基于一个新的五维离散混沌的快速图像加密算法

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 结合 Logistic 映射和三维离散 Lorenz 映射,构造了一个新的五维离散混沌映射。基于该映射,提出了一个只有两轮扩散操作的图像加密算法,在第一轮扩散操作中的密钥流与明文相关,在第二轮扩散操作中的密钥流与第一轮的密文相关,这导致算法中的最终加密密钥与明文相关且密文与明文、密钥之间的关系复杂化。实验结果和安全性分析表明,该算法具有密钥空间大、密文图像统计特性良好、密文对明文和密钥非常敏感、抵抗选择明(密)文的攻击、加密速度快的优点。所提算法在图像保密通信和存储应用中将具有良好的应用前景。

关键词 五维离散混沌,图像加密,两轮扩散,抵抗选择明(密)文的攻击
中图法分类号 TP391 **文献标识码** A

Fast Image Encryption Algorithm Based on Novel Five Dimensional Discrete Chaos

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 Combining the Logistic mapping and 3D discrete Lorenz mapping, a new five dimensional discrete chaotic map was constructed. Based on the map, an image encryption algorithm with only two rounds of diffusion operation was proposed. In the first round of the diffusion operation, the key stream is related to the plaintext and the key stream in the second round diffusion operation is related to the ciphertext of first round. Therefore, the final encryption key of the algorithm is related to the plaintext and the relationship among ciphertext, plain text and key becomes complicated. Experimental results and security analysis show that the algorithm has a large key space, good statistical characteristics for ciphertext, high sensitiveness for ciphertext to plaintext and key, resistance to chosen plaintext and ciphertext, fast encryption speed. So, this algorithm has good application prospects in image secure communication and storage applications.

Keywords Five dimensional discrete chaos, Image encryption, Two rounds of diffusion operation, Resistance to choose plain (cipher) text attack

1 引言

混沌是由确定的非线性系统产生的一种有趣的物理现象,由于它在各个领域中的重要应用,被认为是 20 世纪物理学的三大成就(相对论、量子力学、混沌)之一。自 1963 年 Lorenz 混沌吸引子被发现以来,混沌一直是学术界研究的热点。在过去的几十年里,许多学者致力于构造具有各种动力学行为的混沌吸引子,许多新的混沌系统不断被提出。例如 Liu 等[1]构造了一个三维二次自治混沌系统,该混沌系统不仅产生四涡卷混沌吸引子,也产生共存吸引子;Li 等[2]提出一个三维二次自治系统,该系统具有 4 个二次非线性项,在不同的参数下它表现为 1 个极限环、2 个稳定点和 5 个奇怪吸引子;官国荣等[3]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 指数是 7.0661;朱淑芹等[4]利用 Silnikov 定理构造了一个三维二次多项式混沌系统,该系统具有 Smale 马蹄意义下的混沌。而超混沌系统是指具有两个或两个以上的正的 Lyapunov 指数的混沌系统,表明系统的混沌动力学行为向多个方向扩展,从而产生更复杂的吸引子,因此超混沌引起了越来越多学者的研究兴趣。基于一些知名的三维混沌系统如 Chen 系统[5]、Lü 系统[6]、广义劳伦兹系统[7]、统一混沌系统[8],几个四维超混沌系统[9-13]被构造出来。以上混沌系统都是连续时间混沌系统,并且都是在已知混沌系统的基础上进行改造得到。然而在混沌的许多应用领域中需涉及到计算机的应用,虽然由于计算机精度的限制,连续混沌系统和离散混沌系统在迭代上都会涉及到精度损失,但数字计算机不能支持连续的混沌系统,将连续混沌离散化必将引起巨大的误差,这样连续混沌比离散混沌的误差更大,因此在密码学和扩频通信领域应用离散混沌映射比应用连续混沌映射更有优越性,构造离散混沌映射也更有意义。经典的离散混沌映射主要有 Logistic 映射、Chebyshev 映射、tent 映射、Sine 映射、二维的 Henon 映射、三维离散 Lorenz 映射。韩双霜等[14]基于修正版 Marotto 定理构造了一个二维离散混沌映射,同时基于修正版 Marotto 定理还构造了一个三维离散混沌映射[15];

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。

DraganLambi′c[16]基于排列组合构造了一个一维离散混沌映射。本文结合 Logistic 映射和三维离散 Lorenz 映射，构造了一个五维离散混沌映射。

由于混沌系统的伪随机性、不确定性和对初始条件与系统参数的极为敏感性等特性正好吻合了密码学的扩散和混淆两条基本原则，从而基于混沌的数字图像加密逐渐成为一个研究热点。国内外学者提出了许多加密算法[17-19]，但本文认为算法越复杂，加密速度越慢，好的加密算法不在于算法的复杂性，而需满足以下几点：1)混沌系统生成的密钥流要均匀；2)算法的密钥空间要足够大；3)密文图像统计特性良好；4)密文对明文和密钥非常敏感；5)算法能抵抗选择明(密)文的攻击；6)算法加密速度快。目前基于混沌的数字图像加密算法主要包括两步：像素置乱和像素扩散。在置乱过程中，图像像素位置发生改变，置乱的主要目的是打破图像相邻像素间的相关性，但它不能改变图像的直方图。在扩散过程中，像素值依次被修改，即使像素的一个微小变化都可蔓延到整个图像几乎所有的像素，这样相邻像素之间的相关性也被打破了。事实上，基于混沌的图像加密方案中，置乱过程是不必要的。因为扩散阶段的密钥流一旦被破解，无论置换阶段的密钥流多么复杂，都可以构造特殊向量 $p=\{1,2,3,\cdots,m*n\}$($m\times n$ 代表加密图像的大小)通过选择明文攻击来破解置乱阶段的密钥流。因此，为了节省加密速度，提高加密效率，在新的五维离散混沌映射的基础上，本文提出了一个只有两轮扩散操作的图像加密算法。为了使算法能抵抗选择明(密)文的攻击，达到一次一密的加密效果，有两种方法：1)在混沌密钥流生成阶段使混沌的初始值与明文相关，这样产生的混沌密钥流与明文相关；2)在加密程中，引入密文扩散机制，使得最终的密钥流与明文相关。本文选择了后者，在第一轮扩散操作中，最终的密钥流与明文相关，在第二轮扩散操作中最终的密钥流与第一轮的密文相关。

2 新的五维离散混沌映射的构造

2.1 Logistic 映射[20]

Logistic 映射是一个比较简单的被广泛应用的一维离散混沌映射，其定义为：

$$x(k+1)=\mu x(k)(1-x(k))$$

其中，$\mu(0\leqslant\mu\leqslant4)$为分支参数，$x(k)\in(0,1)$。当 $3.5699456\cdots<\mu\leqslant4$时，Logistic 映射处于混沌状态，此时通过该系统方程产生的序列是非周期的、不收敛的，且对初值是敏感的。

2.2 三维离散 Lorenz 映射[21]

三维离散 Lorenz 映射的定义为：

$$\begin{cases}x(k+1)=x(k)y(k)-z(k)\\y(k+1)=x(k)\\z(k+1)=y(k)\end{cases}$$

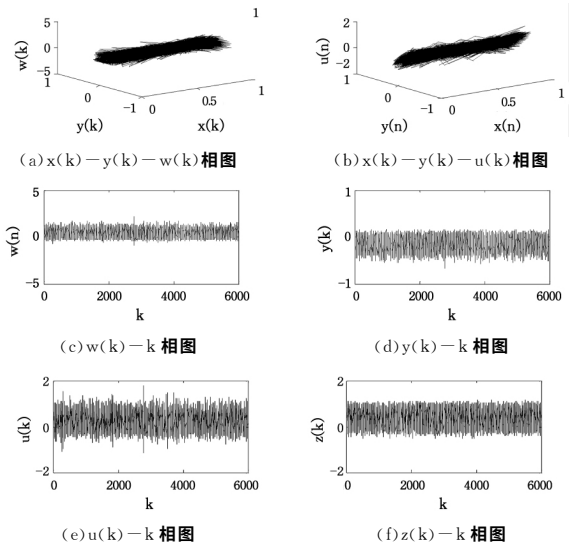
该系统的 3 个李雅普诺夫指数分别为：0.07456，0，−0.07456，因此是混沌系统。

2.3 新的五维离散混沌映射

结合 Logistic 映射和三维离散 Lorenz 映射，构造的新五维离散混沌映射如式(1)所示：

$$\begin{cases}x(k+1)=a(x(k)-x(k)x(k))\\y(k+1)=by(k)z(k)-cw(k)\\z(k+1)=x(k)+y(k)\\u(k+1)=y(k)+dw(k)\\w(k+1)=z(k)+x(k)u(k)\end{cases}\tag{1}$$

其中，$x(k)$，$y(k)$，$z(k)$，$u(k)$，$w(k)$为系统的状态变量，a，b，c，d 为实数，是系统的参数。当 $a=4$，$b=0.5$，$c=0.3$，$d=0.9$ 时，系统为混沌系统，且用 wolf 方法计算的该系统的 5 个李雅普诺夫指数分别为：0.17857，0.07843，−0.06597，−0.16784，−0.18764。由此可见新系统是一个超混沌系统，具有更加复杂的动力学行为，取初值$(x(0),y(0),z(0),u(0),w(0))=(0.9,-0.28,0.183,0.5,0.57)$，系统迭代 6000 次的混沌轨迹如图 1 所示。



(a)x(k)−y(k)−w(k)相图　(b)x(k)−y(k)−u(k)相图

(c)w(k)−k 相图　(d)y(k)−k 相图

(e)u(k)−k 相图　(f)z(k)−k 相图

图 1　五维映射的混沌解轨道

3 基于混沌的图像加密方案

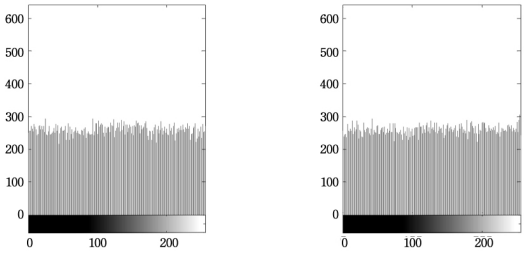
不失一般性，假设明文图像是一个具有 256 级灰度、大小为 $L=m\times n$ 的图像，它是一个 m 行 n 列的整数矩阵，其元素值的范围为 0～255。它的数据可以被视为一个一维向量$R=\{r_1,r_2,r_3,\cdots,r_{mn}\}$，这里 r_i 表示图像矩阵中第 $\mathrm{floor}(i/n)$行、第 $\mathrm{mod}(i,n)$列的像素灰度值。其中 $\mathrm{floor}(x)$表示取不大于 x 的最大整数，$\mathrm{mod}(a,b)$表示求模运算。混沌系统(1)用于生成原始混沌密钥流。在该加密方案中最终的密钥流不仅与原始混沌密钥流有关，还与明文图像有关，图像加密方案包括生成原始混沌密钥流和两轮扩散运算。

3.1 基于混沌系统的密钥流的生成

(1)设明文图像的大小为 $m\times n$，给定$(x(0),y(0),z(0),u(0),w(0))=(0.9,-0.28,0.183,0.5,0.57)$作为初始值，对混沌映射(1)进行 $m*n$ 次迭代，产生长度为 $m\times n$ 的 5 个混沌序列 X,Y,Z,U,W。其中，$X=\{x(1),x(2),x(3),\cdots,x(mn)\}$；$Y=\{y(1),y(2),y(3),\cdots,y(mn)\}$；$Z=\{z(1),z(2),z(3),\cdots,z(mn)\}$；$U=\{u(1),u(2),u(3),\cdots,u(mn)\}$；$W=\{w(1),w(2),w(3),\cdots,w(mn)\}$。

(2)混沌序列是非周期序列，但是由于计算机精度的限制，混沌序列在迭代过程中必将退化为周期序列，而且生成的序列周期也不好度量，为克服这一缺陷，将多个混沌序列进行一个非线性函数运算，以得到周期更长的序列。利用式 $D_1=\cos^2((X+Y+Z)/3)$、式 $D_2=\cos^2((U+W)/2)$的变换将混沌流 X,Y,Z,U,W 转化为[0,1]区间上的序列 D_1、D_2。其次，将[0,1]区间上的 D_1 和 D_2 分别通过下列变换：$S=\mathrm{mod}(\mathrm{round}(10^{15}D_1),256)=(s_1,s_2,s_3,\cdots,s_{mn})$和 $T=\mathrm{mod}(\mathrm{round}(10^{15}D_2),256)=(t_1,t_2,t_3,\cdots,t_{mn})$生成$\{0,1,\cdots,255\}$的密钥流 S 和 T，分别作为两轮扩散操作中的原始密钥。图 2 是混

沌密钥序列 S,T 的数值分布曲线，其中横坐标代表{0,1,…,255}中的 256 个数，纵坐标代表密钥流中取{0,1,…,255}中每个数的频数。由图 2 可以看出，密钥流 S,T 分布均匀，伪随机性良好。



(a)序列 S 的值分布曲线　　(b)序列 T 的值分布曲线

图 2

3.2 两轮扩散操作的图像加密方案

设明文图像的大小为 $m\times n$，把图像数据二维矩阵转化为长度为 $m\times n$ 的一维矩阵，记为 $R=\{r_1,r_2,r_3,\cdots,r_{mn}\}$。

第一轮的加密公式分别由式(2)和式(3)表示：

$$p_1=\text{bitxor}(\text{mod}(r_1+s_0,256),\text{mod}(s_1+p_0,256)) \quad (2)$$

$$p_i=\text{bitxor}(\text{mod}(r_i+s_{i-1},256),\text{mod}(s_i+p_{i-1},256)) \quad (3)$$

其中，$i=2,3,\cdots,mn$，$P=(p_1,p_2,\cdots,p_{mn})$ 为第一轮加密后的密文。p_0,s_0 为{0,255}上的随机数。

第二轮的加密公式分别由式(4)和式(5)表示：

$$c_1=\text{bitxor}(p_1,\text{bitxor}(\text{mod}(p_{m*n}+t_1,256),t_1)) \quad (4)$$

$$c_i=\text{bitxor}(p_i,\text{bitxor}(\text{mod}(c_{i-1}+t_i,256),t_{i-1})) \quad (5)$$

其中，$i=2,3,\cdots,mn$，$C=(c_1,c_2,\cdots,c_{mn})$ 为第二轮加密后的密文。把 C 转化为 m 行 n 列的矩阵后得最终的密文图像。

3.3 图像解密方案

解密秘钥就是加密秘钥，产生过程见 3.1 节。解密方案和加密方案相似，是加密方案的反过程。

第一轮解密是对第二轮加密的反操作，如式(6)、式(7)所示：

$$p_i=\text{bitxor}(c_i,\text{bitxor}(\text{mod}(c_{i-1}+t_i,256),t_{i-1})) \quad (6)$$

其中，$i=mn,\cdots,3,2$。

$$p_1=\text{bitxor}(c_1,\text{bitxor}(\text{mod}(p_{m*n}+t_1,256),t_1)) \quad (7)$$

第二轮解密是对第一轮加密的反操作，如式(8)、式(9)所示：

$$r_i=\text{mod}(\text{bitxor}(p_i,\text{mod}(s_i+p_{i-1},256))-s_{i-1},256 \quad (8)$$

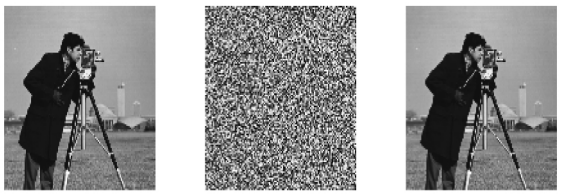
其中，$i=mn,\cdots,3,2$。

$$r_1=\text{mod}(\text{bitxor}(p_1,\text{mod}(s_1+c_0,256))-s_0,256) \quad (9)$$

把 $R=\{r_1,r_2,r_3,\cdots,r_{mn}\}$ 转化为 m 行 n 列的矩阵后得最终的解密图像。

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 $keys=\{(x(0),y(0),z(0),u(0),w(0),c_0,s_0)=(0.9,-0.28,0.183,0.5,0.57,128,234)\}$。其中图 3(a)为原明文图像，图 3(b)为两轮扩散后的密文图像，图 3(c)为解密后复出的明文图像。由图 3(b)可知，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一点关联，由图 3(c)可知，恢复出的明文图像与原明文图像在视觉上看不出任何区别。



(a)原明文图像　(b)两轮扩散后的密文图像　(c)解密后复出的明文图像

图 3

5 安全性分析

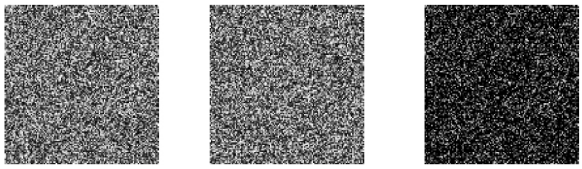
5.1 密钥空间和密钥敏感性分析

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 $keys=\{(x(0),y(0),z(0),u(0),w(0),c_0,s_0)$。下面将对密钥的敏感性进行分析，从而得到相应密钥的空间大小。用参数 P 来描述敏感性，$P\in[0,1]$，P 越大说明该参数越敏感。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 $C3$，则 $C2$ 与 $C1$ 灰度值不同的像素数 $Num1$ 占整个图像的比例和 $C3$ 与 $C1$ 灰度值不同的像素 $Num2$ 占整个图像的比例取均值，得到 P，即 $P=0.5*(Num1/m\times n+Num2/m\times n)$，其中 $m\times n$ 表示图像的大小。以此方法计算出各密钥的敏感性，如表 1 所列。计算的结果表明初始状态值具有很强的敏感性。计算中密钥 $x(0),y(0),z(0),u(0),w(0)$ 的改变量 h 均是 10^{-15}。基于密钥敏感性的结果，$x(0),y(0),z(0),u(0),w(0)$ 的精度可达 10^{-15}，密钥空间可达 $10^{15}\times10^{15}\times10^{15}\times10^{15}\times10^{15}=10^{75}$，进一步若考虑 c_0 和 s_0 的取值，密钥空间更大，这么大的密钥空间是可以抵抗蛮力攻击的。

表 1　各参数的敏感性

密钥	x(0)	y(0)	z(0)	u(0)	w(0)
敏感性 P	0.9965	0.9967	0.9976	0.9956	0.9964

另外，密钥敏感性还可以从可视化的角度来体现。图 4(a)为“cameraman“原密文图像，图 4(b)为密钥集 $keys=\{(x(0),y(0),z(0),u(0),w(0),c_0,s_0)=(0.9+10^{-15},-0.28,0.183,0.5,0.57,128,234)\}$时的解密图像，图 4(c)为图 4(a)与图 4(b)的差值图像。可以看出错误解密后的图像与原始图像毫无关联。对于另外 4 个密钥 $y(0),z(0),u(0),w(0)$ 的微小改变也有类似的结果。



(a)“cameraman”原密文图像　(b) keys $=\{(x(0),y(0),z(0),u(0),w(0),c_0,s_0)=(0.9,-0.28,0.183,0.5,0.57,128,234)\}$时的解密图像　(c)图(a)与图(b)的差值图像

图 4

5.2 明文敏感性测试

可以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。像素变化率和归一化平均变化强度分别表示随机地改变原始图像的某个像素灰度值以后，加密图像像素灰度值发生改变的数目所占的百分比以及变化程度。NPCR 和 UACI 的计算公式[22]分别为：

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

$$UACI=\frac{(\sum_{i=1}^{M}\sum_{j=1}^{N}(\frac{x(i,j)-x'(i,j)}{255}))}{M\times N}\times 100\%$$

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。NPCR 与 UACI 的理想期望值分别由式[22] $NPCR_E=(1-2^{-m})\times 100\%$ 和式 $UACI_E=\frac{1}{2^{2m}}\frac{\sum_{i=1}^{2^m-1}i(i+1)}{2^m-1}\times 100\%$ 计算。m 为图像颜色位深，对于 8 位灰度图像($m=8$)，NPCR 与 UACI 的理想期望值分别为：$NPCR_E=99.6094\%$，$UACI_E=33.4635\%$。本算法随机选取“cameraman”图像中 100 个像素点，改变它们的像素值，结果计算的 NPCR 值最大为99.643%，最小为99.567%，平均值为 99.6089%。UACI 值最大为 33.675%，最小为 33.367%，平均值为 33.466%，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。从而验证了该算法对明文敏感，具有很好的抗差分攻击性能力。

5.3 统计特性分析

本文提出的加密方案中最终所用密钥流不仅与混沌系统有关，还与明文图像有关。加密时顺次加密图像中的每个像素，所以经两轮扩散后的密文图像是一幅随机图像，这主要表现为密文图像直方图呈均匀分布、密文图像相邻像素相关性很小、密文图像的信息熵接近于 8 以及明、密文峰值信噪比较小。

5.3.1 统计直方图

直方图是数字图像的一个基本属性，揭示了图像像素的分布规律，密文图像的直方图分布对整个密码的安全性起着至关重要的作用，直方图分布越均匀，说明加密效果越好。为了表明算法的有效性，本文加密了 4 幅经典图像，图 5－图 8 中的(a)－(d)分别是“rice”、“cameraman”、“pout”、“pepper” 4 幅数字图像的原图像、加密后的图像、原图像的直方图、加密后图像的直方图。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。从统计直方图看出，原图像的直方图中各像素值的概率分布都是不均匀的，而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。

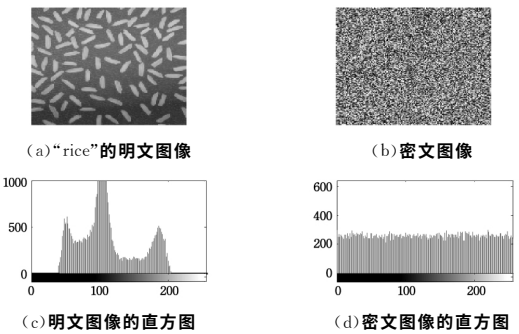


图 5

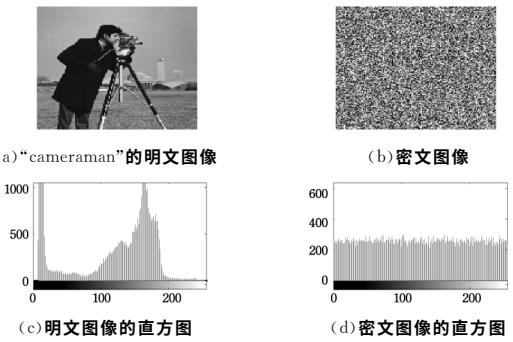


图 6

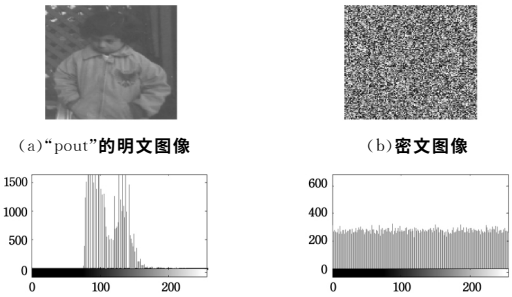


图 7

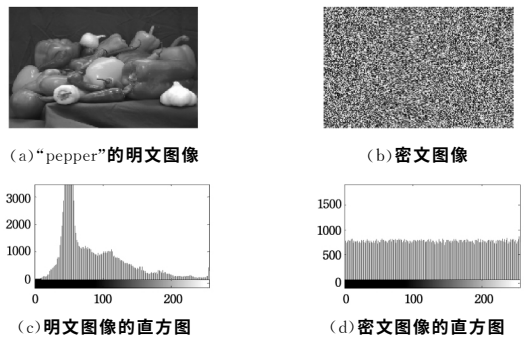


图 8

5.3.2 像素相关性分析

一幅自然图像中各个像素不是独立的，具有很强的相关性，即大块区域中图像的灰度值相差不大，图像信息的冗余度很大，而图像加密的目标之一就是去除图像信息的冗余性，减小相邻像素的相关性。像素相关性分析主要是水平像素、垂直像素和对角线像素的相关分析。对于“cameraman”明文图像和密文图像，分别随机地选取 4000 个像素点作为参考点，以这些点为基准分别沿水平方向、竖直方向和对角线方向取其相邻的像素点与之构成像素对，绘制其相关性分布图，如图 9 和图 10 所示。

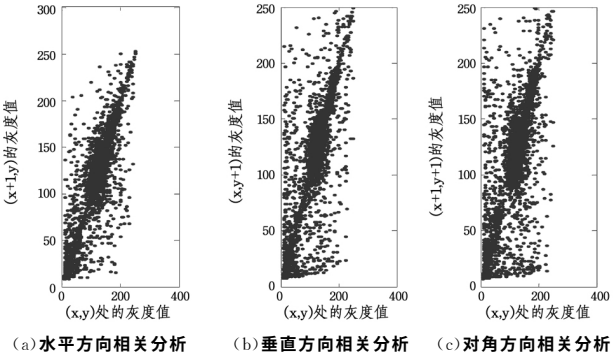
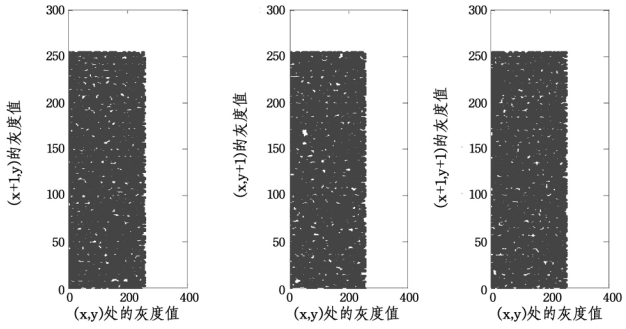


图 9 明文图像的相关性分布图



(a)水平方向相关分析　(b)垂直方向相关分析　(c)对角方向相关分析

图 10　密文图像的相关性分布图

其中图 9(a)为“cameraman”明文图像的水平方向相关分析图，图 9(b)为明文图像的垂直方向相关分析图，图 9(c)为“cameraman”明文图像的对角方向相关分析图。图 10(a)为“cameraman”密文图像的水平方向相关分析图，图 10(b)为“cameraman”密文图像的垂直方向相关分析图，图 10(c)为“cameraman”密文图像的对角方向相关分析图。可以看出明文图像的相邻像素间在 3 个方向上具有很强的线性关系，而密文图像的相邻像素间在 3 个方向上呈现随机的对应关系，表明图像加密效果好、安全性高。

为进一步量化数字图像相邻像素间在 3 个方向上的线性相关性，可利用相关系数公式来计算图像相邻像素间的相关系数值，利用相关系数的计算公式[23]如式(10)，可得原图像和加密图像的相邻元素的相关系数，如表 2 所列。

$$xc=\frac{n\sum_{i=1}^{n}x_i y_i-\sum_{i=1}^{n}x_i\sum_{i=1}^{n}y_i}{\sqrt{n\sum_{i=1}^{n}x_i^2-(\sum_{i=1}^{n}x_i)^2}\sqrt{n\sum_{i=1}^{n}y_i^2-(\sum_{i=1}^{n}y_i)^2}} \tag{10}$$

其中，x_i，y_i 分别表示相邻两个像素的灰度值，n 表示选取的像素对的个数。由表 2 也可以看出原始图像 3 个方向的相邻像素间有很强的相关性，而加密图像各方向相邻像素间相关性大大减弱。

表 2　原图像和加密图像的相邻元素的相关系数

图像	水平方向	垂直方向	对角方向
“rice”的明文图像	0.9427	0.9263	0.8994
“rice”的密文图像	0.000655	0.0074	−0.0053
“cameraman”的明文图像	0.9588	0.9360	0.9095
“cameraman”的密文图像	0.0052	−0.0077	−0.0053
“pout”的明文图像	0.9820	0.9783	0.9716
“pout”的密文图像	−0.0087	0.0142	0.0098
“pepper”的明文图像	0.9894	0.9931	0.9847
“pepper”的密文图像	−0.0140	−0.0184	−0.0137

5.3.3　密文图像信息熵分析

图像信息熵是度量图像信息量大小的概念，图像越混乱，图像信息熵越大，图像提供的信息就越小。信息熵的计算公式为 $H=-\sum_{i=1}^{n}p_i\log2(p_i)$，其中 p_i 为第 i 阶灰度值出现的概率。当密文的概率分布为等概率分布时，即取[0,255]之间每一个值概率均为 1/256 时，具有最大熵为 8bit。本文加密的“rice”、“cameraman”、“pout”、“pepper” 4 幅数字图像的信息熵如表 3 第 2 列所列，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随机性、不可预测性很高。

表 3　加密图像的信息熵和加密后的峰值信噪比

图像	加密后的信息熵	加密后的峰值信噪比
rice	7.9891	8.3267
cameraman	7.9889	8.9786
pout	7.9884	8.3465
pepper	7.9911	8.6657

5.3.4　峰值信噪比分析

峰值信噪比(PSNR)是描述图像加密质量的一个参数，它是在图像的平均平方误差(MSE)这一概念的基础上定义的。平均平方误差(MSE)的公式定义为[24]：

$$MSE=\{\frac{1}{M_1\times M_2}\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}(I_0(i,j)-I_e(i,j))^2\}^{\frac{1}{2}}$$

其中，$I_0(i,j)$是明文图像的像素值，$I_e(i,j)$ 是密文图像的像素值。M_1 是图像的行数，M_2 是图像的列数。峰值信噪比(PSNR)的公式定义为[19] $PSNR=20\log(\frac{I_{\max}}{MSE})$，其中 $I_{\max}$ 是图像的最大像素值，对于灰度图像为 255。显然 PSNR 的值越小，对应的明文图像和密文的差别越大，加密效果越好。本实验中计算“rice”、“cameraman”、“pout”、“pepper” 4 幅数字图像的峰值信噪比如表 3 第 3 列所列，可以看出密文图像的峰值信噪比都较低，表明加密效果良好。

5.4　抵抗已知明文攻击和选择明文攻击

在加密过程中，从式(8)－式(10)可以看出最终的加密密钥为 $\mathrm{mod}(S_1+P_0,256)$、$\mathrm{mod}(S_i+P_{i-1},256)$、$\mathrm{bitxor}(\mathrm{mod}(P_{m*n}+t_1,256),t_1)$、$\mathrm{bitxor}(\mathrm{mod}(C_{i-1}+t_i,256),t_{i-1})$。这里的 S_i，t_i 是混沌系统(1)产生的，它与混沌的初值有关，而 p_i 是一轮加密后的密文像素值，c_i 为最终密文像素值。因此，最终的加密钥匙不仅取决于初始状态值的混沌系统，也与明文图像、密文图像有关。当不同的明文图像加密后，相应的密钥流是不一样的。由于所得到的信息是与所选择的图像相关的，攻击者无法通过加密一些特殊的图像来获得有用的信息，因此该加密方案能抵抗已知明文攻击和选择明文攻击。

5.5　加密速度分析

当满足安全要求时，运行速度成为实际应用的一个重要因素，在提出的算法中只有两轮扩散操作，没有像素的置乱过程，这与图像传统的基于置乱-扩散结构的加密算法相比节省了很多时间，另外两轮扩散操作中只有取模运算和位异或两种算子，运算速度较快。在密钥流生成阶段只包括余弦函数运算和取模运算，运算速度也较快。实验在硬件环境为 Intel Celeron 2.13GHz CPU、2GB 内存和 250GB 硬盘的个人计算机及软件环境为 Windows XP、Matlab2012a 编译器的平台上进行，本文算法在上述计算机系统环境下对一幅 256×256 的 8 位灰度图像“cameraman”经两轮像素替代加密，耗时约 0.0456s，而密钥流的生成时间为 0.0522s。文献[25]的算法包括像素的置乱和一轮扩散操作，而用文献[25]提出的加密算法加密同一幅图像，耗时约 0.1435s，由此可见本文提出的算法节省了许多时间，而图像的置乱过程是很耗时的。

结束语　本文结合 Logistic 映射和三维离散 Lorenz 映射，构造了一个新的五维离散混沌映射，在此基础上提出了一种只有两轮扩散操作的图像加密算法，由于只有两轮扩散操作，加密速度较快。首先算法中的最终加密密钥与明文相关，而且密文与明文、密钥之间的关系复杂，因此算法能抵抗选择明(密)文的攻击；其次为了克服由于计算机精度的限制，混沌

序列在迭代过程中必将退化为周期序列的缺陷，本算法将多个混沌序列进行一个非线性函数运算，以得到周期更长的序列，这个阶段只包括余弦函数运算和取模运算，算法简单、速度较快；最后实验结果和安全性分析表明：该算法具有密钥空间大、加密图像像素分布性均匀、密文相邻像素的相关性极低、密文图像的信息熵接近 8bit、峰值信噪比小、密文对明文和密钥非常敏感、抵抗选择明(密)文的攻击、加密速度快等优点。因此，本文算法在图像保密通信和存储应用中将具有良好的应用前景。

参 考 文 献

[1] Liu W B, Chen G R. A three-dimensional smooth autonomous quadratic Chaotic system generate a single four-scroll attractor [J]. Int. J. Bifurc. Chaos, 2004, 14: 1395-1403

[2] Li C B, Sprott J C. Multistability in a butterfly flow[J]. Int. J. Bifurc. Chaos, 2013, 23: 1350199-1350209

[3] 官国荣，吴成茂，贾倩. 一种改进高性能 Lorenz 混沌系统构造及其应用[J]. 物理学报，2015，64(2)：31-44

[4] 朱淑芹，杨淼，张先华，等. 利用 Silnikov 定理构造混沌系统[J]. 北京科技大学学报，2005，27(5)：635-637

[5] Chen G, Ueta T. Yet another chaotic attractor[J]. Int J Bifurcation Chaos, 1999, 9(7): 1465-1466

[6] Lu J, Chen G. A new chaotic attractor coined[J]. Int J Bifurcation Chaos, 2002, 12(3): 659-661

[7] Čelikovsky′ S, Chen G. On a generalized Lorenz canonical form of chaotic systems[J]. Int J Bifurcation Chaos, 2002, 12(8): 1789-1812

[8] Lu J, Chen G, Cheng D, et al. Bridge the gap between the Lorenz system and the Chen system[J]. Int J Bifurcation Chaos, 2002, 12(12): 2917-2926

[9] Gao T, Chen Z, Yuan Z, et al. A hyperchaos generated from Chen's system[J]. Int J Mod Phys C, 2006, 17(4): 471-478

[10] Li Y, Tang W K S, Chen G. Hyperchaos evolved from the generalized Lorenz equation[J]. Int J Circ Theory, 2005, 33(4): 235-251

[11] Chen A, Lu J, Lu J, et al. Generating hyperchaotic Lu attractor via state feedback control[J]. Physica A, 2006, 364: 103-110

[12] Wang G, Zhang X, Zhen Y, et al. A new modified hyperchaotic Lu system[J]. Physica A, 2006, 371(2): 260-272

[13] Li Y, Chen G, Tang WKS. Controlling a unified chaotic system to hyperchaotic[J]. IEEE Trans Circuits Syst II, 2005, 52(4): 204-207

[14] 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

[15] 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器[J]. 华中科技大学学报(自然科学版)，2013，41(8)：16-19

[16] DraganLambi′c. A new discrete chaotic map based on the composition of permutations[J]. Chaos, Solitons and Fractals, 2015, 78: 245-248

[17] Wang Yong, Wong K W, Liao Xiao-feng, et al. A new chaos-based fast image encryption algorithm[J]. Applied Soft Computing, 2011, 11(11): 514-522

[18] Ye Rui-song. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism[J]. Optics Communications, 2011, 284: 5290-5298

[19] Zhang Guo-ji, Liu Qing. A novel image encryption method based on total shuffling scheme[J]. Optics Communications, 2011, 284: 2775-2780

[20] Rudin L, Osher S, Fatemi E. Nonlinear total variation based on noise removal algorithms[J]. Physica D, 1992, 60: 259-268

[21] Sprott J C. Chaos and time-series analysis[M]. Oxford: Oxford University Press, 2003: 513

[22] 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

[23] 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

[24] Rodriguez J. Computational Cryptography based on trigonometric algorithms and intensity superposition[J]. The Imaging Science Journal, 2010, 58(1): 61-80

[25] 卢辉斌，孙艳. 基于新的超混沌系统的图像加密方案[J]. 计算机科学，2011，38(6)：49-52

(上接第 406 页)

的计算速度不够快、抗攻击性不够高的困难。因此，本文方法适合如气象等收集大量图片资料的领域，也可以应用于灰度和普通彩色图像加密，并且在其它重要的图像信息保密领域也具有巨大的应用潜力。

参 考 文 献

[1] Wang X Y, Teng L, Qin X. A novel colour image encryption algorithm based on chaos [J]. Signal Processing, 2012, 92(4): 1101-1108

[2] Liu H J, Wang X Y. Colour image encryption based on one-time keys and robust chaotic maps [J]. Computers & Mathematics with Applications, 2010, 59(10): 3320-3327

[3] Rhouma R, Soumaya M, Salya B. OCML-based colour image encryption [J]. Chaos, Solitons & Fractals, 2009, 40(1): 309-318

[4] Chai Xiu-li, Gan Zhi-hua. Self-adaptive Bit level Colour Image Encryption Algorithm Based on Spatiotemporal Chaotic System [J]. Computer Science, 2015, 42(7): 204-208

[5] Wolf A, Swift J B. H L Swinney and JA Vastano. Determining Lyapunov' exponents from a time series[J]. Physic, 1985, 16D: 285-317

[6] 罗利军，李银山，李形，等. 李雅普诺夫指数谱的研究与仿真[J]. 计算机仿真，2005，22(12)：285-288

[7] 李银山，李欣业，刘波. 分岔混沌非线性振动及其在工程中的应用[J]. 河北工业大学学报，2004，32(3)：80-83

[8] 李水根，吴纪桃. 分形与小波[M]. 北京：科学出版社，2002

[9] Savi M A. Effects of randomness on chaos and order of coupled logistic maps[R]. Physics Letters A, In Press, Corrected Proof, 2006