基于一个新的四维离散混沌映射的图像加密新算法

朱淑芹[1] 李俊青[1] 葛广英[2]

(聊城大学计算机学院 聊城 252059)[1] (聊城大学物理科学与信息工程学院 聊城 252059)[2]

摘 要 基于修正版 Marotto 定理构造了一个四维离散混沌映射,并利用该四维离散混沌映射序列设计了一种图像加密方案。该方案利用图像的 256 位哈希值来生成混沌序列的初始值,由此混沌序列产生的密钥与明文相关,进一步增强了加密系统的安全性。理论分析和仿真试验表明:该加密方案至少具有 3.4×10^{100} 的密钥空间;加密后图像直方图接近均匀分布;像素的相关性被消除;信息熵接近 8bit,没有明显的统计信息。该加密方案对混沌系统的初始条件扰动极为敏感,任何大于 10^{-15} 的扰动都将使解密失效;加密图像对明文图像极为敏感,能够抵抗差分攻击。

关键词 混沌,图像加密,Marotto 定理,SHA-256 哈希函数,位异或运算,循环移位操作

中图法分类号 TP391 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.01.036

New Image Encryption Algorithm Based on New Four-dimensional Discrete-time Chaotic Map

ZHU Shu-qin[1] LI Jun-qing[1] GE Guang-ying[2]

(School of Computer Science, Liaocheng University, Liaocheng 252059, China)[1]

(School of Physics and Information Engineering, Liaocheng University, Liaocheng 252059, China)[2]

Abstract A novel four-dimensional discrete-time chaotic system was constructed on the basis of a modified version of Marotto's theorem. On the basis of this system, a digital image encryption scheme was proposed, in which the 256-bit hash value of plain image is used to generate the initial value of the chaotic sequence. Therefore, the encryption key generated by the chaotic sequence is related with plain image to enhance the security of the encryption system. Theoretical analysis and simulation experiments show that the key space of the image encryption scheme is as large as 3.4×10^{100}. The histogram of the encrypted image is close to the uniform distribution. The correlation of pixels is eliminated. The information entropy of encrypted image is close to 8 bit and the encrypted image has no obvious statistical information. The scheme is extremely sensitive to perturbations of the initial conditions of the chaos system. Any perturbations which are larger than 10^{-15} will make corresponding decryptions impossible. The encrypted image is also very sensitive to the plain image and can resist differential attack.

Keywords Chaos, Image encryption, Marotto's theorem, SHA-256 hash function, Bitwise XOR operation, Circular shifting operation

1 引言

30 年来混沌动力学系统在数字图像加密、通信和信息处理、大脑神经网络分析、生物医学等领域得到了极其广泛的应用,因此构造出新的、高维的、具有优良伪随机性的混沌系统得到越来越多学者的关注。关国荣等人[1]把 Lorenz 系统的一个非线性项 xy 改为 x^2,构造了一个新的三维混沌系统,该系统的最大 Lyapunov 指数为 7.0661,与原 Lorenz 系统相比,其具有更加复杂的动力学行为;王兴元等[2]在原三维 Lorenz 系统的基础上添加一个非线性项,构造了四维超混沌 Lorenz 系统;Sun Kehui 等人[3]通过引入正弦参数构造四维 Lorenz 混沌系统;仓诗建等人[4]在一个三维二次混沌系统的基础上,增加一个状态变量,构建了一种新的四维二次超混沌系统;刘扬正[5]在三维 Liu 系统的基础上构造了四维 Liu 系统;庞寿全等人[6]在三维 Lorenz 系统上增加一个非线性控制器,构造了一个四维超混沌;满峰泉等人[7]在三阶 Qi 系统的基础上,构造了一个具有两个较大的正的 Lyapunov 指数和较大参数范围的新超混沌系统;Shi Xuerong 等[8]在以 Lorenz 系统为基础的一个新超混沌系统上,加入一个驱动信号,组成了一个四维非自治超混沌系统;张帆等[9]通过 Duffing 混沌系统和 lorenz 混沌系统的结合,产生了一个新的结构复杂、多参数的六维超混沌系统。但是这些混沌系统的构造都是在已知混沌系统的基础上进行改造得到的,并且这些混沌系统都是连续时间混沌系统。

利用离散混沌序列进行数字图像加密比利用连续混沌系统进行数字图像加密更具优越性,因为离散混沌映射比连续混沌系统产生混沌序列的速度快,并且省去了连续系统加密中的采样,从而加快了加密速度。最近,韩双霜等人[10]基于

到稿日期:2015-11-20 返修日期:2016-03-25 本文受国家自然科学基金面上项目(61573178),山东省高校智能信息处理与网络安全重点实验室资助。

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;葛广英(1964—),男,博士,教授,主要研究方向为图像处理、模式识别、机器视觉、物联网技术。

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，这对构造高维离散混沌映射具有借鉴意义。受此启发，本文构造了一个新的四维离散混沌映射，与文献[10]中的三维混沌映射相比，本文所构造的混沌映射具有更复杂的动力学行为，其产生的伪随机数范围更大；同时，利用新的四维混沌映射设计了一种图像加密新算法。在密码学中，SHA-256 是一种广泛使用的具有 256 位哈希值的加密哈希函数，若两幅图像只有细小差异，它们的哈希值将是完全不同的。在所设计的新算法中，将明文图像的哈希值按一定规则进行转换，使混沌映射的初值与其相关，所以混沌映射产生的密钥与明文相关，即加密不同的明文图像所用的密钥流不同，克服了一些混沌图像加密算法中密钥与明文无关使攻击者可以通过已知明文或选择明文攻击来获取加密密钥的缺点[11-19]，提高了算法的安全性。

2　新四维离散混沌映射的构造

2.1　修正的 Marotto 定理及文献[10]构造的三维混沌映射

定理 1[20]　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 $\bar{B}_r(Z)$ 上扩张，其中 $\bar{B}_r(Z)$ 是空间 $(R^n,\|\cdot\|)$ 中以 Z 为中心的闭球。

(2) Z 是 f 的返回扩张不动点，即存在点 $X_0\in B_r(Z)$ 及正整数 m，使得 $f^m(X_0)=Z$，其中 $B_r(Z)$ 是空间 $(R^n,\|\cdot\|)$ 以 Z 为中心的开球，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[10]构造的三维混沌映射如式(1)所示。

$$\begin{cases} x_{n+1}=\sin(x_n)\cdot\sin(y_n)-a\sin(z_n)\\ y_{n+1}=b\sin(x_n)\cdot\cos(y_n)\\ z_{n+1}=cy_n \end{cases} \tag{1}$$

其中，参数 $a=4,b=1.8,c=2$。选择初始值 $x_1=0.5,y_1=0.2,z_1=0.1$，其相图如图 1 所示。

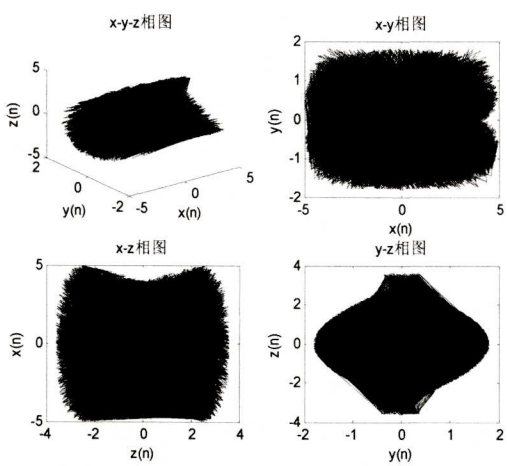


图 1　三维映射的混沌解轨道

2.2　新的四维离散混沌系统构造及其动力学分析

在混沌映射(1)的基础上对第三个式子添加了一个非线性项，第一个式子中的 z_n 换成 w_n，并通过增加一个关于 w_n 的迭代式子即可得到一个四维离散混沌系统，如式(2)所示：

$$\begin{cases} x_{n+1}=\sin(x_n)\cdot\sin(y_n)-a\sin(w_n)\\ y_{n+1}=b\sin(x_n)\cdot\cos(y_n)-x_n\\ z_{n+1}=cy_n+t\sin(z_n)\\ w_{n+1}=dy_n \end{cases} \tag{2}$$

其中，参数分别为 $a=b=4,c=3.5,d=2,t=4$ 时，此系统产生的序列是混沌序列，选择初始值 $x_1=2.7,y_1=0.8,z_1=1.5,w_1=0.8$，其相图如图 2 所示。

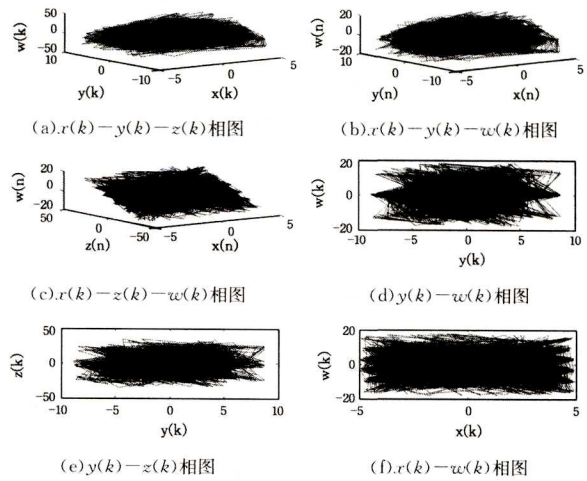


图 2　四维映射的混沌解轨道

计算混沌映射(1)的最大 Lyapunov 指数为 0.5453，而混沌映射(2)的最大 Lyapunov 指数为 0.8976，所以混沌映射(2)具有更复杂的动力学行为。对比图 1 和图 2 可以看出，混沌映射(2)产生的随机数范围更大，观察计算可知 $Z=(0,0,0,0)^{\mathrm{T}}$ 为该映射(2)的一个不动点，计算点 $Z=(0,0,0,0)^{\mathrm{T}}$ 的雅可比矩阵的 4 个特征值分别为：$\lambda_1=4,\lambda_2=-2.8845,\lambda_3=1.4422+2.4980\mathrm{i},\lambda_4=1.4422-2.4980\mathrm{i}$，即所有特征值的绝对值都大于 1，满足定理 1 中的(1)。另外经计算存在点 $X_0=(0,0,\arcsin(\mathrm{pi}/4),0)^{\mathrm{T}}\neq Z$ 及正整数 $m=2$，使得 $f^2(X_0)=Z$，其中 $X_1=f(X_0)=(0,0,\mathrm{pi},0)^{\mathrm{T}}$ 且 $\det Df(X_0)=-59.4231$，$\det Df(X_1)=96$，根据定理 1 可知，若 f 分别在 X_0,X_1 的某邻域内连续可微并满足 $\det Df(X_j)\neq 0(0\leqslant j\leqslant m-1)$ 且 $X_0\in Br_0(Z)$，则不动点 Z 为 f 的返回扩张不动点。式(2)是混沌映射的详细证明过程可参见文献[10]。

3　基于混沌的图像加密方案

3.1　混沌系统初始值的生成

在密码学中，SHA-256 是一种广泛使用的具有 256 位哈希值的加密哈希函数。本文的加密系统利用了由 SHA-256 产生的 256 位的外部密钥 K，即使两幅图像有细微差异，它们的哈希值将是完全不同的。因此，加密系统总复杂度为 2^{256}，可以抵抗蛮力攻击。把 256 位的密钥以 8 位为一组分成 32 组，因此 K 可以表示为 $K=k_1,k_2,k_3,\cdots,k_{32}$（$k_i$ 为由 0 和 1 组成的 8 位二进制位）。则混沌系统的初始值按式(3)－式(6)生成：

$$x_1=x_1'+\frac{(k_1\oplus k_2\oplus k_3\oplus k_4\oplus k_5\oplus k_6\oplus k_7\oplus k_8)}{256} \tag{3}$$

$$y_1=y_1'+\frac{(k_9\oplus k_{10}\oplus k_{11}\oplus k_{12}\oplus k_{13}\oplus k_{14}\oplus k_{15}\oplus k_{16})}{256} \tag{4}$$

$$z_1=z_1'+\frac{(k_{17}\oplus k_{18}\oplus k_{17}\oplus k_{20}\oplus k_{21}\oplus k_{22}\oplus k_{23}\oplus k_{24})}{256} \tag{5}$$

$$w_1=w_1'+\frac{(k_{25}\oplus k_{26}\oplus k_{27}\oplus k_{28}\oplus k_{29}\oplus k_{30}\oplus k_{31}\oplus k_{32})}{256} \tag{6}$$

其中，x_1'，y_1'，z_1'，w_1'是给定的初始值。

3.2 图像加密方案

(1)设明文图像为 G，图像数据二维矩阵为 $R1$，它的大小为 $m\times n$，给定 x_1'，y_1'，z_1'，w_1'，用式(3)－式(6)生成的 x_1，y_1，z_1，w_1 作为初始值，对混沌映射(2)迭代 $m*n$ 次，产生长度为 $m*n$ 的 4 个混沌序列 x,y,z,w。其中，$x=\{x_1,x_2,x_3,\cdots,x_{mn}\}$；$y=\{y_1,y_2,y_3,\cdots,y_{mn}\}$；$z=\{z_1,z_2,z_3,\cdots,z_{mn}\}$；$w=\{w_1,w_2,w_3,\cdots,w_{mn}\}$。

(2)利用混沌序列 x 按式(7)生成序列 $S=\{s_1,s_2,\cdots,s_{mn}\}\in[2,3,4,5,6,7]$。

$$\begin{cases} s_i=floor(x_i\times 10^{14}) \bmod 3+2, & \text{若 } i \bmod 2=0 \\ s_i=floor(x_i\times 10^{14}) \bmod 3+5, & \text{若 } i \bmod 2=1 \end{cases} \tag{7}$$

其中，$floor$ 函数代表向下取整。生成的序列 S 用来进行循环右移位操作。

(3)利用序列 y,z,w 生成的序列 T，引入如下变换方法[21]。令

$$T(X_k)=\mathrm{mod}(\mathrm{round}(\frac{255\sqrt{2}L(X_k-\min(X))}{\max(X)-\min(X)}),256) \tag{8}$$

其中，$X_k=k_1y_k+k_2z_kw_k$，$k_1=\sqrt{3}$，$k_2=\sqrt{5}$，$L=10^5$。$\min(X)=\min\{X_k\mid k=1,2,\cdots,mn\}$；$\max(X)=\max\{X_k\mid k=1,2,\cdots,mn\}$；round($a$)表示对数 a 四舍五入取整。由式(8)可以得到一个{0,1,…,255}范围的密钥流 $T=\{t_1,t_2,\cdots,t_{mn}\}$。图 3 是混沌密钥序列 T 的数值分布曲线。由图 3 可以看出，密钥流 T 分布均匀，伪随机性良好。

(4)把图像数据二维矩阵 $R1$ 转化为长度为 $m\times n$ 的一维矩阵，记为 $R=\{r_1,r_2,r_3,\cdots,r_{mn}\}$；把每一个 $r_i\in R$ 转化为一个八位二进制 r_i^t，然后按式(9)对 r_i^t 进行循环右移位操作，得到 $P^s=\{p_1{}^s,p_2{}^s,\cdots,p_{mn}^s\}$。

$$p_i^s=circshift(r_i^t,s_i) \tag{9}$$

其中，$i=1,2,3,\cdots,mn$。

再把每个 p_i^s 转化为十进制 p_i，得到序列 $P=\{p_1,p_2,\cdots,p_{mn}\}$。

(5)对得到的 P 进行如式(10)的操作，得到一维序列 $C^t=\{c_1{}^t,c_2{}^t,\cdots,c_{mn}^t\}$，再把 C^t 转化为 $m\times n$ 的矩阵即得密文图像 C。

$$c_i^t=p_i^t\oplus p_{i+1}^t\oplus p_{i+2}^t\oplus t_i \tag{10}$$

其中，$i=1,2,3,\cdots,mn$。p_{mn+1}^t 和 p_{mn+2}^t 是[1,255]中的随机数，可以看作密钥。

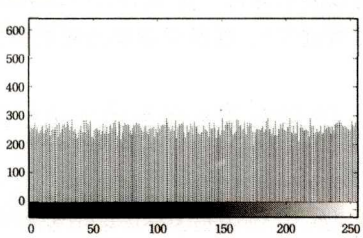


图 3 序列 T 的值分布曲线

3.3 图像解密算法设计

解密算法的前 3 步与加密算法的前 3 步是一样的。后面的两个步骤如下。

(1)$p_i^t=c_i^t\oplus p_{i+1}^t\oplus p_{i+2}^t\oplus t_i$

其中，$i=mn,mn-1,\cdots,1$。

(2)把每一个 P_i^t 转化为一个八位二进制 r_i^t，然后按式(11)对 r_i^t 进行循环左移位操作，得到 $R^k=\{r_1{}^k,r_2{}^k,\cdots,r_{mn}^k\}$，把 R^k 转化为 $m\times n$ 的矩阵即得明文图像 R。

$$r_i^k=circshift(r_i^t,-s_i) \tag{11}$$

其中，$i=1,2,\cdots,mn$。

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，其 sha-256 哈希值为“d6f35e24b1f70a68a37c9b8bfdcd91dc3977d7a98e67d453eb6f8003b6c69443”。加密系统的初始密钥集为 $keys=\{x_1',y_1',z_1',w_1',p_{mn+1}^t,p_{mn+2}^t$，明文图像 256 位哈希值$\}=\{2.7,0.8,1.5,0.8,123,234$，明文图像 256 位哈希值$\}$。由图 4(b)可见，在密文图像中看不出明文图像的任何信息，加密图像已经与明文图像没有任何关联。图 4(c)为解密后恢复出的明文图像。

(a)原图像 (b)最终加密后的图像 (c)正确密钥解密图像

图 4

5 安全性分析

本文进行了密钥空间分析、各种统计特性分析和敏感性分析以检测加密方案的安全性。其中统计特性分析包括统计直方图分析、密文熵分析、像素相关性分析。敏感性分析包括明文敏感性分析和密钥敏感性分析。

5.1 密钥空间分析

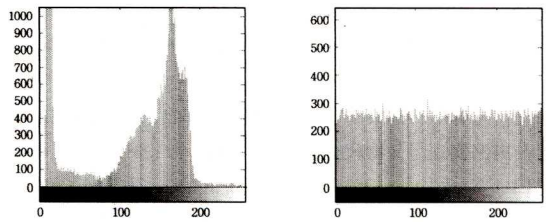
密钥空间是加密时可用的不同密钥数。密钥空间越大，算法抵抗蛮力攻击的性能越好。本算法的密钥集为 x_1'，y_1'，z_1'，w_1'，p_{mn+1}^t，p_{mn+2}^t 和 256 位长的哈希值。实验验证 x_1'，y_1'，z_1'，w_1'的精度可达 10^{-15}，密钥空间可达 10^{60}；进一步，SHA-256 的密钥空间可达 2^{128}，所以总的密钥空间可达 $10^{60}\times 2^{128}\approx 3.4\times 10^{100}$，若考虑 p_{mn+1}^t 和 p_{mn+2}^t 的取值，密钥空间可以达到 $10^{60}\times 256\times 256\times 2^{128}\approx 2.2\times 10^{105}$，如此大的密钥空间是可以抵抗蛮力攻击的。

5.2 统计特性分析

5.2.1 统计直方图

密文图像的直方图可以直观地反映加密质量的好坏，密文图像的直方图各级灰度分布越均匀，加密效果越好。图 5(a)和图 5(b)分别为明文图像及密文图像的统计直方图，横坐标表示灰度图像的 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。从统计直方图看，明文图像的直方图呈双峰分布，具有明显的统计特性；而密文图像的直方图中各像素取每个灰度级的频数基本相等，直方图没有明显的统

计特性，因而可以抵抗统计攻击。



(a)原图像统计直方图　　(b)加密后图像的直方图

图 5

5.2.2　密文图像信息熵分析

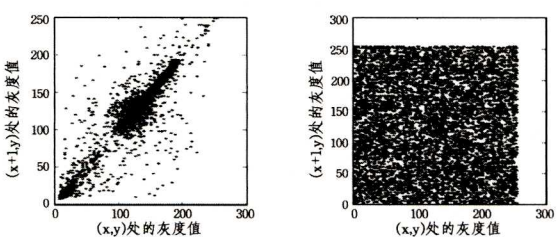
图像信息熵是衡量图像信息量大小的一个量，越杂乱无章的图像，其提供的信息量越小，但是信息熵越大。信息熵的计算公式如式(12)所示：

$$H=-\sum_{i=1}^{n}p_i\log_2(p_i) \tag{12}$$

其中，P_i 为第 i 级灰度出现的概率，当密文的概率分布为等概率分布时，即取[0,255]之间每一个值的概率均为$\frac{1}{256}$时，具有最大熵 8bit 。即信息熵越大，密文图像提供的信息量越小，加密效果越好。仿真实验中的密文图像的信息熵为 7.9894bit，非常接近理想值 8bit，表明加密效果良好。

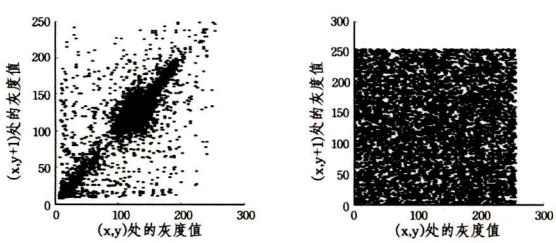
5.2.3　像素相关性分析

自然图像的特点之一便是相邻像素具有较强的相关性，从图 6(a)、7(a)、8(a)可以看出，明文图像沿竖直方向、水平方向和对角线方向 3 个方向的相邻像素间呈直线关系，具有很强的相关性。一般希望密文图像能消除这种相关性，即密文图像沿竖直方向、水平方向和对角线方向 3 个方向的相邻像素分布均衡。对于明文图像和密文图像，分别随机地选取 8000 个像素点作为参考点，以这些点为基准分别沿竖直方向、水平方向和对角线方向取其相邻的像素点与之构成 8000 个像素对，绘制这 3 个方向的相关性分布图，如图 6－图 8 所示。相关系数的计算公式如式(13)[17]所示，利用式(13)可得原明文图像和密文图像各自的相邻元素的相关系数，如表 1 所列。



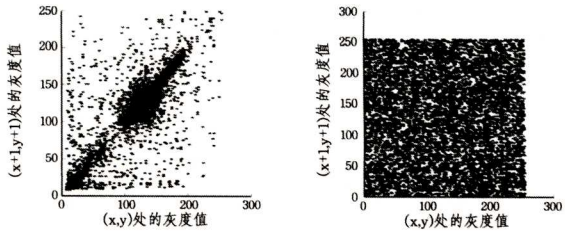
(a)明文图像水平方向相关分析　　(b)密文图像水平方向相关分析

图 6　水平方向相关性分布图



(a)明文图像垂直方向相关分析　　(b)密文图像垂直方向相关分析

图 7　垂直方向方向相关性分布图



(a)明文图像对角方向相关分析　　(b)密文图像对角方向相关分析

图 8　对角方向相关分析图

表 1　明文图像和密文图像中相邻像素的相关系数表

方向	原图像	密文图像
对角	0.9047	−0.0250
垂直	0.9307	−0.0032
水平	0.9618	−0.0143

$$xc=\frac{n\sum_{i=1}^{n}x_iy_i-\sum_{i=1}^{n}x_i\sum_{i=1}^{n}y_i}{\sqrt{n\sum_{i=1}^{n}x_i^2-(\sum_{i=1}^{n}x_i)^2}\sqrt{n\sum_{i=1}^{n}y_i^2-(\sum_{i=1}^{n}y_i)^2}} \tag{13}$$

其中，x_i，y_i 分别表示相邻两个像素的灰度值，n 表示选取的像素对数。从图 6(b)、图 7(b)、图 8(b)可以看出密文图像在 3 个方向的相邻像素分布均衡；从表 1 可以看出，密文图像各方向相邻像素间相关系数的绝对值很小，几乎为零。

5.3　敏感性分析

5.3.1　明文敏感性分析

密文对明文的敏感性是指明文图像即使只有很小的变化，加密后的密文图像将与原密文图像完全不同，像素数改变率(Number of Pixels Change Rate，NPCR)和归一化平均改变强度(Unified Average Changing Intensity，UACI)这两个概念可以度量加密算法对明文的敏感性。当两个明文图像仅存在一个像素不同时，设它们的密文图像中第(i,j)点的像素值分别为 $C_1(i,j)$和 $C_2(i,j)$。若 $C_1(i,j)=C_2(i,j)$，定义 $D(i,j)=0$；若 $C_1(i,j)\neq C_2(i,j)$，定义 $D(i,j)=1$。则 NPCR 与 UACI 的计算公式[22]分别为式(14)和式(15)所示：

$$NPCR=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D_{ij}}{M\times N}\times 100\% \tag{14}$$

$$UACI=\frac{(\sum_{i=1}^{M}\sum_{j=1}^{N}(\frac{c_1(i,j)-c_2(i,j)}{255}))}{M\times N}\times 100\% \tag{15}$$

NPCR 与 UACI 的理想期望值分别由式(16)[22]和式(17)计算。

$$NPCR_E=(1-2^{-m})\times 100\% \tag{16}$$

$$UACI_E=\frac{1}{2^{2m}}\frac{\sum_{i=1}^{2^m-1}i(i+1)}{2^m-1}\times 100\% \tag{17}$$

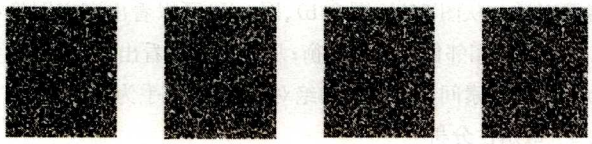
其中，M 和 N 分别是图像像素的行数与列数，m 为图像颜色位深。对于 8 位灰度图像($m=8$)，计算可得 $NPCR_E=99.6094\%$，$UACI_E=33.4635\%$。本算法中随机选取原图像中的 5 个像素点并改变其像素值，计算的 NPCR 和 UACI 如表 2 所列。由表 2 可见，计算出的 NPCR 和 UACI 都非常接近他们的理想期望值，原图像中一个像素灰度值的变化会导致加密图像中几乎所有像素灰度值发生变化，从而验证了该算法具有很好的抗差分攻击性能。

表 2 明文图像微小改变时 NPCR 和 UACI 测试结果

明文的微小改变	NPCR(%)	UACI(%)
G(35,45) 由 215 变为 216	99.5315561	33.412465
G(112,57) 由 34 变为 35	99.5789335	33.581594
G(135,145) 由 115 变为 116	99.6155685	33.451508
G(235,45) 由 25 变为 26	99.5647873	33.205069
G(128,173) 由 229 变为 230	99.4057973	33.105069

5.3.2 密钥敏感性测试

算法对密钥敏感是指当解密密钥与真实密钥即使有微小的误差时，解密出的图像与明文图像也毫无关联。数值模拟显示：本算法对密钥集中 x_1'，y_1'，z_1'，w_1' 的敏感程度非常高，都可以达到 10^{-15} 以上，即即使密钥值有 10^{-15} 的微小偏差，也破解不出原图像。图 9(a)－图 9(d)分别为密钥集 $keys=\{x_1',y_1',z_1',w_1'\}$ 中的密钥分别取下列值时的解密图像，$\{x_1',y_1',z_1',w_1'\}=\{2.7+10^{-15},0.8,1.5,0.8\}$；$\{x_1',y_1',z_1',w_1'\}=\{2.7,0.8+10^{-15},1.5,0.8\}$；$\{x_1',y_1',z_1',w_1'\}=\{2.7,0.8,1.5+10^{-15},0.8\}$；$\{x_1',y_1',z_1',w_1'\}=\{2.7,0.8,1.5,0.8+10^{-15}\}$。从图 9 可以看出在解密图像中得不到原图像的任何信息。



(a) (b) (c) (d)

图 9 错误密钥解密后的图像

结束语 本文在一个三维离散混沌系统的基础上构造了一个新四维离散混沌系统，新四维离散混沌系统比原三维离散混沌系统的动力学行为更复杂，生成的伪随机序列范围更大，并利用新四维离散混沌系统设计了一个图像加密新方案。在方案中用明文图像的 256 位哈希值来生成混沌系统的初值，由此生成的伪随机序列与明文相关，四维混沌生成的 4 个伪随机序列中，一个序列用来进行循环位移操作，另外 3 个序列生成一个{0,1,…,255}范围的密钥流，用来进行位异或操作。理论分析和仿真试验表明：该加密方案具有 3.4×10^{100} 的密钥空间；加密后的图像没有明显的统计信息，加密方案对混沌系统的初始条件和明文图像的变化都很敏感。因此密文图像能够抵抗蛮力攻击、统计攻击、差分攻击以及选择明(密)文的攻击。同时该算法经改进后也可以应用于 RGB 图像的加密。

参 考 文 献

[1] GUAN Guo-rong, WU Cheng-mao, JIA Qian. An improved high performance Lorenz system and its application[J]. Acta Physica Sinica, 2015, 64(2): 31-44. (in Chinese)
官国荣，吴成茂，贾倩. 一种改进的高性能 Lorenz 系统构造及其应用[J]. 物理学报，2015，64(2)：31-44.

[2] WANG Xing-yuan, WANG Ming-jun. Hyperchaotic Lorenz system[J]. Acta Physica Sinica, 2007, 56(9): 5136-5141. (in Chinese)
王兴元，王明军. 超混沌 Lorenz 系统[J]. 物理学报，2007，56(9)：5136-5141.

[3] SUN Kei-hui, LIU Xuan, ZHU Cong-xu, et al. Hyperchaos and hyperchaos control of the sinusoidally forced simplified Lorenz system[J]. Nonlinear Dynamics, 2012, 69(3): 1383-1391.

[4] CANG Shi-jian, CHEN Zeng-qiang, YUAN Zhu-zhi. Analysis and circuit implementation of a new four-dimensional non-autonomous hyper-chaotic system[J]. Acta Physica Sinica, 2008, 57(3): 1493-1501. (in Chinese)
仓诗建，陈增强，袁著祉. 一个新四维非自治超混沌系统的分析与电路实现[J]. 物理学报，2008，57(3)：1493-1501.

[5] LIU Yang-zheng. Circuit Implementation of Hyperchaotic Lü system [J]. Acta Physica Sinica, 2008, 57(3): 1139-1143. (in Chinese)
刘扬正. 超混沌 Lü 系统的电路实现[J]. 物理学报，2008，57(3)：1139-1143.

[6] PANG Shou-quan, LIU Yong-jian, ZHU Cong-xu. Circuit implementation and application of hyperchaotic Lorenz system[J]. Computer Engineering and Applications, 2013, 49(7): 235-239. (in Chinese)
庞寿全，刘永建，朱从旭. 超混沌 Lorenz 系统的电路实现与应用[J]. 计算机工程与应用，2013，49(7)：235-239.

[7] MAN Feng-quang, HOU Cheng-xi, WANG Zhong-lin, et al. Design and Implementation o f a Novel Hyper chaotic System[J]. Communications Technology, 2010, 43(11): 108-111. (in Chinese)
满峰泉，侯承玺，王忠林，等. 一个新的超混沌系统设计与实现[J]. 通信技术，2010，43(11)：108-111.

[8] SHI Xue-rong, WANG Zuo-lei. A single adaptive controller with one variable for synchronizing two identical time delay hyperchaotic Lorenz systems with mismatched parameterss[J]. Nonlinear Dynamcs, 2012, 69(1): 117-125.

[9] ZHANG Fan, LIU Jian-ming. A New Six-dimensional Hyperchaotic System and Its Circuit Implementation[J]. Science Technology and Engineering, 2013, 13(23): 6659-6666. (in Chinese)
张帆，刘剑鸣. 一种新六维超混沌系统及其电路实现[J]. 科学技术与工程，2013，13(23)：6659-6666.

[10] HAN Shuang-shuang, MIN Le-quan, HAN Dan-dan. A pseudo-random number generator using three dimensional chaotic map [J]. Hua Zhong Univ of Sci &-Tech (Natural Science Edition), 2013, 41(8): 16-19. (in Chinese)
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.

[11] HAN Shuang-shuang, MIN Le-quan, HAN Dan-dan. The algorithm design of a new chaotic image encryption[J]. Journal of Henan University of Science and Technology (Natural Science Edition), 2014, 35(5): 37-41. (in Chinese)
韩双霜，闵乐泉，韩丹丹. 一种新的混沌图像加密算法设计[J]. 河南科技大学学报(自然科学版)，2014，35(5)：37-41.

[12] SUI Lian-sheng, LIU Ben-qing, WANG Qiang, et al. Double-image encryption based on Yang-Gu mixture amplitude-phase retrieval algorithm and high dimension chaotic system in gyrator domain[J]. Optics Communications, 2015, 354(2015): 184-196.

[13] CAI Jun, CHEN Xin, XIANG Xu-dong. Substitution-Permutation Network Structred image Encryption algorithm based on chaotic map[J]. Computer Science, 2014, 41(9): 158-164. (in Chinese)
蔡俊，陈昕，向旭东. 一种基于混沌的代换-置换结构图像加密算[J]. 计算机科学，2014，41(9)：158-164.

[14] HAN Feng-ying, ZHU Cong-xu. New permutation-substitution Image Encryption Scheme Based on Chaos[J]. Journal of Wuhan

University(Natural Science Edition), 2014, 60(5): 447-452(in chinese)
韩凤英，朱从旭. 新型置换和替代结构的图像混沌加密算法[J]. 武汉大学学报(理学版)，2014，60(5)：447-452.

[15] HUANG Wei-qi, CHEN Zhi-gang, LIANG Di-qing, et al. Medical image encryption algorithm based on multiple chaotic systems[J]. Computer Science, 2012, 39(12): 261-263, 299. (in Chinese)
黄伟琦，陈志刚，梁涤青，等. 基于多混沌系统的医学图像加密算法[J]. 计算机科学，2012，39(12)：261-263，299.

[16] ZHOU Guo-min, ZHANG Da-xing, LIU Yan-jian, et al. A novel image encryption algorithm based on chaos and Line map[J]. Neurocomputing, 2015, 169(2015): 150-157.

[17] WANG Jing, JIANG Guo-ping. Cryptanalysis of a hyper-chaotic image encryption algorithm and its improved version[J]. Acta Physica Sinica, 2011, 60(6): 83-93. (in Chinese)
王静，蒋国平. 一种超混沌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.

[18] DENG Shao-jiang, ZHANG Dai-gu, PU Zhong-liang. Digital Image Scrambling Algorithm Based on Chaotic System[J]. Computer Science, 2008, 35(8): 238-240. (in Chinese)
邓绍江，张岱固，濮忠良. 一种基于混沌的图像置乱算法[J]. 计算机科学，2008，35(8)：238-240.

[19] 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.

[20] SHI Yu-ming, CHENG Guan-rong. Discrete Chaos in Banach Spaces [J]. Science in China Series A: Mathematics, 2005, 48(2): 222-238.

[21] LI Pei, MIN Le-quan, ZANG Hong-yan. A generalized chaos synchronization based pseudo random number generator and performance analysis [C]// International Conference on Communications, Circuits and Systems. Cheng du: Institute of Electrical and Electronics Engineers Computer Society, 2010: 781-785.

[22] BEHNIA 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

(上接第 171 页)

属性加密方案的特点，该加密方案适合一对多的广播加密应用，在数字内容安全方面有着较好的应用前景。

参 考 文 献

[1] SAHAI A, WATERS B. Fuzzy identify based encryption[M]// Advances in Cryptology-EUROCRYPT 2005. Springer Berlin Heidelberg, 2005: 457-473.

[2] LI Da-wei, YANG Geng, ZHU Li. A Verifiable key sharing scheme based on identity encryption[J]. Acta Electronica Sinica, 2010, 38(9): 2059-2065. (in Chinese)
李大伟，杨庚，朱莉. 一种基于身份加密的可验证秘密共享方案[J]. 电子学报，2010，38(9)：2059-2065.

[3] FENG Hua-min, SUN Tie-ru, SUN Ying. Private key share scheme based on identity authentication encryption and its application[J]. Journal of Computer Research and Application, 2014, 31(5): 1507-1510. (in Chinese)
封化民，孙铁茹，孙莹. 基于身份认证加密的私钥共享方案及其应用[J]. 计算机应用研究，2014，31(5)：1507-1510.

[4] SU Jin-shu, CAO Dan, WANG Xiao-feng, et al. Attribute-based encryption mechanism[J]. Journal of Software, 2011, 22(6): 1299-1315. (in Chinese)
苏金树，曹丹，王小峰，等. 属性基加密机制[J]. 软件学报，2011，22(6)：1299-1315.

[5] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]// IEEE Symposium on Security & Privaly. IEEE Computer Society. 2007: 321-334.

[6] CHEN Yan-li, DU Ying-jie, YANG Geng. An efficient certified key negotiation protocol based on attributes [J]. Computer Science, 2014, 41(4): 150-177. (in Chinese)
陈燕俐，杜英杰，杨庚. 一种高效的基于属性的认证秘钥协商协议[J]. 计算机科学，2014，41(4)：150-154，177.

[7] WATERS B. Ciphertext-Policy Attribute-based encryption: An expressive, efficient, and provably secure realization[C]// Lecture Notes in Computer Science. 2008: 321-334.

[8] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// Proc of Acmccs'. 2006: 89-98.

[9] SONG Shuai-feng. Research of data access control based on attribute collection encryption[D]. Zhengzhou: Zhengzhou University, 2013. (in Chinese)
宋帅峰. 基于属性集合加密的数据访问控制研究[D]. 郑州：郑州大学，2013.

[10] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE[C]// Proceedings of the 14th ACM Conference on Computer and Communications Security. ACM, 2007: 456-465.

[11] NISHIDE T, YONEYAMA K, OHTA K. Attribute-based encryption with partially hidden encryptor-specified access structures: Applied cryptography and network security[C]// New York: Lecture Notes in Computer Science. 2008: 111-129.

[12] KARCHMER M, WIGDERSON A. On span programs: Structure in complexity theory conference[C]// San Diego, California: Proceedings of the Eighth Annual. IEEE, 1993: 102-111.

[13] BEIMEL A. Secure schemes for secret sharing and key distribution[D]. Haifa, Israel: Technion-Israel Institute of technology, Faculty of Computer Science, 1996.

[14] LIU Zhen, CAO Zhen-fu. On efficiently transferring the linear secret-sharing scheme matrix in ciphertext-policy attribute-based encryption[J/OL]. http://www.iacr.org/cryptodb/data/paper.php?pubkey=23275.

[15] DAN B, FRAKLIN M. Identity based encryption from the Weil pairing: Advances in Cryptology[J]. Lecture Notes in Computer Science, 2003, 32(3): 213-229.

[16] REN Yan-li, ZHANG Xin-peng, QIAN Zhen-xing. Anonymous identity-based encryption scheme in groups of prime order [J]. Journal of Beijing University of Posts and Telecommunications, 2013, 36(5): 96-98. (in Chinese)
任艳丽，张新鹏，钱振兴. 素数阶群中基于身份的匿名加密方案[J]. 北京邮电大学学报，2013，36(5)：96-98.

[17] XIA Chuan, ZHOU Ji-shuai. Research on cloud manufacturing resource-aware and access technology using RFID[J]. Journal of Harbin Institute of Technology, 2014, 21(3): 101-110.