546:1063-1083.

[16] TANG J N,ZHANG Z Z,CHEN P Y,et al.An image layered scrambling encryption algorithm based on a novel discrete chaotic map[J].IET Image Processing,2023,17(2):518-532.

[17] TENG L,WANG X Y,YANG F F,et al.Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion[J].Nonlinear Dynamics,2021,105(2):1859-1876.

[18] LAI Q,HU G W,ERKAN U,et al.A novel pixel-split image encryption scheme based on 2D Salomon map[J].Expert Systems with Applications,2023,213:118845.

[19] HU Y S,NAN L Y.Image encryption algorithm based on 1D-SFACF with cross-cyclic shift and adaptive diffusion[J].Physica Scripta,

2023，98(5)：055209.

[20] KUMAR PATRO K A，ACHARYA B.An efficient colour image encryption scheme based on 1-D chaotic maps[J].Journal of Information Security and Applications，2019，46：23-41.

[21] KUMAR M，SATHISH G，ALPHONSE M，et al.A new RGB image encryption using generalized heat equation associated with generalized Vigenère-type table over symmetric group[J].Multimedia Tools and Applications，2019，78(19)：28025-28061.

[22] DUAN C F，ZHOU J，GONG L H，et al.New color image encryption scheme based on multi-parameter fractional discrete Tchebyshev moments and nonlinear fractal permutation method[J].Optics and Lasers in Engineering，2022，150：106881.

[23] WANG Q，ZHANG X Q，ZHAO X H.Color image encryption algorithm based on novel 2D hyper-chaotic system and DNA crossover and mutation[J].Nonlinear Dynamics，2023，111(24)：22679-22705.

An image encryption algorithm based on a fractional-order discrete noninvertible map

Liu Xiaojun，Wang Pu，Lu Chenhao

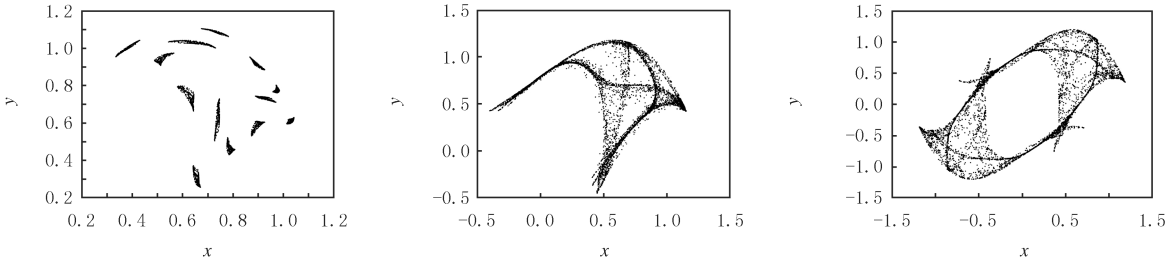
(School of Sciences，Xi'an University of Posts and Telecommunications，Xi'an 710121，China)

Abstract：Based on the chaotic characteristics of fractional-order discrete maps，a color image encryption algorithm based on the fraction-order cyclic shift is proposed. Firstly，the random initial values are generated for each layer by a random binary sequence associated with the original color image using a pseudo-randomizer. Secondly，a fractional-order discrete map is used to generate the chaotic sequences，circular shift position chaotic encryption and diffusion operations are performed on the re，green and blue components of a color image，respectively. Finally，the encrypted image is obtained by matrix transformation of the encryption matrix for each layer based on the pseudo-random binary sequence and chaotic sequence control. Simulation results show that correlation coefficients for an image by the proposed method are approximately 0，and the average values of information entropy，number of pixels change rate and unified average changing intensity are 7.997 8，99.609% and 33.442%，respectively. Therefore，the algorithm has a good reliability and an anti-attack capability. Meanwhile，the algorithm can enhance the security of images.

Keywords：fractional-order discrete map；image encryption；cyclic shift encryption；matrix transformation

[责任编校　杨浦　刘洋]

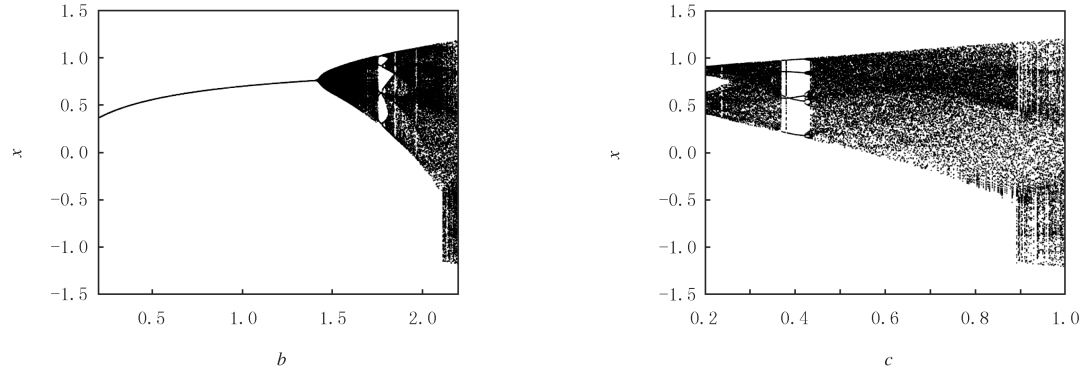
附　录



(a) v=0.84　　(b) v=0.95　　(c) v=0.98

图S1　系统(1)的混沌系统吸引子

Fig.S1　Chaotic attractors of map(1)

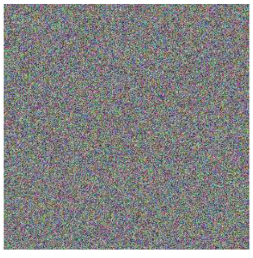


(a)参数b变化　　(b)参数c变化

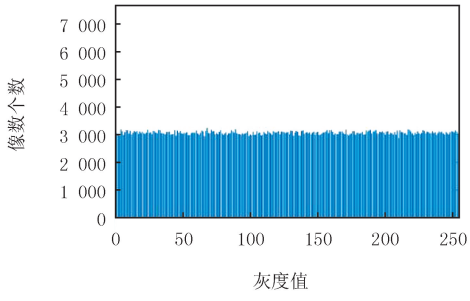
图S2　系统(1)的分岔图

Fig.S2　Bifurcation diagrams of map(1)

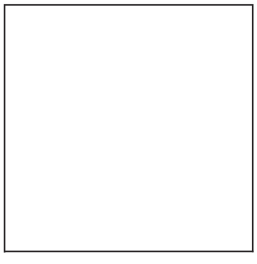
(a)全黑原始图像



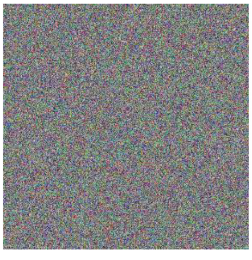
(b)全黑加密图像



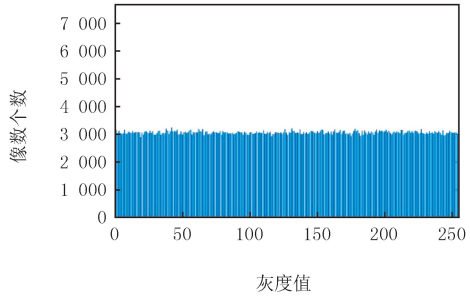
(c)全黑加密图像直方图



(d)全白原始图像



(e)全白加密图像



(f)全白加密图像直方图

图S3　全白全黑图像加密结果及直方图

Fig.S3　All-white and all-black image encryption results and histograms