一种基于广义混沌同步系统的图像加密方案

柴宏玉 臧鸿雁
(北京科技大学数理学院 北京 100083)

摘 要 传统图像加密技术和低维混沌加密技术都有各自的局限性,而高维混沌映射比低维映射具有更复杂的动力学行为以及更好的随机性。在离散混沌广义同步定理的基础上构造了一种四维离散广义混沌同步系统,并设计了一种图像加密方案。对加密图像进行了安全性测试,如分布直方图、相邻像素相关系数、密文信息熵、密钥敏感性、密钥空间和雪崩效应等。理论分析和数值实验表明,该加密方案的密钥空间达到 10^{288},具有较强的抗攻击性能;对混沌系统参数及初始条件极其敏感,符合保密通信的要求。

关键词 保密通信,图像加密,广义混沌同步

中图法分类号 TP309.7 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.8.021

Image Encryption Scheme Based on Generalized Chaotic Synchronization Systems

CHAI Hong-yu ZANG Hong-yan
(School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 100083, China)

Abstract Many people apply the low-dimension chaotic map to encryption, however, the high-dimension map is more complex and has more parameters. Firstly, a 4-dimensional generalized chaotic synchronization (GCS) system was constructed based on generalized chaotic synchronization theorem. Combining this system, we designed a digital image encryption scheme, which can successfully encrypt and decrypt color images without any distortion. Secondly, performance test and security analysis were performed by using key space analysis and the pixels distribution character, correlation coefficients, the key sensitivity test, information entropy and avalanche effect. The results of analysis and simulation show that the key space of the image encryption scheme is more than 10^{288} and it has strongly anti-attacking performance. Additionally, the scheme is extremely sensitive to the system's parameters and initial conditions. Results suggest that the image scheme is effective in network communication.

Keywords Secure communication, Image encryption, Generalized chaotic synchronization

1 引言

很多图像加密使用如帐篷映射、Henon 映射、Logistic 映射等低维的离散混沌映射[9-11],少数基于 3 维混沌系统[12]。有研究表明,对于基于低维的混沌系统的序列,其系统参数和初始条件相对较少,密钥量也相对较少,混沌攻击者们有效利用此特点,提出了很多具有良好攻击效果的方法[13]。相较于低维混沌系统,高维混沌系统具有 4 个以上的状态变量及更多的系统参数,大大地增加了密钥空间。一般破译低维混沌加密的方法很难破译高维混沌加密信息,因此高维的混沌系统尤其是超混沌受到越来越多人的关注。文献[14]提出了一种改进的超混沌图像加密算法,通过理论分析了此算法不仅可以抵御选择明文攻击和选择密文攻击,还具有较好的统计特性及差分特性。文献[15]提出了一种基于超混沌系统优化序列并结合密文交错扩散的并行图像加密策略,通过对密钥空间、相关系数等进行测试,证明了方案的安全性。

本文基于离散系统广义同步定理,构造了一个四维广义同步系统。广义同步系统可使密钥量增加,因此本文提出了基于四维混沌映射的图像加密方案。由于密钥量随四维映射参数和系统变量的增大而增加,可高达 10^{288},因此其能有效地抵抗穷举攻击。对像素分布特性、相邻像素相关系数、密文信息熵、密钥敏感性、密钥空间和雪崩效应等指标进行了安全性测试,实验结果表明,该加密方案具有较高的安全性。

2 离散广义同步系统定义和定理

定义 1[4] 考虑两个离散混沌系统:

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

$$Y(k+1)=G(X(k),Y(k)) \tag{2}$$

其中,

$$X(k)=(x_1(k),\cdots,x_n(k))^{\mathrm{T}} \tag{3}$$

$$Y(k)=(y_1(k),\cdots,y_m(k))^{\mathrm{T}},m\leqslant n \tag{4}$$

$$F(X(k))=(f_1(X(k)),\cdots,f_n(X(k)))^{\mathrm{T}} \tag{5}$$

到稿日期:2015-07-21 返修日期:2015-09-29 本文受国家自然科学基金(61170037)资助。

柴宏玉(1990-),女,硕士生,主要研究方向为混沌密码学,E-mail:yuhongchaiyjm@126.com;臧鸿雁(1973-),女,博士,副教授,主要研究方向为非线性系统同步理论、混沌密码学。

$$G(Y(k),X(k))=(g_1(Y(k),X(k)),g_2(Y(k),X(k)),\cdots,g_m(Y(k),X(k)))^{\mathrm{T}} \tag{6}$$

系统(1)称为驱动系统，系统(2)称为响应系统。若存在可逆映射 $H:R^m\to R^m$ 和开集 $B=B_X\times B_Y\subset R^n\times R^m$，使得初始条件满足 $(X(0),Y(0))\in B$ 时，系统(1)和(2)的解满足：

$$\lim_{k\to\infty}\|H(X)-Y(X)\|=0$$

则称响应系统(2)与驱动系统(1)关于变换 $H(X(k))$ 在 B 上广义混沌同步。

引理 1[5] 设按式(3)－式(6)定义 $X(k)$，$Y(k)$，$F(X(k))$ 和 $G(Y(k),X(k))$，$H:R^m\to R^m$ 是可逆变换。假设系统(1)和(2)关于 H 是广义混沌同步，那么系统(2)的 $G(X(k),Y(k))$ 可写成下述形式：

$$G(Y(k),X(k))=H(F_m(X(k)))-q(X_m(k),Y(k))$$

其中，$F_m(X(k))=(f_1(X(k)),\cdots,f_m(X(k)))^{\mathrm{T}}$ 且函数 $q(X_m(k),Y(k))=(q_1(X_m(k),Y(k)),\cdots,q_m(X_m(k),Y(k)))^{\mathrm{T}}$。则误差方程

$$e(k+1)=H(X_m(k+1))-Y(k+1) \tag{7}$$

是渐进稳定的。

3 离散广义同步系统

广义混沌同步使密钥量增加，因此本文利用文献[17]中的四维混沌系统和广义混沌同步定理构造一个新的离散广义混沌同步系统。设驱动系统数学表达式可描述为如下形式[17]：

$$\begin{cases}x_1(k+1)=a_1x_1(k)-a_2(a_3-a_4x_4(k))x_2(k)-a_5x_3(k)\\ x_2(k+1)=b_1(b_2-x_4(k))x_1(k)-b_3x_2(k)-b_4x_3(k)\\ x_3(k+1)=c_1x_1(k)-c_2x_2(k)-c_3x_3(k)\\ x_4(k+1)=d_1x_1(k)x_2(k)+d_2x_4(k)\end{cases} \tag{8}$$

其中参数取值如下：

$$a_1=0.115;a_2=1.195;a_3=0.5;a_4=0.21;a_5=0.15;$$
$$b_1=0.359;b_2=5.995;b_3=0.285;b_4=0.4;c_1=0.25;$$
$$c_2=0.13;c_3=0.2;d_1=0.12;d_2=0.3 \tag{9}$$

初始条件为 $x_1(1)=0.387$，$x_2(1)=0.77$，$x_3(1)=0.771$，$x_4(1)=0.395$ 时产生混沌轨迹。

根据引理 1 构造可逆非线性变换 $H(X(k))$，其形式可记为 $H(X(k))=(y_1(k),y_2(k),y_3(k),y_4(k))$，具体如下：

$$\begin{cases}y_1(k)=\ln\frac{1}{2}(-x_1(k)+7x_3(k)-9x_4(k)+\sqrt{4+(x_1(k)-7x_3(k)+9x_4(k))^2})\\ y_2(k)=\ln\frac{1}{2}(4x_1(k)+2x_2(k)-24x_3(k)+30x_4(k)+\sqrt{4+(4x_1(k)+2x_2(k)-24x_3(k)+30x_4(k))^2})\\ y_3(k)=\ln\frac{1}{2}(-5x_1(k)-4x_2(k)+33x_3(k)-41x_4(k)+\sqrt{4+(5x_1(k)+4x_2(k)-33x_3(k)+41x_4(k))^2})\\ y_4(k)=\ln\frac{1}{2}(2x_1(k)+2x_2(k)-14x_3(k)+18x_4(k)+\sqrt{4+(2x_1(k)+2x_2(k)-14x_3(k)+18x_4(k))^2})\end{cases} \tag{10}$$

则可得其逆映射 V 为：

$$\begin{cases}x_1(k)=\frac{1}{2}(5(e^{y_1(k)}-e^{-y_1(k)})+5(e^{y_2(k)}-e^{-y_2(k)})+3(e^{y_3(k)}-e^{-y_3(k)})+e^{y_4(k)}-e^{-y_4(k)})\\ x_2(k)=\frac{1}{2}(2(e^{y_1(k)}-e^{-y_1(k)})+e^{y_4(k)}-e^{-y_4(k)})\\ x_3(k)=\frac{1}{2}(e^{y_1(k)}-e^{-y_1(k)}+2(e^{y_2(k)}-e^{-y_2(k)})+3(e^{y_3(k)}-e^{-y_3(k)})+4(e^{y_4(k)}-e^{-y_4(k)}))\\ x_4(k)=\frac{1}{2}(e^{y_2(k)}-e^{-y_2(k)}+2(e^{y_3(k)}-e^{-y_3(k)})+3(e^{y_4(k)}-e^{-y_4(k)}))\end{cases} \tag{11}$$

取

$$q(X_m(k),Y(k))=\frac{1}{8}e(k)=\frac{1}{8}(X_m(k)-V(Y(k)))$$
$$=\frac{1}{8}\begin{pmatrix}x_1(k)-V_1(y_1,y_2,y_3,y_4)\\ x_2(k)-V_2(y_1,y_2,y_3,y_4)\\ x_3(k)-V_3(y_1,y_2,y_3,y_4)\\ x_4(k)-V_4(y_1,y_2,y_3,y_4)\end{pmatrix}=\begin{pmatrix}q_1\\ q_2\\ q_3\\ q_4\end{pmatrix}$$

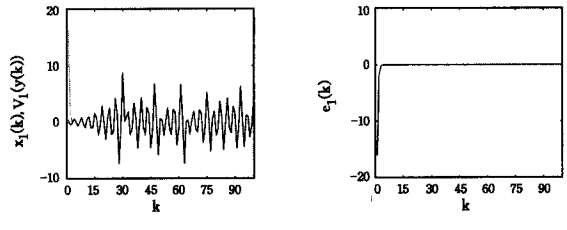
则

$$F_m(X)-q(X_m(k),Y(k))=$$
$$\begin{pmatrix}a_1x_1(k)-a_2(a_3-a_4x_4(k))x_2(k)-a_5x_3(k)-q_1\\ b_1(b_2-x_4(k))x_1(k)-b_3x_2(k)-b_4x_3(k)-q_2\\ c_1x_1(k)-c_2x_2(k)-c_3x_3(k)-q_3\\ d_1x_1(k)x_2(k)+d_2x_3(k)-q_4\end{pmatrix}=\begin{pmatrix}A\\ B\\ C\\ D\end{pmatrix}$$

$$Y(k+1)=G(Y,X)=H(F_m(X)-q(X_m(k),Y(k)))=$$
$$\begin{pmatrix}\ln\frac{1}{2}(-A+7C-9D+\sqrt{4+(A-7C+9D)^2})\\ \ln\frac{1}{2}(4A+2B-24C+30D+\sqrt{4+(4A+2B-24C+30D)^2})\\ \ln\frac{1}{2}(-5A-4B+33C-41D+\sqrt{4+(5A+4B-33C+41D)^2})\\ \ln\frac{1}{10}(2A+2B-14C+18D+\sqrt{4+(2A+2B-14C+18D)^2})\end{pmatrix}$$

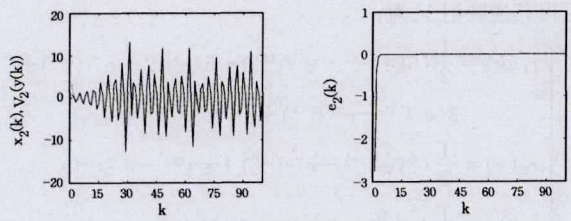
在初始条件 $X(0)=(0.387,0.77,0.771,0.395)$，$Y(0)=(1,1,1,1)$ 时，选取状态变量 $x_1(k)$，$V_1(y(k))$，$x_2(k)$，$V_2(y(k))$，其动力学曲线分别见图 1(a)和图 2(a)。其中实线表示 k-$X(k)$ 动力学曲线，虚线表示 k-$V(Y(k))$ 动力学曲线，$e(k)=X(k)-V(Y(k))$，k-$e(k)$ 的动力学曲线分别见图 1(b)和图 2(b)。可见，$X(k)$ 和 $Y(k)$ 关于变换 H 是广义同步的。随 k 的增大，$e(k)$ 趋向于(0,0,0,0)。

初始条件为式(12)时，广义混沌系统的状态变量 $X(k)$ 和 $Y(k)$ 迭代 2000 次的图像如图 3 所示，由图 4 的同步效果图可看出状态变量 $X(k)$ 和 $Y(k)$ 关于变换 H 广义同步。



(a)实线为 k-$x_1(k)$ 曲线；虚线为 k-$V_1(y(k))$ 曲线　　(b)k-$e_1(k)$ 曲线

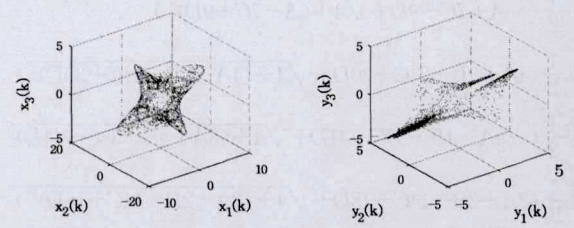
图 1



(a)实线为 k-$x_2(k)$ 曲线；虚线为 k-$V_2(y(k))$ 曲线　　(b)k-$e_2(k)$ 曲线

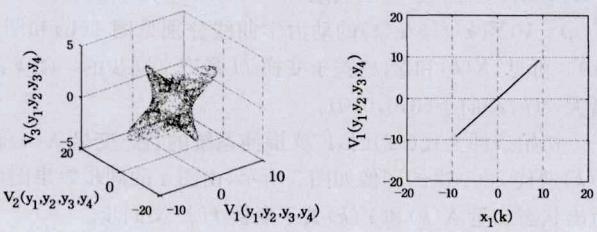
图 2

$$
\begin{cases}
x_1(0)=0.387\\
x_2(0)=0.77\\
x_3(0)=0.771\\
x_4(0)=0.395\\
y_1(0)=\ln\dfrac{1}{2}(-x_1(0)+7x_3(0)-9x_4(0)+\sqrt{4+(-x_1(0)+7x_3(0)-9x_4(0))^2})\\
y_2(0)=\ln\dfrac{1}{2}(4x_1(0)+2x_2(0)-24x_3(0)+30x_4(0)+\sqrt{4+(4x_1(0)+2x_2(0)-24x_3(0)+30x_4(0))^2})\\
y_3(0)=\ln\dfrac{1}{2}(-5x_1(0)-4x_2(0)+33x_3(0)-41x_4(0)+\sqrt{4+(-5x_1(0)-4x_2(0)+33x_3(0)-41x_4(0))^2})\\
y_4(0)=\ln\dfrac{1}{2}(2x_1(0)+2x_2(0)-14x_3(0)+18x_4(0)+\sqrt{4+(2x_1(0)+2x_2(0)-14x_3(0)+18x_4(0))^2})
\end{cases}
\tag{12}
$$



(a)$x_1(k)$，$x_2(k)$，$x_3(k)$状态变量轨迹图　　(b)$y_1(k)$，$y_2(k)$，$y_3(k)$状态变量轨迹图

图 3



(a)$V_1(y_1,y_2,y_3,y_4)$，$V_2(y_1,y_2,y_3,y_4)$，$V_3(y_1,y_2,y_3,y_4)$状态变量轨迹图　　(b)$x_1(k)-V_1(y_1,y_2,y_3,y_4)$曲线图

图 4

4　图像加密算法描述

图像加密方案为：假设甲方需要通过 Internet 向乙方发送一幅 $m\times n$ 的图像，其中 m 和 n 分别表示图像像素的行数和列数，像素值为[0，255]之间的整数，表示像素的灰度值。甲、乙双方共享系统(8)、(10)和密钥集

$$keys=\{a_1,a_2,a_3,a_4,a_5,b_1,b_2,b_3,b_4,c_1,c_2,c_3,d_1,d_2,x_1(k),x_2(k),x_3(k),x_4(k)\} \tag{13}$$

(1)取 m=123456789012，甲方通过式(8)、式(10)生成的加密序列$\{y_1(k),y_2(k),y_3(k),y_4(k)\mid k=1,2,\cdots,m\times n\}$得到 $z_i(i=1,2,3,4)$：$z_i=m\times(y_1+y_2+y_3+y_4)$。

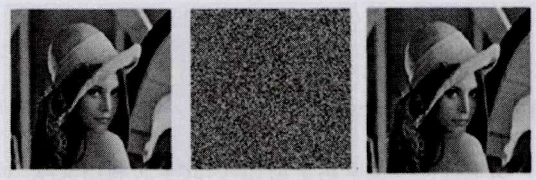
(2)甲方从生成的序列 z_1,z_2,z_3,z_4 中分别任意选出$m\times n$行，得到序列 t_1,t_2,t_3,t_4。

(3)读取彩色图像，M_1,M_2,M_3 分别代表图像的红、绿、蓝 3 层。甲方取生成的 t_1,t_2,t_3 对原始图像的像素值进行加密得到密文：$C_i=\mathrm{mod}(round(M_i+t_i),256)(i=1,2,3,4)$。

(4)乙方利用混沌系统的参数、初始值、变换 H 得到的序列，按照(3)和(4)逆向求解出明文图像。

5　实验仿真与性能分析

明文是 256×256 的 Lena 图像，如图 5(a) 所示。对明文按照第 3 节所述方案进行加、解密，效果如图 5(b)、(c)所示。



(a)原始图像　　(b)加密图像　　(c)正确密钥解密图像

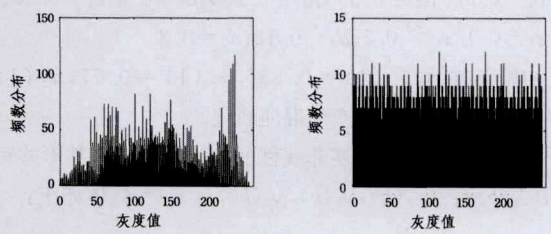
图 5

5.1　统计特性分析

统计分析从两个方面对加密效果进行测试，其一是图像加密前后的直方图，其二是相邻像素点之间的相关性。

(1)统计直方图

图 6(a)、(b)分别给出了 Lena 原始图像和加密图像的像素值统计直方图。由图 6(a)可知，原始图像的像素呈现明显的不均匀分布；而图 6(b)显示，加密图像的像素值呈现平坦分布，即加密图像的各个像素值的概率分布趋近于等概率分布。



(a)原始图像统计直方图　　(b)加密图像统计直方图

图 6

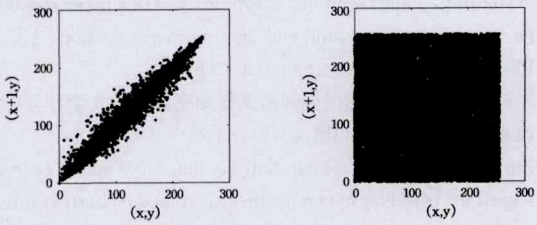
(2)相邻像素之间的相关性分析

由于图像包含了大量的冗余信息，两个相邻像素点是高度相关的，因此一个好的图像加密算法应尽量让密文图像相邻像素的相关性接近零。

图 7(a)、(b)示出垂直方向原始图像和加密图像相邻像素的相关关系。可见，原始图像像素间呈明显的线性关系，而密文图像像素间没有明显的相关性。

原始图像和加密图像相邻像素之间的相关系数如表 1 第 2、第 3 列所示。可见，尽管明文图像的相邻像素高度相关，但密文图像相邻像素点间的相关性几乎为零。从表 1 中可以看

到，相比文献[10]、文献[15]、文献[16]和文献[20]中 Lena 加密图像的相邻像素相关性，本算法的相关系数更低。



(a)原始图像相邻像素　　(b)加密图像相邻像素

图 7

表 1　Lena 图像明文和密文的相邻像素相关性

相邻方向	明文	密文	密文[10]	密文[15]	密文[16]	密文[20]
水平	0.9798	−0.0020	0.0058	0.0021	0.0033	0.0026
垂直	0.9930	−0.0001	0.0094	−0.0002	−0.0037	0.0034
对角	0.9710	−0.0016	0.0214	0.0009	−0.0043	−0.0019

5.2　密文信息熵分析

在信息论中，信息熵用以表征信源的不确定性程度。设 s 是一种信息源，信息熵的计算公式为：

$$H(s)=\sum_{i=1}^{n}p(s_i)\log p(s_i)$$

其中，信息值 s_i 的相应概率为 $\{p(s_1),p(s_2),\cdots,p(s_n)\}$。由最大信息熵定理可知，当信源等概率分布时，信息熵取到最大值 $\log_2(n)$bit。

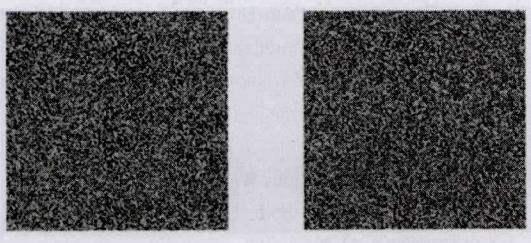
类似地，可以用密文的信息熵来度量加密后密文的像素值分布的均匀程度，若像素值为等概率分布，则信息熵取得最大值 8bit。本文算法中的信息熵与文献[18]、文献[19]和文献[21]算法中的信息熵的对比结果见表 2。可见，该加密算法得到的密文熵更接近理想值。

表 2　密文信息熵对比结果

图像三色	红色	绿色	蓝色
密文信息熵	7.9971	7.9972	7.9971
密文信息熵[18]	7.9909	7.9909	7.9905
密文信息熵[19]	7.9881	7.9899	7.9854
密文信息熵[21]	7.9896	7.9893	7.9896

5.3　密钥敏感性测试

一个安全的加密算法必须对密钥具有强烈的敏感性。本文密钥对参数的敏感度均达到了 10^{-15} 以上，即在 10^{-15} 扰动范围内，攻击者试图解密出原图像的几率接近于 0。该算法的敏感性高于文献[15]的敏感性 10^{-10}，高于文献[16]的敏感性 10^{-14}。下面对参数 b_2，c_1 分别依次进行精度为 10^{-15} 和 10^{-16} 的扰动，用生成的扰动密钥流进行解密，扰动解密图像见图 8。从图中可见，微扰后的密钥完全不能正确地解密出原始图像。因此，本算法对密钥有极强的敏感性。



(a)　　(b)

图 8　参数 b_2，c_1 扰动密钥解密图像

5.4　密钥空间

为了能够有效抵抗穷举攻击，理想的加密方案应尽可能使得密钥空间足够大。在广义同步混沌序列的产生过程中，该加密方案的密钥主要取决于广义混沌系统的系统参数和初始条件。对密钥敏感性测试的仿真结果表明，本文的密钥空间为 10^{288}（大于 2^{956}），与文献[10]、文献[15]、文献[16]、文献[19]和文献[20]密钥空间的对比结果见表 3。

表 3　密钥空间对比表

	本文	文献[10]	文献[15]	文献[16]	文献[19]	文献[20]
密钥空间	2^{956}	2^{508}	2^{198}	2^{198}	2^{196}	2^{190}

5.5　雪崩效应

雪崩效应是所有的密码加密算法都应该具备的一种特殊性质，它是指对密钥或原图的一个微小改变将引起加密图像的很大改变，就像发生雪崩一样。严格的雪崩效应要求修改原图或密钥的一个比特就能引起 50%的密文发生变化。

设扰动精度 $k=1\times10^{13}\times(rand(1)-0.5)$，对系统的部分参数和初始条件进行 100 次扰动，测得的平均变化率结果如表 4 所列。

表 4　对系统参数和初始值微小变化的敏感性

参数微变	平均变化率(%)	参数微变	平均变化率(%)
a_2+k	49.83	a_3+k	49.83
a_4+k	49.82	b_1+k	49.82
b_2+k	49.82	b_3+k	49.85
x_2+k	49.85	x_3+k	49.74

结束语　本文基于离散混沌系统广义同步理论，构造了一个四维广义混沌同步系统。基于该同步系统设计了一种图像加密方案，并对该方案进行了安全性分析。本文所采用的混沌系统维数高，参数多，密钥空间高达 10^{288}；该加密方案对密钥十分敏感，任何超过 10^{-15} 的密钥扰动都会使解密失效；密文和明文相邻像素的相关性接近于零；密文分布均匀，密文熵为 7.9971，7.9972，7.9971，非常接近于理想值 8；通过对部分参数和初始条件进行雪崩测试，测得的平均变化率均达到 49.80%左右，可以有效地抵抗差分攻击。分析结果表明，本文所设计的图像加密方案具有较高的安全性。

参 考 文 献

[1] Wu Wen-juan, Chen Zeng-qiang, Yuan Zhu-zhi. The evolution of a novel four-dimensional autonomous system: Among 3-torus, limit cycle, 2-torus, chaos and hyper[J]. Chaos Solition & Fractals, 2009, 39(5): 2340-2356

[2] Li Zhen-bo, Tang Jia-shi. Chaotic synchronization with parameter perturbation and its secure communication scheme[J]. Control Theory & Applications, 2014, 31(5): 592-600(in Chinese)
李震波，唐驾时. 参数扰动下的混沌同步控制及其保密通信方案[J]. 控制理论与应用，2014，31(5)：592-600

[3] Huang Li-lian, Yin Qi-tian. A chaos synchronization secure communication system based on output control[J]. Journal of Electronics & Information Technology, 2009, 31(10): 2402-2405(in Chinese)
黄丽莲，尹启天. 基于输出控制的混沌同步保密通信系统[J]. 电子与信息学报，2009，31(10)：2402-2405

[4] Guo Cheng, Chang Chin-chen, Sun Chin-yu. Chaotic maps-based mutual authentication and key agreement using smart cards for

wireless communications[J]. Journal of Information Hiding and Multimedia Signal Processing, 2013, 4(2): 99-109

[5] Zang Hong-yan, Min Le-quan, Zhao Geng. A generalized synchronization theorem for discret-time chaos system with application in data encryption scheme[C]// Proceeding of the 2007 Int. Conf. on Communications. Konkuoka Japan: Circuit and Systems, 2007: 1325-1329

[6] Liu Shu-tang, Zhang Fang-fang. Complex function projective synchronization of complex chaotic system and its applications in secure communication[J]. Nonlinear Dynamics, 2014, 76(2): 1087-1097

[7] Sheikhan M, Shahnazi R. Synchronization of general chaotic systems using neural controllers with application to secure communication[J]. Neural Computing and Applications, 2013, 22(2): 361-373

[8] Min Le-quan, Chen Guo-rong. Generalized synchronization in an array of nonlinear dynamic systems with applications to chaotic cnn [J]. International Journal of Bifurcation and Chaos, 2013, 23(1): 1350016-1-1350016-53

[9] Abdurahman K, Askar H, Guo Wen-qiang. Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN [J]. Optik-International Journal for Light and Electron Optics, 2014, 125(5): 1671-1675

[10] Zhu He-gui, Zhao Cheng, Zhang Xiang-de. A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem[J]. Signal Processing, 2013, 28(6): 670-680

[11] Edi S, Suryadi M T, Agus M M. The implementation of henon map algorithm for digital image encryption [J]. Telkomnika, 2015, 12(3): 2775-2780

[12] Guan Zhi-hong, Huang Fang-jun, Guan Wen-jie. A Chaos-based image encryption algorithm [J]. Physics Letters A, 2005, 346(1): 153-157

[13] Wang Shi-hong, Kuang Jin-yu, Li Jing-hua, et al. Chaos-based secure communications in a large community [J]. Phys Rev E, 2002, 66(6): 65202

[14] Wang Jing, Jiang Guo-ping. Cryptanalysis of a hyper-chaotic image encryption algorithm and its improved version [J]. Acta Phys. Sin., 2011, 60(6): 83-93(in Chinese)
王静, 蒋国平. 一种超混沌加密图像加密算法的安全性分析及其改进[J]. 物理学报, 2011, 60(6): 83-93

[15] Zhu Cong-xu, Hu Yu-ping, Sun Ke-hui. New image encryption algorithm based on hyperchaotic system and ciphertext diffusion in crisscross pattern[J]. Journal of Electronics & Information Technology, 2012, 34(7): 1735-1743(in Chinese)
朱从旭, 胡玉平, 孙克辉. 基于超混沌系统和密文交错扩散的图像加密新算法[J]. 电子与信息学报, 2012, 34(7): 1735-1743

[16] Chen Jun-xin, Zhu Zhi-liang, Fu Chong, et al. A fast image encryption scheme with a novel pixel swapping-based confusion approach [J]. Nonlinear Dynamics, 2014, 77(4): 1191-1207

[17] Xu Dao-lin, Chin Y C, Li Chang-pin. A necessary condition of projective synchronization in discrete-time systems of arbitrary dimensions[J]. Chaos Solitons and Fractals, 2004, 22(1): 175-180

[18] Liu Hong-jun, Wang Xing-yuan. Triple-image encryption scheme based on one-time key stream generated by chaos and plain images[J]. The Journal of Systems and Software, 2013, 86(3): 826-834

[19] Liu Shu-bo, Sun Jing, Xu Zheng-quan. An improved image encryption algorithm based on chaotic system [J]. Journal of Computers, 2009, 4(11): 1091-1100

[20] Fouda J S A E, Effa J Y, Samrat L S, et al. A fast chaotic block cipher for image encryption [J]. Communications in Nonlinear Science & Numerical Simulation, 2014, 19(3): 578-588

[21] Liu Hong-jun, Abdurahman K. Asymmetric color image encryption scheme using 2D discrete-time map [J]. Signal Processing, 2015, 113(2): 104-112

(上接第 73 页)

[3] Guo Bei-chen. Research on Self-adaptive Satellite Communication System Modulation Decision and Modulation Recognition Technology[D]. Harbin: Harbin Institute of Technology, 2013 (in Chinese)
国北辰. 自适应卫星通信调制方式决策与识别技术研究[D]. 哈尔滨: 哈尔滨工业大学, 2013

[4] Liu Guang-zu, Wang Jian-xin. Improved SNR estimation technique for BPSK and QPSK signals[J]. Applied Mechanics and Materials, 2013, 239: 994-999

[5] Rice M. Data-Aided and Non-Data-Aided Maximum Likelihood SNR Estimators for CPM[J]. IEEE Transactions on Communications, 2015, 63(11): 4244-4253

[6] Salman T, Badawy A, Elfouly T M, et al. Non-data-aided SNR Estimation for QPSK Modulation in AWGN Channel[C]// Proceedings of the 10th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). Larnaca: IEEE, 2014: 611-616

[7] Xu Hua, Wang Ai-fen, Yang Xiao-yu. Survey of the SNR Estimation of Conventional Digital Communication Signals[J]. Journal of Signal Processing, 2013, 29(6): 723-733(in Chinese)
许华, 王爱粉, 杨晓宇. 常规数字通信信号信噪比估计综述[J]. 信号处理, 2013, 29(6): 723-733

[8] Beaulieu N C, Toms A S, Pauluzzi D R. Comparison of four SNR estimators for QPSK modulations [J]. IEEE Communication Letters, 2000, 4(2): 43-45

[9] Li Zhi-xin, Wu Nan, Shi De-sheng, et al. A Low Complexity SNR Estimation for QPSK Modulation in AWGN Channel[C]// Proceedings of the 8th International ICST Conference on Communications and Networking in China. Guilin: IEEE, 2013: 129-132

[10] Xu Hua, Fan Long-fei, Zheng Hui. A precise SNR estimation algorithm for QPSK signals [J]. Journal on Communications, 2004, 25(2): 55-60(in Chinese)
许华, 樊龙飞, 郑辉. 一种精确的 QPSK 信号信噪比估计算法[J]. 通信学报, 2004, 25(2): 55-60

[11] Shin D J, Sung W, Kim I K. Simple SNR Estimation Methods for QPSK Modulated Short Bursts[C]// Proceedings of the IEEE Global Telecommunications Conference, 2001 (GLOBECOM'01). IEEE, 2001: 3644-3647

[12] Wu Tao, Zheng Hai-xin, Yan Di, et al. A modified SNR estimation algorithm based on singular value decomposition[C]// Proceedings of the 2014 International Conference on Information and Communications Technologies. Nanjing, China: IET, 2014: 1-5

[13] Chen Chao, Xu Chang-chun, Wang Yue, et al. Research on an Improved Algorithm for SNR Estimation[J]. Radio Engineering, 2012, 42(2): 62-64(in Chinese)
陈超, 徐长纯, 王玥, 等. 一种改进的信噪比估计算法[J]. 无线电工程, 2012, 42(2): 62-64