参数扰动下的混沌的图像加密方案

朱淑芹 李俊青
(聊城大学计算机学院 聊城 252059)

摘 要 针对计算机有限数字精度的限制导致混沌序列将退化为周期序列的缺陷,提出一种参数扰动下混沌的图像加密方案。首先,对已有的一个离散混沌系统进行了改进,得到了一个新的混沌系统。其次,将已有混沌系统的状态变量作为参数扰动,来扰动新构造的混沌系统以生成参数扰动下的混沌系统。在加密方案中,利用密文反馈的方式来控制迭代次数,动态产生密钥流。实验结果和安全性分析表明,该算法具有对密钥敏感、密钥空间大、密文图像统计特性良好、密文对明文敏感、能抵抗选择明(密)文的攻击等优点。

关键词 Marotto 定理,混沌加密,参数扰动,密文反馈
中图法分类号 TP391 **文献标识码** A

Image Encryption Scheme Based on Chaos with Parameter Perturbation

ZHU Shu-qin LI Jun-qing
(School of Computer Science, Liaocheng University, Liaocheng 252059, China)

Abstract Due to the limitation of the numerical accuracy of the computer, the chaotic sequence will degenerate into the periodic sequence. An image encryption scheme based on chaotic system with parameter perturbation was proposed. Firstly, an existing chaotic system was improved to obtain a new chaotic system. Secondly, the new chaotic system was perturbed by the state variables of the existing chaotic systems, so that Chaotic system with parameter perturbation can be produced. In the encryption scheme, the number of iterations is controlled by the feedback of the cipher text and the key stream is generated dynamically. Experimental results and security analysis show that the algorithm is sensitive to the key and has a large key space, the encrypted image has good statistical properties and the encrypted image is very sensitive to the plain image, and the algorithm can resist the attack of choosing plain or cipher text.

Keywords Marotto theorem, Chaotic encryption, Parameter perturbation, Cipher text feedback

1 概述

近年来,人们对混沌与密码学之间的关系进行了深入研究,混沌系统具有其独有的特性,如:对初始条件与系统参数的极为敏感性、伪随机性、非周期性、非收敛性等[1]。正是因为这些特性,使得与传统加密算法相比,混沌系统用于图像加密时显示出强大的优越性[2-5]。从而基于混沌的数字图像加密逐渐成为一个研究热点[6-9]。但是由于计算机有限数字精度的限制,其混沌特性存在明显退化,生成的混沌序列将退化为周期序列,而且实际生成的序列的周期和密码学特征难以度量,致使实际结果与理论结果大相径庭,安全性降低。针对这一缺陷,人们提出了多种不同的方法来解决这一问题,比如提高运算精度、多个系统切换控制、多个混沌序列进行非线性运算、多个混沌系统的级联等方法[10-13]。众所周知,对参数的高度敏感性是混沌系统的一大特性,如果对混沌系统的参数施加一定的扰动使其在一定范围内变化,同时确保系统依然处于混沌状态,则系统将产生更加难以预测的混沌行为,如果进一步利用混沌序列来构造参数扰动项,即在混沌系统中引入另一混沌系统的状态变量作为参数扰动,则加密系统的安全性将大大提高。韩双霜等人[14]基于陈关荣与史玉明提出的修正版 Marotto 定理构造了一个三维离散混沌映射,本文对该三维离散混沌映射进行了改进,并利用修正的 Marotto 定理证明了改进系统是一个混沌系统,对改进的混沌系统的敏感性进行了定量分析,通过引进同步误差来比较两个混沌系统的敏感性,结果表明新系统比原系统具有更强的敏感性。本文用文献[14]中的混沌系统的状态变量作为参数扰动,来扰动新构造的混沌系统以生成参数扰动下的混沌系统,然后基于参数扰动下的混沌系统设计了一种新的混沌图像加密算法。

通过研究大量图像加密算法,笔者发现不论设计多么巧妙的算法,只要密钥流与明文图像无关,都可以通过选择明文(密文)攻击将算法破解[15-18]。另外,有些算法不能抵抗噪声、剪切及压缩的攻击[19];有些算法对明文的敏感度较低[20]。为了克服以上缺陷,本文提出一个新的加密算法。为了使算法抵抗噪声、剪切及压缩的攻击,首先对明文图像进行了置乱操作;其次,为了使算法抵御选择明文(密文)攻击,在混沌迭代过程中利用密文反馈的方式来控制迭代次数。具体来说就是对置乱的明文图像分块,每一分块与参数扰动下的混沌系

本文受国家自然科学基金面上项目(61573178),聊城大学自然科学基金(318011606)资助。
朱淑芹(1979-),女,硕士,讲师,主要研究方向为混沌理论、图像处理,E-mail:shuqinzhu2008@163.com;李俊青(1976-),男,博士,副教授,主要研究方向为优化调度理论、保密通信。

统生成的伪随机序列进行异或操作，进行下一块加密时，利用上一块密文反馈的方式来控制迭代次数。也就是说，加密下一块明文块所产生的密钥流与上一密文块有关。

2　三维离散混沌映射的构造

2.1　修正的 Marotto 定理及文献[14]构造的三维混沌映射

定理 1[21]　设 $Z\in R^n$ 为映射 $f:R^n\to R^n$ 的一个不动点，假设：

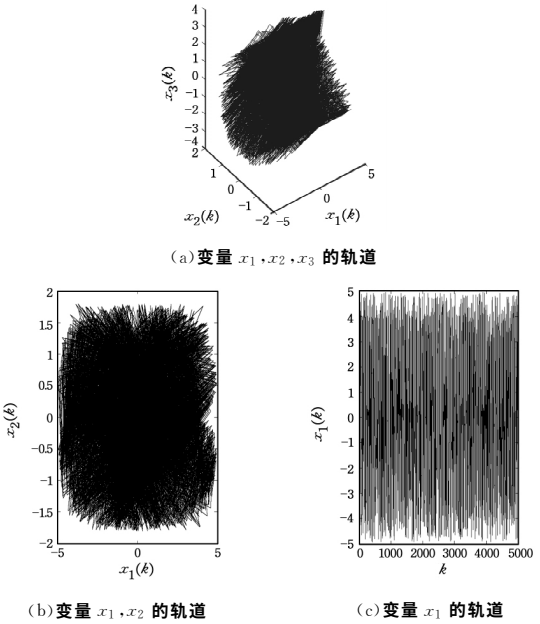
(1) f 在 Z 的某领域内连续可微且 $Df(Z)$ 的所有特征值的绝对值大于 1，从而存在一个正常数 r 和 R^n 的一个范数 $\|\cdot\|$，使得 f 在 $\|\cdot\|$ 之下，在 $\overline{B}_r(Z)$ 上扩张，其中 $\overline{B}_r(Z)$ 是空间 $(R^n,\|\cdot\|)$ 的以 Z 为中心的闭球；

(2) Z 是 f 的返回扩张不动点，即存在点 $X_0\in Br(Z)$ 及正整数 m，使得 $f^m(X_0)=Z$。其中 $Br(Z)$ 是空间 $(R^n,\|\cdot\|)$ 以 Z 为中心的开球，且 f 在 $X_0,X_1,\cdots,X_{m-1}$ 的某邻域内连续可微且满足 $\det Df(X_j)\neq 0(0\leqslant j\leqslant m-1)$，其中 $X_j=f(X_{j-1})$，$0\leqslant j\leqslant m-1$。则映射 f 在 Li－Yorke 意义下是混沌的。

基于定理 1，文献[14]中构造的三维离散混沌映射如式(1)所示：

$$\begin{cases}x_1(k+1)=\sin(x_1(k)).\sin(x_2(k))-a\sin(x_3(k))\\ x_2(k+1)=b\sin(x_1(k)).\cos(x_2(k))\\ x_3(k+1)=cx_2(k)\end{cases}\tag{1}$$

其中，参数 $a=4,b=1.8,c=2$。选择初始值 $x_1(0)=0.5,x_2(0)=0.2,x_3(0)=0.1$ 时，其相图如图 1 所示。



(a)变量 x_1,x_2,x_3 的轨道　(b)变量 x_1,x_2 的轨道　(c)变量 x_1 的轨道

图 1　三维映射的混沌解轨道

2.2　一种新的三维离散混沌系统的构造

在混沌映射(1)的基础上对第 3 个式子添加了一个非线性项 $\sin(x_3(k))$，第 2 个式子添加了一项 $-x_1(k)$，得到一个改进的三维离散混沌系统，如式(2)所示：

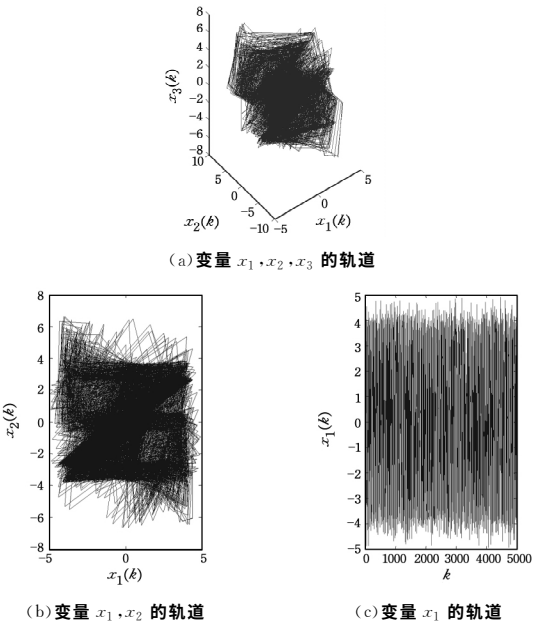
$$\begin{cases}x_1(k+1)=\sin(x_1(k)).\sin(x_2(k))-a\sin(x_3(k))\\ x_2(k+1)=b\sin(x_1(k)).\cos(x_2(k))-x_1(k)\\ x_3(k+1)=cx_2(k)+\sin(x_3(k))\end{cases}\tag{2}$$

当式中的参数分别为 $a=4,b=2,c=1$ 时，此系统产生的序列是混沌序列。

可以看出 $Z=(0,0,0)$ 为该映射的一个不动点，计算点 $Z=(0,0,0)$ 的雅可比矩阵的 3 个特征值分别为：$\lambda_1=-1.3146,\lambda_2=1.1573+1.3052i,\lambda_3=1.1573-1.3052i$。即所有特征值的绝对值都大于 1，满足定理 1 中的条件(1)。经计算存在点 $X_0=(-pi,0,pi)\neq Z$ 及正整数 $m=3$，使得 $f^3(X_0)=Z$。其中 $X_1=f(X_0)=(0,pi,0),X_2=f(X_1)=(0,0,pi)$，$\det Df(X_0)=-4,\det Df(X_1)=12,Df(X_2)=4$。

根据定理 1 可知若 f 分别在 X_0,X_1,X_2 的某邻域内连续可微并满足 $\det Df(X_j)\neq 0(0\leqslant j\leqslant m-1)$，即 $X_0\in Br(Z)$，则 Z 是 f 的返回扩张不动点。证明式(2)是混沌映射的详细过程可参考文献[12]。

对系统(2)进行 Matlab 仿真模拟，选择初始值 $X_0=(-1.8,0.7,0.6)$，其相图如图 2 所示。



(a)变量 x_1,x_2,x_3 的轨道　(b)变量 x_1,x_2 的轨道　(c)变量 x_1 的轨道

图 2　三维映射的混沌解轨道

2.3　改进系统与原系统的初值(参数)敏感性分析

众所周知，若混沌系统状态变量对参数(初值)的敏感度越高，则把它用于加密时密钥越敏感，其安全特性越高。本节的实验结果表明新构造的混沌系统(2)比原混沌系统(1)对参数(初值)的敏感度高。

设 n 维离散系统为式(3)：

$$X(k+1)=F(X(k))\tag{3}$$

其中，$X(k)=(x_1(k),x_2(k),\cdots,x_n(k)),F(X(k))=(f_1(X(k)),f_2(X(k)),f_3(X(k)),\cdots,f_n(X(k)))$。

设参数向量 $\alpha\in R^m$ 使系统(3)处于混沌状态，则 α 和初值 $X(0)$ 组成向量 $D=[\alpha,X(0)]$。

系统(3)的同构系统为式(4)：

$$Y(k+1)=F(Y(k))\tag{4}$$

设参数向量 $\beta\in R^m$ 使系统(4)处于混沌状态，则 β 和初值 $Y(0)$ 组成向量 $T=[\beta,Y(0)]$。

经过 k 步迭代后，系统(3)与系统(4)的同步误差为式(5)：

$$e(k)=X(k)-Y(k)\tag{5}$$

令系统(3)与系统(4)的 D,T 存在微小偏差 $\delta=\|D-T\|=10^{-t}$，若 $e(k)$ 经 k 步迭代达到稳态后的范数满足 $\|e(k)\|=\|X(k)-Y(k)\|>L$，其中 $L(L>0)$ 是提前设定的轨道分离的下界，这时称 k 为系统(3)与系统(4)的参数或

初值偏差为 l 级时的分离迭代步数。显然 k 越小分离速度越快，系统变量对参数或初值越敏感。

对于系统(1)，$D=(4,1.8,2,0.5,0.2,0.1)$时，构造其同构系统的 $T=(4+10^{-l},1.8,2,0.5,0.2,0.1)$，即初值相同而参数存在偏差 $\delta=10^{-l}$，取 $L=0.9$，则 l 与迭代步数 k 的关系如图 3 中的上方曲线所示。同理对于系统(2)，$D=(4,2,1,-1.8,0.7,0.6)$时构造其同构系统的 $T=(4+10^{-l},2,1,-1.8,0.7,0.6)$，即初值相同而参数存在偏差 $\delta=10^{-l}$，取 $L=0.9$，则 l 与迭代步数 k 的关系如图 3 中的下方曲线所示。

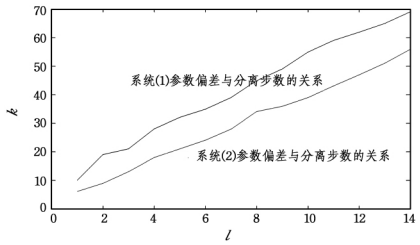


图 3 参数敏感曲线图

由此可见系统(2)比系统(1)对参数 a 更敏感，实验也可证明系统(2)比系统(1)对参数 b,c 更敏感。

对于系统(1)，$D=(4,1.8,2,0.5+10^{-l},0.2,0.1)$时构造其同构系统的 $T=(4,1.8,2,0.5+10^{-l},0.2,0.1)$，即参数相同而初值存在偏差 $\delta=10^{-l}$，取 $L=0.9$，则 l 与迭代步数 k 的关系如图 4 中的上方曲线所示。同理对于系统(2)，$D=(4,2,1,-1.8,0.7,0.6)$时构造其同构系统的 $D=(4,2,1,-1.8+10^{-l},0.7,0.6)$，即参数相同而初值存在偏差，取 $L=0.9$，则 l 与迭代步数 k 的关系如图 4 中的下方曲线所示。

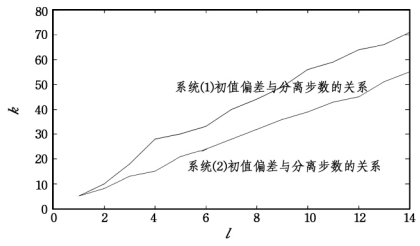


图 4 初值敏感曲线图

由此可见系统(2)比系统(1)对初值 x_1 更敏感，实验也可以证明系统(2)比系统(1)对初值 x_2,x_3 更敏感。

3 变参数的混沌系统的加密方案

3.1 变参数混沌系统的生成

由于系统(2)比系统(1)对参数具有更高的敏感性，故用系统(1)来扰动系统(2)从而产生参数扰动下的混沌系统，如式(6)所示：

$$\begin{cases} y_1(k+1)=\sin(y_1(k)).\sin(y_2(k))-(a+\sigma x_1(k))\\ \qquad\qquad \sin(y_3(k))\\ y_2(k+1)=(b+\sigma x_2(k))\sin(y_1(k)).\cos(y_2(k))-y_1(k)\\ y_3(k+1)=(c+\sigma x_3(k))y_2(k)+\sin(y_3(k)) \end{cases} \tag{6}$$

其中，$y_i(k)(i=1,2,3)$为系统的状态变量，$a=4,b=2,c=1$ 为系统的参数，$x_i(k)(i=1,2,3)$为参数扰动，由系统(1)提供，σ 为扰动强度。由 Matlab 仿真可知系统(1)产生的序列中数值的范围为$(-5,5)$，计算系统(6)在系统(1)的扰动下的最大李雅谱诺夫指数，当 $-0.09\leqslant\sigma\leqslant0.09$ 时，系统的最大李雅谱诺夫指数为正，即系统保持混沌状态。

3.2 加密算法

3.2.1 置乱操作

为了使算法抵抗噪声、剪切及压缩的攻击，必须进行置乱操作。同时，为使密文图像对明文敏感，置乱时，使用初值与明文图像像素总值有关的 logstic 映射产生的混沌序列进行置乱。具体如下。

(1)设图像的大小为 $m\times n$，将像素矩阵 A 按从左到右，从上到下的顺序转化为长度为 $m*n$ 的一维数组 Pt，即变换公式为 $pt((i-1)n+j)=A(i,j)$，式中，$i=1,2,3,\cdots,m,j=1,2,3,\cdots,n$。

(2)Logistic 映射定义为 $t(k+1)=r*t(k)*(1-t(k))$，其中，$0\leqslant r\leqslant4$ 为分支参数；$t(k)\in(0,1)$。当 $3.5699456\cdots<r\leqslant4$ 时，系统处于混沌状态。

取 $r=3.893456$，$t(1)=(\mathrm{mod}(\mathrm{sum}(\mathrm{sum}(A)),256)/256+t(0))\ \mathrm{mod}\ 1$($t(0)$可以作为一个密钥)对 Logistic 映射进行 $m*n$ 次迭代，得到一个混沌序列 $t=\{t(i)\mid i=1,2,3,\cdots,m\times n\}$。

(3)对混沌序列 t 按升序排序得到新的有序序列 $tx=\{tx(i)\mid i=1,2,3,\cdots,m\times n\}$，由 tx 在 t 中的位置索引为序列值生成服从$[1,m\times n]$的混沌随机序列 $sx=\{sx_i\mid i=1,2,3,\cdots,m\times n\}$，按该序列值一一将 Pt 数组变换到新数组 P，变换公式为 $P(i)=Pt(sx_i)$。P 即为置乱后的图像。

3.2.2 混淆操作

在混淆操作中，以 8 个像素为一组对置乱后的一维向量 P 进行分块，对每一块加密时，把 8 个像素转化为长度为 64 的 0、1 字符串序列，然后对字符串序列进行循环移位操作，再用参数扰动下的混沌系统生成的 0、1 伪随机序列与循环移位操作后的明文 0、1 字符串序列进行异或操作，最后再把 64 位长的 0、1 字符串序列以 8 个为一组，每一组再转化为十进制，得到对应的密文块。

利用密文反馈的方式来控制混沌系统的迭代次数，进行下一块加密，直至所有块加密结束。具体步骤如下：

(1)把 P 中的每个数值转化为 8 位二进制数，每 8 个数值的二进制数并在一起构成一个 64bit 的明文块 $p_j(j=1,2,3,\cdots,m*n/8$，若 $m*n$ 不能被 8 整除，则对向量 P 进行补零操作)。

(2)对于系统(6)，首先迭代 $N+70$ 次，N 为一个正整数，可以作为一个密钥，取后 70 次迭代的结果，生成 3 个序列 $y_1=\{y_1(1),y_1(2),\cdots,y_1(70)\}$，$y_2=\{y_2(1),y_2(2),\cdots,y_2(70)\}$，$y_3=\{y_3(1),y_3(2),\cdots,y_3(70)\}$。利用序列 y_1,y_2,y_3 进行变换，得到序列 Z，$Z=k_1y_1+k_2y_2y_3=(z(1),z(2),\cdots,z(70))$，$k_1=sqrt(3)$，$k_2=sqrt(5)$，对于序列 Z 的每个元素的小数点后的第 8 位数字，若该位数字小于 5，则取 0，否则取 1，这样得到一个长度为 70 的 0、1 序列 T，T 的前 64 位构成序列 $T1$，T 的后 8 位构成序列 $T2$。

(3)d 为 $T2$ 对应的十进制数，对明文块 p_j 进行循环左移 d 位的操作，得到新的明文块 p_j'。

(4)用序列 $T1$ 与新的明文块 p_j'进行异或操作，得到密文块 C_j，即 $C_j=T1\oplus p_j'$，然后将 C_j 每 8 位为一组，分成 8 组，再把每一组转化成对应的十进制数 $c_j^1,c_j^2,c_j^3,c_j^4,c_j^5,c_j^6,c_j^7,c_j^8$。

(5)如果所有明文块都被加密，则加密结束。否则继续迭

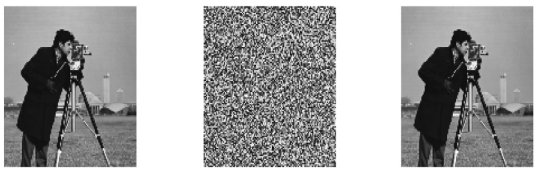
代系统(6)$H=T1+\mathrm{mod}((c_j^1+c_j^2+c_j^3+c_j^4+c_j^5+c_j^6+c_j^7+c_j^8),64)$次，然后重复步骤(2)－(5)的操作直到所有明文块加密完。

(6)最后所有的 $c_j^1,c_j^2,c_j^3,c_j^4,c_j^5,c_j^6,c_j^7,c_j^8(j=1,2,3,\cdots,m*n/8)$组成了密文 C。

解密过程是上述过程的逆过程，本文不再赘述。

4　仿真实验

在本文算法的仿真过程中，选择 256×256 的“cameraman”灰度图像进行实验，加密系统的初始密钥集为 $keys=\{x_1(0),x_2(0),x_3(0),y_1(0),y_2(0),y_3(0),\sigma,N,t(0),$明文图像的总像素值$\}=\{0.5,0.2,0.1,-1.8,0.7,0.6,0.0897,234,0.8765,7780728\}$。其中图 5(a)为原明文图像，图 5(b)为密文图像，图 5(c)为解密后复出的明文图像。由图 5(b)可知，加密图像与明文图像无任何关联；由图 5(c)可知，恢复出的明文图像与原明文图像在视觉上完全相同。



(a)原明文图像　(b)密文图像　(c)解密后复出的明文图像

图 5

5　安全性分析

5.1　密钥空间和密钥敏感性分析

密钥空间的大小是加密时可用的不同密钥数。密钥空间越大，算法抵抗蛮力攻击的性能越好。本算法的密钥集为 $keys=\{x_1(0),x_2(0),x_3(0),y_1(0),y_2(0),y_3(0),\sigma,N,t(0),$明文图像的总像素值$\}$。首先对密钥的敏感性进行分析，得到相应密钥空间大小。为了计算某密钥的敏感性，令该密钥的大小改变 h，其他参数保持不变。如计算密钥 a 的敏感性时，用密钥 a 加密明文得到密文图像 $C1$，用密钥 $a+h$(其他密钥不变)加密得到密文图像 $C2$，用密钥 $a-h$ 加密得到 $C3$，利用式(7)[22]来计算 $C1$、$C2$ 以及这两个密文图像的关联系数，关联系数越小，说明算法对密钥越敏感。

$$C_r=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(C1(i,j)-\overline{C}1)(C2(i,j)-\overline{C}2)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}(C1(i,j)-\overline{C}1)^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}(C2(i,j)-\overline{C}2)^2}} \tag{7}$$

其中，$C1(i,j)$是密文图像中点(i,j)处的像素值，$\overline{C}_1$ 是密文图像 $C1$ 的像素平均值，$C2(i,j)$是密文图像中点(i,j)处的像素值，$\overline{C}_2$是密文图像 $C2$ 的像素平均值。同理，利用式(7)可以计算出 $C1$、$C3$ 和 $C2$、$C3$ 的关联系数。计算密钥 $x_1(0),x_2(0),x_3(0),y_1(0),y_2(0),y_3(0),t(0)$的改变量 h 均为 10^{-15}。σ 的改变量 h 为 10^{-17}。$C1$，$C2$，$C3$ 3 幅图像中任意两幅的相关系数表如表 1 所列。由此可以看出虽然加密密钥有微小的变化，得到的密文图像大不相同，相关性很小，因此密钥空间可达 $10^{15}\times10^{15}\times10^{15}\times10^{15}\times10^{15}\times10^{15}\times10^{17}=10^{123}$，这么大的密钥空间是可以抵抗蛮力攻击的。若考虑 N 的取值，密钥空间将更大。

表 1　各参数变化时密文图像的相关系数表

密钥 \ 相关系数	$C1$ 与 $C2$ 的相关系数	$C1$ 与 $C3$ 的相关系数	$C2$ 与 $C3$ 的相关系数
$x_1(0)$	0.0028	0.0023	0.0013
$x_2(0)$	−0.0041	−0.0047	−0.0026
$x_3(0)$	−0.0022	−0.0032	0.0012
$y_1(0)$	0.000324	0.0004532	−0.0002572
$y_2(0)$	−0.00669	−0.0006512	−0.0004167
$y_3(0)$	−0.0017	−0.0014	−0.0023
$t(0)$	−0.00127	0.000125	0.0002786
σ	0.0025	0.0054	0.0036

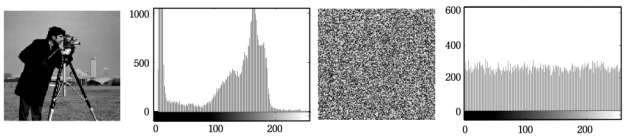
5.2　明文敏感性测试

对明文图像修改敏感是衡量加密算法好坏的一个重要指标，如果修改明文图像的一个像素值会引起密文图像的巨大变化，则认为该算法能抵抗差分攻击。本文算法中涉及的置乱、Logistic 映射的初值与明文图像的像素总灰度值有关，混沌迭代次数由密文控制等，这些因素都会使算法对明文图像敏感。用数字图像像素变化率(NPCR)和归一化平均变化强度(UACI)来衡量数字图像加密算法对明文敏感的程度。NPCR 和 UACI 的计算公式[23]分别为 $NPCR=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D_{ij}}{M\times N}\times100\%$ 和 $UACI=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(\frac{x(i,j)-x'(i,j)}{255}\right)}{M\times N}\times100\%$。其中，$D_{ij}=\begin{cases}1, & x(i,j)\neq x'(i,j)\\ 0, & x(i,j)=x'(i,j)\end{cases}$，$M\times N$ 为图像的大小，x 为原密文图像，x'为明文改变后对应的密文图像。由文献[23]知，对于 8 位灰度图像($m=8$)，NPCR 与 UACI 的理想期望值分别为：$NPCR\ E=99.6094\%$，$UACI\ E=33.4635\%$。本算法中随机选取“cameraman”图像中的 50 个像素点，改变它们的像素值，结果计算的 NPCR 值最大为 99.743%，最小为 99.467%，平均值为 99.6489%。UACI 值最大为 33.675%，最小为33.367%，平均值为 33.456%，非常接近理想值。可见，原图像中一个像素灰度值的变化会导致加密图像中几乎所有像素灰度值发生变化。从而验证了该算法具有很好的抗差分攻击的性能。

5.3　统计特性分析

5.3.1　统计直方图

直方图是数字图像的一个基本属性，密文图像的直方图呈现均匀分布或高斯分布均说明加密效果良好。为了说明算法的有效性，本文加密了“rice”，“cameraman”，“pout”，“pepper” 4 幅经典图像，其密文图像的直方图都呈现等概率分布。因篇幅所限，只给出“cameraman”加密后的图像的直方图，如图 6(d)所示。



(a)“cameraman”的明文图像　(b)明文图像的直方图　(c)密文图像　(d)密文图像的直方图

图 6

在直方图中，横坐标代表灰度图像的 256 个灰度级，纵坐标代表图像所有像素取每个灰度级的频数。从统计直方图可以看出，加密图像的直方图中各像素值的概率分布都接近等

概率分布，因此加密后的图像是一幅随机图像。

5.3.2 密文图像信息熵分析

通常图像越混乱，图像提供的有用信息就越少，而信息熵就是度量图像混乱程度的一个量，信息熵越大，图像就越混乱。信息熵的计算公式为 $H=-\sum_{i=1}^{n} p_i \log 2(p_i)$，其中，$p_i$ 为第 i 阶灰度值出现的概率。对于灰度图像来说有 $256=2^8$ 个灰度级，当密文的概率分布为等概率分布时，具有的最大熵为 8bit。本文加密的“rice”，“cameraman”，“pout”，“pepper” 4 幅数字图像的信息熵见表 2 第 2 列，可以看出 4 幅图像的密文图像的信息熵都非常接近 8。这表明加密后图像的混乱程度很高，由密文图像得不到明文图像的任何信息。

表 2 加密图像的信息熵和明文图像与密文图像的相关系数

图像	加密后的信息熵	明文图像与密文图像的相关系数
rice	7.9882	−0.0042
cameraman	7.9872	0.0107
pout	7.9875	−0.0043
pepper	7.9885	0.0070

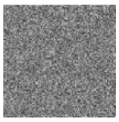
5.3.3 原图像和密文图像的关联系数分析

关联系数是度量原明文图像和密文图像对应像素点的相似度的一个量，而加密的目标是最小化该相似度，相似度越小，算法越安全。计算关联系数的公式如式(7)所示，本实验中计算“rice”，“cameraman”，“pout”，“pepper”4 幅数字图像的关联系数见表 2 第 3 列，可以看出密文图像的关联系数比都较小，这表明加密效果良好，密文图像和明文图像没有任何关联。

5.4 抗攻击测试

1)抗噪声污染攻击测试

在加密后的图像中人为地加入各种噪声来测试加密图像的抗击噪声的能力。从图 7 可以看出，加密后的图像经过椒盐噪声污染后，解密后的图像微有噪声，但不影响图像的整体效果。从图 8 和图 9 可以看出该算法抗击泊松噪声的能力稍差，而抗击高斯噪声的能力最差。这是因为虽然椒盐噪声的强度最大，但是噪声分布最稀松；泊松噪声和高斯噪声的分布比较密，但是高斯噪声的强度比泊松噪声的强度大。

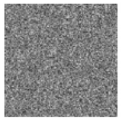


(a)加密后的图像经椒盐噪声污染后的图像

(b)解密图像

(c)对(b)进行中值滤波后的图像

图 7

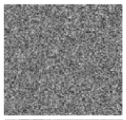


(a)加密后的图像经泊松噪声污染后的图像

(b)解密图像

(c)对(b)进行中值滤波后的图像

图 8



(a)加密后的图像经强度为 0.002 高斯噪声污染后的图像

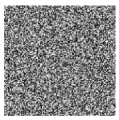
(b)解密图像

(c)对(b)进行中值滤波后的图像

图 9

2)抗压缩攻击测试

对密文图像进行压缩，再对压缩后的密文图像解密，以进行抗压缩攻击测试。从图 10 和图 11 可以看出压缩比越大，解密后的图像噪声越严重，图像越模糊，但仍能看出图像的大体轮廓。

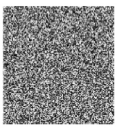


(a)加密后的图像压缩为原图像 60%后的图像

(b)解密图像

(c)对(b)进行中值滤波后的图像

图 10



(a)加密后的图像压缩为原图像 80%后的图像

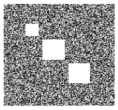
(b)解密图像

(c)对(b)进行中值滤波后的图像

图 11

3)抗裁剪测试

图 12(a)和图 12(b)为加密后的图像经中间部分裁剪后的图像及其解密图像。从图 12 可以看出加密后的图像经过不同程度的裁剪后，解密后的图像微有噪声，但不影响图像的整体效果，这是因为本文的混沌解密算法对图像各点置乱均匀，无论剪切任何部位的一定面积的加密后的图像，其解密后的图像都能辨清其轮廓。



(a)加密后的图像经部分裁剪后的图像

(b)解密图像

(c)对(b)进行中值滤波后的图像

图 12

5.5 抵抗选择明(密)文攻击分析

加密系统的安全性不依赖于加密算法本身，而是依赖于密钥，当我们分析一个加密算法的安全性时，假设密码破译者能准确地知道一个加密方案中除了密钥之外的任何信息。也就是说破译者知道这个加密系统的设计和运作。常用的密码分析技术有下 4 种[24]。

1)唯密文攻击(ciphertext-only attack)

攻击者只拥有密文，在这种情况下破解出全部或部分明文。

2)已知明文攻击(known-plaintext attack)

攻击者同时拥有一部分明文和相对应的密文，破解出全部或部分明文和密钥。

3)选择明文攻击(chosen-plaintext attack)

攻击者暂时获得加密机的使用权，因此他能加密任意的明文，并获得相对应的密文，以此破译出全部或部分明文和密钥。

4)选择密文攻击(Chosen-plaintext Attack)

攻击者暂时获得解密机的使用权，因此他能解密任意的密文，从而获得相对应的明文，以此破译出密钥。

显然，选择明文攻击是最强的攻击，如果一个密码系统能够抵抗这种攻击，则它一定能抵抗其他攻击。

(下转第 384 页)

tions [DB/OL]. http://www.nist.gov.

[3] SOTO J. Randomness Testing of the AES Candidate Algorithms [OLL]. http://www.nist.gov.

[4] HUANG G B, ZHU Q Y, SIEW C K. Extreme Learning Machine: A New Learning Scheme of Feedforward Neural Networks[C]// Proceedings of International Joint Conference on Neural Networks (IJCNN2004). Budapest, Hungary, July, 2004: 25-29.

[5] HUANG G B, ZHU Q Y, SIEW C K. Extreme learning machine: Theory and applications[J]. Neurocomputing, 2006, 70(1-3): 489-501.

[6] HUANG G B, ZHOU H, DING X, et al. Extreme learning machine for regression and multiclass classification [J]. IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, 2012, 42(2): 513-529.

[7] MICHE Y, SORJAMANN A, BAS P, et al. OP-ELM: optimally pruned extreme learning machine [J]. IEEE Transactions on Neural Networks, 2010, 21(1): 158-162.

[8] KIM M S, YU H J, KWAK K C, et al. Robust text-independent speaker identification using hybrid PCA & LDA[C]// MICAI'06. Mexico, Nov. 2006: 1067-1074.

[9] LIU C. Gabor-based kernel PCA with fractional power polynomial models for face recognition[J]. IEEE Trans, Pattern Analysis and Machine Intelligence, 2004, 26(5): 573-581.

(上接第 360 页)

本文的加密算法分为两步：置乱和混淆。在置乱阶段混沌映射的初值与明文图像的像素值的总和有关；在混淆阶段，对下一块加密时，混沌映射需迭代 $H+70$ 次后，取后 70 次的混沌序列作为所需的密钥流，而 H 是与上一块的密文相关的。基于以上两点，加密不同的图像，加密系统所产生的置乱阶段的密钥流和混淆阶段的密钥流都不同，所以加密一些特殊的图像并不能得到目标密文的密钥流，因而本文提出的加密算法能抵抗选择明(密)文攻击。

结束语 本文提出了一种参数扰动下混沌的图像加密方案，与已有的加密算法相比，该算法具有以下特点：1)所用混沌系统是参数扰动下的混沌系统，且扰动参数是另一混沌系统所产生的随机序列，克服了由于计算机有限数字精度的限制，混沌序列将退化为周期序列的缺陷。2)已有的加密算法都是先用混沌系统生成密钥流，然后用密钥流与明文图像做混淆或扩散操作，而本文的算法是根据密文动态产生密钥流，这样加密不同的明文图像所用密钥流不同，达到“一次一密”的效果。实验模拟和安全性分析表明，该算法具有对密钥敏感，密钥空间大，密文图像统计特性良好，密文对明文敏感，抵抗选择明(密)文的攻击及抗噪声、抗压缩、抗剪切攻击的优点。

参 考 文 献

[1] AHMAD J, HWANG S O. A Secure Image Encryption Scheme Based on Chaotic Maps and Affine Transformation[J]. Multimedia Tools Applications, 2015, 75(21): 1-26.

[2] BAPTISTA M. Cryptography with Chaos[J]. Physics Letters A, 1998, 240(1): 50-54.

[3] CHEN G, MAO Y, CHUI C K. A symmetric image encryption scheme based on 3d chaotic cat maps[J]. Chaos Solitons Fractals, 2004, 21(3): 749-761.

[4] LI S, ZHENG X. Cryptanalysis of a Chaotic Image Encryption Method[C]// IEEE International Symposium on Circuits and Systems, 2002(ISCAS'2002), EEE, 2002: 708-711.

[5] WANG Y, WONG K W, LIAO X, et al. A new chaos-based fast image encryption algorithm[J]. Applied Soft Computing, 2011, 11(1): 514-522.

[6] 刘泉，李佩玥，章明朝，等. 基于可 Markov 分割混沌系统的图像加密算法[J]. 电子与信息学报，2014，36(6)：1271-1277.

[7] 置与比特双重置乱的图像混沌加密算法[J]. 通信学报，2014，35(3)：216-223.

[8] 张顺，高铁杠. 基于类 DNA 编码分组与替换的加密方案[J]. 电子与信息学报，2015，37(1)：150-157.

[9] 文昌辞，王沁，黄付敏，等. 基于仿射和复合混沌的图像自适应加密算法[J]. 通信学报，2012，33(11)：119-127.

[10] 李树钧. 数字化混沌密码的分析与设计[D]. 西安：西安交通大学，2003.

[11] ALVAREZ G, LI S J. Some Basic Cryptographic Requirements for Chaos-based Cryptosystems[J]. International Journal of Bifurcation and Chaos, 2006, 16(8): 2129-2151.

[12] KOCAREV L. Chaos-based Cryptography: a Brief Overview[J]. IEEE Circuits and Systems Magazine, 2001, 1(3): 6-21.

[13] 罗启彬，张健. 一种新的混沌伪随机序列生成方式[J]. 电子与信息学报，2006，28(7)：1262-1265.

[14] 韩双霜，闵乐泉，韩丹丹. 一种基于三维离散混沌映射的伪随机数生成器[J]. 华中科技大学学报(自然科学版)，2013，41(8)：16-19.

[15] WANG X, LIU L T. Cryptanalysis of a Parallel Sub-Image Encryption Method with High-Dimensional Chaos[J]. Nonlinear Dynamics, 2013, 73(73): 795-800.

[16] LI C Q, ZHANG L Y, OU R, et al. Breaking a Novel Colour Image Encryption Algorithm Based on Chaos[J]. Nonlinear Dynamics, 2012, 70(4): 2383-2388.

[17] ZHU C, LIAO C L, DENG X. Breaking and Improving an Image Encryption Scheme Based on Total Shuffling Scheme[J]. Nonlinear Dynamics, 2013, 71(1/2): 25-34.

[18] 朱从旭，卢庆. 对结合超混沌序列和移位运算图像密码的攻击[J]. 山东大学学报(理学版)，2016，51(6)：67-71.

[19] ZHU C. A Novel Image Encryption Scheme Based on Improved Hyperchaotic Sequences[J]. Optics Communications, 2012, 285(1): 29-37.

[20] 廖琪男，卢守东，孙宪波. 结合超混沌序列和移位密码的数字图像加密算法[J]. 小型微型计算机系统，2015，36(2)：332-337.

[21] SHI Y M, CHENG G R. Discrete Chaos in Banach Spaces[J]. Science in China Series A: Mathematics, 2005, 48(2): 222-238.

[22] LIAN S. Efficient Image or Video Encryption Based on Spatiotemporal Chaos System[J]. Chaos, Solitons & Fractals, 2009, 40(5): 2509-2519.

[23] BENIA S, AKHSHANI A, MAHMODI H, et al. A Novel Algorithm for Image Encryption Based on Mixture of Chaotic Maps [J]. Chaos, Solitons & Fractals, 2008, 35(2): 408-419.

[24] WANG X Y, TENG L, QIN X. A novel colour image encryption algorithm based on chaos[J]. Signal Processing, 2012, 92(4): 1101-1108.