文章编号: 1001- 2486(2009) 02- 0094- 05

二维混沌置乱矩阵构成置换群的理论和实验证明*

丁文霞, 王 浩, 卢焕章
(国防科技大学 电子科学与工程学院, 湖南 长沙 410073)

摘 要: 群论是研究对称性问题的强有力的数学工具。混沌指的是确定性非线性动力系统表现出来的内在随机性, 具有有界、非周期、对初始条件和参数极度敏感等特点, 由其产生的离散序列可用来对数字图像等数据进行加密。目前已有的文献中对二者之间的关联现象鲜有研究。基于群和混沌的基本理论, 结合置换群的概念, 从理论和实验两方面证明了二维混沌置乱矩阵对置换变换构成置换群的结论, 并由此指明了试图用不同初值, 经不同混沌系统产生多个混沌二维置乱矩阵对数字图像、视频等多媒体数据进行多重置乱加密以加强安全性的做法的无效性。

关键词: 混沌; 群; 置换群; 多重加密; 密码学
中图分类号: TP273 文献标识码: A

Theoretical and Experimental Proof That 2D Chaotic Arrays Are Permutation Groups

DING Wen-xia, WANG Hao, LU Huan-zhang
(College of Electronic Science and Engineering, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: Group theory is a sort of strong mathematics tool for the researches of the symmetry property. Chaos is the internal randomicity put up by the definite non-linear dynamical system. It has several properties, including the limitary, the nonperiodic and the dependence on initial condition and parameters. The discrete sequences produced by chaos system are often used to encrypt data such as digital pictures. In former papers, the relationship of Group theory and Chaotic system has seldom been studied. In this paper, it proves the result that the scrambling transform of two-dimensional chaotic scrambling arrays will form permutation groups. It is proposed on the basic theory of Group and Chaos and is proved in theoretical and experiment ways. According to the result, it is demonstrated invalid to use two-dimensional chaotic scrambling arrays created by different chaotic system and different initial values to encrypt multimedia data such as digital images and videos.

Key words: chaos; group; permutation group; multiple encryption; cryptography

目前, 利用混沌映射生成随机无序的一维序列或二维矩阵对数字图像等数据进行位置置乱的加密方式得到了广泛研究[1-6]。尽管李树钧等指出该类算法从严格的密码学意义上来讲都是不够安全的[7-8], 因为它们都不能从本质上抵抗已知明文攻击和选择明文攻击, 只需要一个明密文图像对即可有效地破解出等效密钥, 但由于混沌系统具有良好的非线性、随机性和初值敏感性, 此类算法还是得到了大多数研究人员的认可, 并被广泛应用于数字图像等数据加密的预处理过程中。

群论[9-10]是研究对称性问题的强有力的数学工具。自 19 世纪 Galoise 创立以来, 群论不仅成为近代数学的重要分支, 而且其应用范围已深入到科学技术的各个领域; 混沌现象是非线性动力系统中出现的确定性的、类似随机的过程, 这种过程既非周期又不收敛, 并且对初始值有极其敏感的依赖性[1]; 混沌与群之间存在着密切关系, 如文献[11]给出了混沌二值密钥对异或运算构成群的理论和实验证明, 文献[3]中提及了混沌无重复随机排列序列为置换群的结论, 然而目前对二者关系的研究总体上仍是非常有限的。

本文在上述研究的基础上, 首先从群的基本定义出发, 结合置换群的概念, 给出了二维混沌置乱矩

* 收稿日期: 2008- 08- 28
作者简介: 丁文霞(1973—), 女, 副教授, 在职博士生。

阵为置换群的相应的理论证明, 并用实验进行了验证, 随后将此结论应用于数字图像加密, 得出如下结论: 试图用不同初值, 经不同混沌系统产生多个混沌二维置乱矩阵对数字图像等数据进行单纯多重加密以加强安全性的做法将是无效的。

1 混沌系统的特性及二维混沌置乱矩阵设计

1.1 混沌系统的特性

简而言之, 混沌指的是由确定性非线性动力系统所表现出来的内在随机性, 具有如下一些特性[1]:

(1) 长期运动对初值的极端敏感依赖性, 即长期运动的不可预测性;

(2) 运动轨迹的无规则性: 相空间中的轨迹具有复杂、扭曲、缠绕的几何结构;

(3) 是一种有限范围的运动, 在相空间有受约束的轨道;

(4) 具有正的 Lyapunov 指数, 有限的 Kohnogorov-sinai 熵和连续功率谱;

(5) 具有分数维的奇异点集, 对耗散系统有分数维的奇异吸引子出现, 对于保守系统亦有奇异的混沌区。

目前在保密通信方面研究较多的混沌动力学系统包括一维 Logistic 映射、k 阶 Chebyshev 映射、线性分段函数(PLCM)映射、Hénon 混沌映射、Lorenz 混沌系统和陈氏混沌系统等等。其中, 一维 Logistic 映射和 k 阶 Chebyshev 映射的数学定义如下:

(1) Logistic 映射方程定义为

$$x_{n+1} = rx_n(1 - x_n), \quad 0 \leqslant r \leqslant 4, x_n \in (0, 1) \tag{1}$$

其中, r 为分支参数, 当 $0 \leqslant r \leqslant 3.569945972$ 时, 该动力系统因从稳定状态到分叉而产生倍周期, 当 $3.569945972 < r \leqslant 4$ 时, 该动力系统进入混沌状态。

(2) k 阶 Chebyshev 映射定义式为

$$x_{n+1} = \cos(k(\arccos x_n)), \quad x_n \in (-1, 1) \tag{2}$$

其中, k 为自然数, 当 $k \geqslant 2$ 时, 系统为混沌的。

文献[1, 3]等的研究指出, 由于 Logistic 和 Chebyshev 映射生成的混沌序列具有遍历性, 同时它们还具有 δ-like 型自相关函数和零的互相关函数, 并且具有初值敏感性, 因而可以提供数量众多、非相关、类随机而又可确定可再生的混沌序列, 其非常大的周期性和优良的随机性, 不仅非常适合产生符合安全要求的序列密码, 而且可以提供数量众多的密钥, 因而可以很好地被应用于各种混沌保密通信系统中。

1.2 二维混沌置乱矩阵设计

本文分别采用 Logistic 映射(式(1))和 Chebyshev 映射(式(2))来生成混沌置乱矩阵的行列坐标, 大小为 $N \times N$(如 128×128), 具体作法是: 将初值 x_0 带入 Logistic 映射, 舍弃起始段数据(如前 200 个数值), 从中段取出 N 个不重复的实数值(重复数值舍弃), 将其按升序或降序排列, 对应的序号即为混沌置乱矩阵的行坐标; 将同一初值 x_0 带入 k 阶 Chebyshev 映射, 按上述方法生成混沌置乱矩阵的列坐标, 行列坐标是无序和不重复的 1~ N 之间的整数。由混沌系统的初值敏感性知, 对应不同的初值 x_0, 可以生成不同的二维混沌置乱矩阵。需特别指出的是, 之所以将同一初值带入这两个映射, 并不是出于节省密钥空间的考虑, 而是利用二者在表达式结构上较大的相异程度来克服一维混沌动力系统中广泛存在的平凡密钥和拟平凡密钥现象[5], 以得到高质量的置乱矩阵。

2 二维混沌置乱矩阵构成置换群的理论证明

文献[9]中给出了详细严格的群和置换的定义, 介绍如下。

2.1 群的基本定义

数学上抽象群的定义极其严格, 指在抽象集合(有限或无限个元素) $W = \{A, B, C, \ldots\}$ 中各元素之间建立一种运算关系, 通常称为"乘法", 将 2 元素复合为第 3 个元素: $AB = D$, 若集合 W 的全部元素在

上述群运算(乘法)下满足如下4个公理,则构成一个群。

(1)封闭性:对$\forall A, B \in W$,有$AB = C \in W$;

(2)存在单位元:即$\exists E \in W$,满足对$\forall A \in W$,有$AE = EA = A$,元素E称为单位元;

(3)存在逆元:对$\forall A \in W$,均存在元素B,使得$AB = BA = E$,B称为A的逆元素,记为A^{-1}。显然,A亦为B的逆元;

(4)结合律:对$\forall A, B, C \in W$,群运算满足$(AB)C = A(BC)$。

另外,群元素的个数称为群的阶,根据群的阶可将群分为有限群和无限群。对群运算(乘法)而言,一般$AB \neq BA$,若群元素乘法满足$(\forall A, B \in W)AB = BA$,则该群为阿贝尔群。

2.2 置换的定义

设有$1, 2, \cdots, n$,n个编号的对象r_i与s_i($i = 1, \cdots, n$),均是编号$1, 2, \cdots, n$的排列,则称

$$P = \begin{bmatrix} r_1 & r_2 & \cdots & r_n \\ s_1 & s_2 & \cdots & s_n \end{bmatrix} \tag{3}$$

为一个置换。由置换的定义显见,这种记号显然与列的编序无关,因此总可以通过适当调整列的排序,将(3)式中的2个排列等价地表示为:

$$R = \begin{bmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{bmatrix}, \quad Q = \begin{bmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{bmatrix} \tag{4}$$

两个置换R与Q的连续置换QR,定义为置换的乘积,亦即第l个对象经过R置换为i_l,再经过Q置换到j_l。

2.3 二维混沌置乱矩阵对置换变换构成置换群的理论证明

置换群又称对称群,不仅被广泛应用于量子理论中多粒子体系的研究,而且也是研究其它群的有力工具。下面首先证明n个对象所有置换操作的集合在置换"乘积"定义下构成群,称为置换群,记为S_n,显然$S_n \subseteq I_n$。

证明 (1)对于如(4)式定义的任意两个置换$R \in S_n$,$Q \in S_n$,其连续置换

$$\begin{aligned} QR &= \begin{bmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{bmatrix} \begin{bmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{bmatrix} \\ &\equiv \begin{bmatrix} i_1 & i_2 & \cdots & i_n \\ k_1 & k_2 & \cdots & k_n \end{bmatrix} \begin{bmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{bmatrix} \in S_n \end{aligned} \tag{5}$$

记$QR = P$,则$P \in S_n$,所以封闭性成立。

(2)易知,置换中的恒等变换即不变序号

$$I = \begin{bmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{bmatrix} \tag{6}$$

显然$I \in S_n$,且对$\forall R \in S_n$,$RI = IR = R$,即单位元E存在,且$E = I$。

(3)对$\forall R \in S_n$,令将R中上、下两行交换的变换为R^{-1},显然$R^{-1} \in S_n$,且

$$R^{-1}R = \begin{bmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{bmatrix} \begin{bmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{bmatrix} = \begin{bmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{bmatrix} = RR^{-1} = I \tag{7}$$

即S_n中任意元素均存在逆元素。

(4)又设$\forall R, P, Q \in S_n$,由于R, P, Q都是n个元素的置换变换,它们一经确定,置换关系即唯一对应,所有三者之间的连续置换与先后次序无关,也即有$(RP)Q = R(PQ)$成立,即结合律成立。

综上所证,S_n确实在置换"乘积"定义下构成群,称为置换群,若$n = N$,则S_N为一有限群,其阶

$n(S_N)=N!$。证毕。

下面将此结论拓展到二维空间, 以二维混沌置乱矩阵为例证明所有二维矩阵置换操作的集合在"乘积"定义下亦构成置换群。

易知, 1.2 节中设计的任意 $N\times N$ 大小的混沌置乱矩阵均可以表示成式(3)所示的形式, 其中$\{r_1, r_2, \cdots, r_N\}$为行地址排列, $\{s_1, s_2, \cdots, s_N\}$为列地址排列, 且令所有行列地址排列变换的集合为 W, 则 $W\subseteq I_{N\times N}$。若 $A, B, C\in W$, 则由(4)式可知, A 可等价地表示成如下形式:

$$R_A=\begin{bmatrix}1 & 2 & \cdots & N\\ i_{A1} & i_{A2} & \cdots & i_{AN}\end{bmatrix},\quad Q_A=\begin{bmatrix}1 & 2 & \cdots & N\\ j_{A1} & j_{A2} & \cdots & j_{AN}\end{bmatrix}\quad R_A, Q_A\in S_N \tag{8}$$

即 $A\leftarrow\!\!\!\shortmid(R_A, Q_A)$, 同理, $B\leftarrow\!\!\!\shortmid(R_B, Q_B)$, $C\leftarrow\!\!\!\shortmid(R_C, Q_C)$。

(1)封闭性。即对任意 $A, B\in W$, 若 $AB=D$, 必有 $D\in W$。

证明　对 $\forall A, B\in W$, 其连续置换 $AB\leftarrow\!\!\!\shortmid(R_{AB}, Q_{AB})$, 由(8)式定义和 S_N 的置换群特性知定义 $R_{AB}=R_BR_A$, $Q_{AB}=Q_BQ_A$ 成立, 则由 S_N 的封闭性知 $R_{AB}, Q_{AB}\in S_N$, 又 $AB=D$, 即可令 $R_D=R_{AB}\in S_N$, $Q_D=Q_{AB}\in S_N$, 则 $D\leftarrow\!\!\!\shortmid(R_D, Q_D)\in W$。

(2)存在单位元素。即有 $E\in W$, 对任意 $A\in W$, 都有 $AE=EA=A$。

证明　由 $R_AI=IR_A=R_A$, $Q_AI=IQ_A=Q_A$(I 的定义如式(6))知, W 中存在单位元素 $E\leftarrow\!\!\!\shortmid(I, I)$, 使得 $AE\leftarrow\!\!\!\shortmid(R_AI, Q_AI)=(R_A, Q_A)\leftarrow\!\!\!\shortmid A$, 即 $AE=A$, 同理, $EA=A$。

(3)存在逆元。即对任意 $A\in W$, 存在 $A^{-1}\in W$, 使 $A^{-1}A=AA^{-1}=E$。

证明　A^{-1}即 A 中上、下两行交换的变换, 易知, $A^{-1}\leftarrow\!\!\!\shortmid(R_A^{-1}, Q_A^{-1})\in W$, 其中 R_A^{-1} 即 R_A 中上、下两行交换的变换, Q_A^{-1} 即 Q_A 中上、下两行交换的变换, 由 S_N 的置换群特性知: $R_A^{-1}R_A=I$, $Q_A^{-1}Q_A=I$。则 $A^{-1}A\leftarrow\!\!\!\shortmid(R_{A^{-1}A}, Q_{A^{-1}A})=(R_A^{-1}R_A, Q_A^{-1}Q_A)=(I, I)\leftarrow\!\!\!\shortmid E$, 即 $A^{-1}A=E$, 同理, $AA^{-1}=E$。

(4)结合律。即对 $\forall A, B, C\in W$, 满足 $(AB)C=A(BC)$。

证明　由 S_N 的结合律易证:

$$\begin{aligned}&(AB)C\leftarrow\!\!\!\shortmid(R_{(AB)C}, Q_{(AB)C})=(R_CR_{(AB)}, Q_CQ_{(AB)})=(R_CR_BR_A, Q_CQ_BQ_A)\\&=((R_CR_B)R_A, (Q_CQ_B)Q_A)=(R_{(BC)}R_A, Q_{(BC)}Q_A)=(R_{A(BC)}, Q_{A(BC)}))\leftarrow\!\!\!\shortmid(BC)\end{aligned} \tag{9}$$

即对 $\forall A, B, C\in W$, $(AB)C=A(BC)$ 成立。

综上所证, W 为一个置换群, 且为有限群, 其阶 $n(W)=(N\times N)!$。由此可知, 作为 W 的一个特例, 所有 $N\times N$ 二维混沌置乱矩阵组成的集合对置换操作亦构成置换群, 其阶亦为 $(N\times N)!$。证毕。

3　实验验证结果及分析

现行应用密码学的一个流行思路是在不设计新算法的情况下增加分组密码算法的强度[12]。实现这种想法的有效方法之一是加长密钥; 另一种作法是进行多重加密, 即用同一个算法在多重密钥的作用下多次加密同一个明文分组。实行多重加密的首要前提是所选的分组密码算法不是一个群, 否则多重加密是无效的[12]。以三重加密为例, 设三重密钥分别为 $K1$、$K2$、$K3$, 若所选的分组密码算法是一个群, 那么总会存在一个 $K4$, 使得

$$C=E_{K3}(E_{K2}(E_{K1}(P)))=E_{K4}(P) \tag{10}$$

其中, P 为要加密的明文, C 为加密后的密文, $E_{Ki}(i=1, 2, 3, 4)$ 为不同密钥作用的同一加密算法。

在第 2 节中我们已经证明 $N\times N$ 大小的混沌置乱矩阵对置乱变换构成置换群, 所以当我们用混沌置换矩阵作为密钥对二维图像等数据进行单纯的位置置乱加密时, 使用多重加密将是无效的。对此, 我们也通过实验进行了验证。图 1 中, 分别对两幅图像("F14.bmp"和"peppers.bmp")按由不同密钥随机生成的二维混沌置乱矩阵的对应关系分别进行了 1 次、3 次和 5 次置乱加密, 图 1(a1)、(a2)、(a3)分别为对原图 1(a)进行单重、三重、五重加密后的效果图, 图 1(b1)、(b2)、(b3)分别为对原图(b)进行单重、三重、五重加密的效果图。由主观感觉来看, 这种加密算法并未因加密次数的增多而达到更好的效果。同时,

表 1 列出了 2 幅图像在不同加密次数下对应的加密图与原图相同点的个数(N)和相关系数(NC)的 20 次实验的平均值,这些数值也表明图像并未因为置乱次数的增多而达到更好的随机性(或不相关性)。这些均有力地证明了二维混沌置乱矩阵对置换变换构成了置换群。

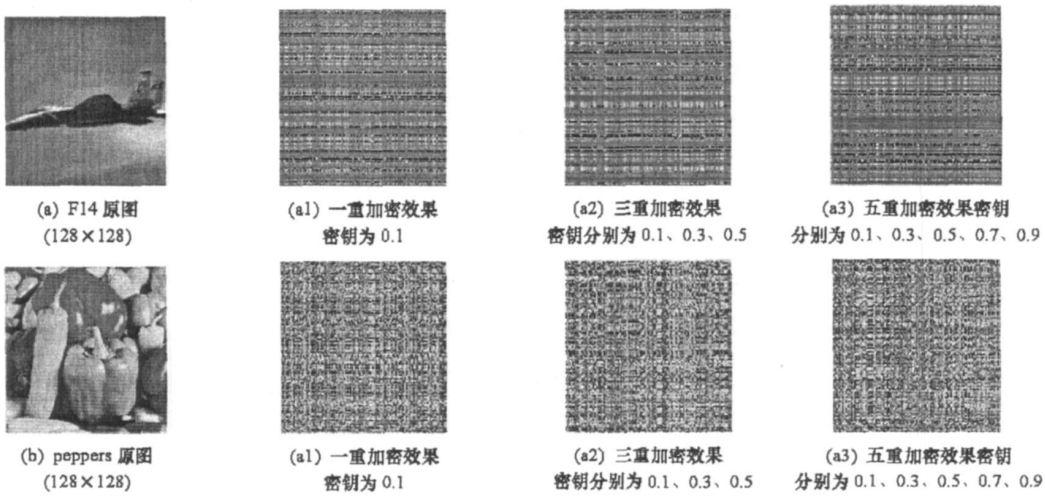

图 1 用混沌二维矩阵对数字图像进行单重及多重简单置乱加密的对比效果图

Fig. 1 The contrast effect figures of single and multiple permutation encryption for digital images with 2D chaotic matrix

表 1 混沌置乱矩阵不同置乱次数下的加密性能分析(20 次实验的平均值)

Tab. 1 The performance analysis of encryption with chaotic permutation matrix under different permutation times (20 times average)

次数	加密图与原图相同点的个数(N)		加密图与原图的相关系数(NC)	
	F14	peppers	F14	peppers
$n=1$	288	99	0.9084	0.8156
$n=3$	286	97	0.9067	0.8171
$n=5$	276	96	0.9064	0.8190

4 结束语

应用密码学[12]指出:在讨论算法设计时,有一个问题是值得考虑的,即该算法是否构成一个群,其中,群的元素是每一个可能密钥的密文分组,群的运算是合成。考察算法群结构的目的是掌握在多重加密的情况下会有多少额外的混乱发生,若该算法构成一个群,则用其进行多次加密以提高安全性将是无意义的。本文从理论和实验角度证明了二维混沌置乱矩阵对置乱变换构成置换群的结论,由于现有基于混沌系统设计的许多加密算法中均含有"置乱"变换,若算法设计时不采用其它方法(如扩散等)来破坏其群特性,则设计的算法亦会构成群,因而,此结论对此类基于混沌系统的加密算法设计提供了非常重要的理论参考。

参考文献:

[1] 陈关荣,江小帆. 动力系统的混沌化——理论、方法和应用[M]. 上海:上海交通大学出版社,2006.
[2] 秦红磊,郝燕玲,孙枫. 一种基于混沌的图像置乱网络的设计[J]. 计算机工程与应用,2002,38(7):104-106.
[3] 孙鑫,易开祥,孙优贤. 基于混沌系统的图像加密算法[J]. 计算机辅助设计与图形学学报,2002,14(2):136-139.
[4] 刘云江,刘向东,王光兴. 一类改进型基于混沌的图像置乱网络设计[J]. 中国图象图形学报,2004,9(3):360-364.
[5] 范延军,孙燮华,阎晓东,等. 一种基于混合混沌序列的图像置乱加密算法[J]. 中国图象图形学报,2006,11(3):387-393.
[6] 田岩,谢玉波,李涛,等. 一种基于分块和混沌网的图像置乱方法[J]. 中国图象图形学报,2007,12(1):56-60.
[7] Li S, Mou X, Cai Y, et al. On the Security of a Chaotic Encryption Scheme: Problems with Computerized Chaos in Finite Computing Precision [C]// Computer Physics Communications, 2003, 153: 52-58.
[8] 李树钧,牟轩沁,纪震,等. 一类混沌流密码的分析[J]. 电子与信息学报,2003,25(4):473-478.
[9] 张端明,钟志成. 应用群论导引[M]. 武汉:华中科技大学出版社,2005.
[10] 孟道骥,朱萍. 有限群表示论[M]. 北京:科学出版社,2006.
[11] 丁文霞,卢焕章,谢剑斌. 混沌二值序列对异或运算构成群的理论和实验证明[J]. 系统工程与电子技术,2006,28(10):1420-1422.
[12] Bruce Schneiner(美). 应用密码学——协议、算法与 C 源程序[M]. 北京:机械工业出版社,2000.