基于复合混沌的自适应图像加密算法

车生兵 黄 达 李 光
(中南林业科技大学电子与信息工程学院,长沙 410004)

摘 要 复合混沌迭代系统保持了所有迭代子系统的混沌特性,比单个子系统的动力学行为复杂得多,其生成的密钥串按二进制位独立同分布。为了更好地进行图像加密,提出了一种基于复合混沌的自适应图像加密算法。该算法是利用密钥串的值,结合图像像素值确定的置乱顺序对图像进行加密。实验表明,用该算法可以达到很好的自适应加密效果。当总密钥长度大于 128bits 时,该系统是很难破解的。

关键词 图像置乱 复合离散混沌迭代系统 遍历 自适应
中图法分类号: TP309 **文献标识码**: A **文章编号**: 1006-8961(2006)11-1557-05

An Adaptive Image Encryption Algorithm Based on Composite Discrete Chaotic System

CHE Sheng-bing, HUANG Da, LI Guang
(*College of Electron & Information, Central South University of Forestry & Technology, Changsha* 410004)

Abstract Composite discrete chaotic iterative system keeps all characteristics of each single chaotic iterative system and its dynamic behavior is more complicated. Because the key generated from composite discrete chaotic iterative system is independent identically distributed, encrypting the image by using the key and adaptive image scrambling algorithm can get a satisfied result. When the length of the entire key is more than 128 bits, the encryption system is robust under attack.

Keywords image scramble, composite discrete chaotic iteration system, ergodicity, adaptive

1 概 述

伴随着数字时代的到来,多媒体数据已逐渐成为人们获取信息的重要来源,并已成为人们生活的重要组成部分,但侵权现象也日益增多,因此版权保护也越来越重要。图像作为一种重要的信息载体,它的加密技术发展得非常快。如今,图像加密已成为多媒体信息安全的一个研究热点。

图像加密的思想通常分为以下 3 大类:位置置乱、数值转化和前面两类方法的结合形式。其中,位置置乱就是打乱了原数据的位置,将图像像素重新排列。通常,图像有大量的数据,由于简单地打乱就能使从加密图像中辨别原始图像变得非常困难,因而,图像置乱是一种简单快速的加密方法。常用的置乱方法虽有很多,但依据附加信息的置乱,在保密附加信息时需要另外考虑,使用起来不够方便,而仅利用图像本身所携带的信息,就可以进行置乱的自适应方法更加方便实用。但是,单纯地用置乱方法对图像进行加密能被统计分析的方法所破译[1,2]。如果置乱算法能够保证置乱规律是独立同分布的,那么,统计分析的攻击方法就失去了理论基础。

混沌系统是一种复杂的非线性动力学系统,由于混沌具有良好的伪随机特性、轨道的不可预测性以及对初始状态和控制参数极端敏感等特性,因此将混沌应用于图像加密已很多。但是,这些应用仍有一定的局限性,其中一点就是容易被破解,特别是抗统计分析的能力差[3,4]。单一的离散混沌迭代系

基金项目:国家自然科学基金项目(60373000)
收稿日期:2006-04-18;**改回日期**:2006-08-05

第一作者简介:车生兵(1970~),男,副教授。2005 年于长沙理工大学获计算机应用技术专业硕士学位。主要研究方向为人工智能、网络安全、数字图像处理。E-mail: cheshengbing727@tom.com

统,其动力学行为容易破译,而复合离散混沌迭代系统,由于其动力学行为与复合序列和各个混沌迭代子系统的动力学行为有关,因此其动力学行为更加复杂。如果能够找到在取值范围内迭代值均匀分布的混沌动力系统,那么要破译该混沌系统也就相当困难了。

综上所述,本文提出了一种结合复合混沌和图像置乱的自适应图像加密算法。本文以两个混沌函数组成的复合混沌迭代系统为例,首先通过一个 0,1 序列来分别选择两个函数做运算,使得置乱密钥串具有均匀的、独立同分布的特性,因而其抗统计分析的性能良好;然后结合图像置乱算法,根据图像一半像素值决定的置乱顺序来对图像的另一半像素进行加密。从实验结果来看,其性能指数及视觉效果均优于一般的图像加密技术。特别是,本系统对加密密钥组合十分敏感,且有 3 个加密参数可供选择,这也使得安全性得到大大提高。

2 复合离散混沌迭代系统

下面在(0,1)上首先构造两个特殊的函数,然后对其性质进行分析,并在(0,1)上定义函数 $f_q(x), q=0,1$

$$f_0(x) = \sqrt{|2x-1|} \tag{1}$$

$$f_1(x) = 1 - \sqrt{|2x-1|} \tag{2}$$

由此可以得到两个迭代函数,即 $x_{n+1}=f_q(x_n), q=0,1$。$f_q(x), q=0,1$ 这两个函数还分别对应着两个特殊的非线性离散混沌动力系统,其性质可由以下定理给予说明,证明过程略。

定理

(1) $x_{n+1}=f_q(x_n), q=0,1$ 是混沌迭代系统;

(2) 与该混沌迭代系统对应的不变分布密度函数(invariant distribution density,简称不变分布)分别是 $\rho_0(x)=2x, \rho_1(x)=2-2x$,在概率 $p(q=0)=p(q=1)0.5$ 时,$\rho_q(x)=1$;

(3) 若 $\rho_q(x)=1$,则通过定义转换算子 $R_j:[0,1]\to\{0,1\}$, $R_j(x)=\lfloor x\times 2^j\rfloor \bmod 2, j\in N$ 就可使得到的密钥串按二进制位独立同分布[5]。

大家知道混沌系统对初始值的敏感性,那么初始值 x_0 的微小改变也将使得最后的迭代结果不相同。假设复合离散混沌迭代系统的初始值分别为 $x_0=0.87654321$ 和 $x_1=0.87654322$,则经过 3 次迭代后的结果如表 1 所示。

表 1 复合混沌迭代结果

Tab. 1 Results of composite chaotic iteration

x_0	$x_1=f_1(x_0)$	$x_2=f_0(x_1)$	$x_3=f_1(x_2)$
0.876 543 21	0.132 194 480 3	0.857 677 701 4	0.154 213 145 8
0.876 543 22	0.132 194 468 8	0.857 677 714 8	0.154 213 129 9

将复合混沌应用于数据加密,其生成的置乱密钥串满足上述定理,而且非法攻击将无法通过分析置乱密钥串的统计规律来破解本文置乱算法的规律,从而使得统计分析攻击成为不可能,其安全性很高。

3 基于复合混沌的自适应加密算法

3.1 遍历及自适应置乱

从矩阵的某一个元素开始,可以沿某一特定的顺序依次访问各个元素,直至最后一个,这个特定的顺序即形成了一种遍历。常见的遍历顺序如图 1 所示。给定一个矩阵 M,就可以定义:根据 M 中元素值的大小对 M 进行遍历,这种按照访问顺序值得到的矩阵即为该矩阵的遍历矩阵,记作 E。显然,E 与 M 的元素是一一对应的,那么就可以根据 E 中的顺序,以按行遍历顺序来对待加密对象进行置乱。例如,如果按照 E 的顺序直接对 M 进行置乱,则得到的置乱矩阵 R 如图 2 所示。

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

(a)按行遍历

1	2	3	4	5
10	9	8	7	6
11	12	13	14	15
20	19	18	17	16
21	22	23	24	25

(b)"之"字形遍历

1	2	3	4	5
16	17	18	19	6
15	24	25	20	7
14	23	22	21	8
13	12	11	10	9

(c)螺旋式遍历

图 1 常见遍历顺序

Fig. 1 Usual order of ergodic

13	7	5	9
39	0	7	2

(a)原矩阵 M

6	3	2	5
8	1	4	7

(b)遍历矩阵 E

0	5	7	39
20	13	9	7

(c)置乱矩阵 R

图 2 求遍历矩阵和置乱矩阵

Fig. 2 Get the ergodic matrix and scramble matrix

同理,也可以用 E 对与 M 同维的矩阵进行置乱。如果把图像分割成若干大小相同的部分,先求

出其一半的遍历矩阵 E,再对另一半进行置乱,反之亦然,则可以演化出很多种置乱方法。由此可见,由于自适应的图像置乱不需要其他附加信息,只要利用本身所携带的信息就可以进行置乱,因此,不仅速度快,而且实现方便。

3.2　算法设计

利用复合离散混沌系统和自适应置乱算法各自的特点,将它们结合起来,本文提出如下加密算法。该算法由两大部分构成,其一是用复合混沌生成具有独立同分布特性的置乱密钥串;其二是根据置乱密钥串的 0,1 值采用置乱算法对图像进行加密。算法的整体流程如图 3 所示。

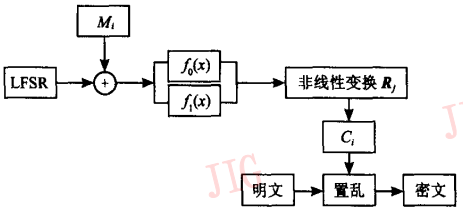


图 3　算法流程

Fig. 3　Flow chart of Algorithm

3.2.1　生成置乱密钥串

由于复合混沌迭代系统中的两个函数需要均匀的选取才能保证置乱密钥串的独立同分布特性。因此可以利用密码学里的线性反馈移位寄存器(linear feedback shift register, LFSR)来生成 0,1 均匀分布的序列串。用线性反馈移位寄存器生成的序列具有良好的伪随机性,在一个周期内,0 和 1 出现的次数接近相等。序列的最大周期为 2^{n-1},其中 n 为 LFSR 的二进制位数,可以用 8,16 或者 32bits。用户可以给定一个密钥,先将其转化为二进制串 $\boldsymbol{M}=\{M_i\}(i=1,2,\cdots,m)$,再用 M_i 与 LFSR 生成的 0,1 串进行逐位异或,即得到选择混沌子系统的控制串 $\boldsymbol{Q}=\{Q_i\}(i=1,2,\cdots,m)$。设复合混沌系统的初始迭代值为 x_0,进行第 1 次迭代时,若 $Q_i=0$,则 $x_1=f_0(x_0)$,若 $Q_i=1$,则 $x_1=f_1(x_0)$。同理,以后的迭代,可根据 Q_i 来选择 $x_{i+1}=f_0(x_i)$ 或 $x_{i+1}=f_1(x_i)$。得到的 x_i 经过一个非线性变换函数即可得到置乱密钥串 $\boldsymbol{C}=\{C_i\}(i=1,2,\cdots,m)$。给定变换算子 $\boldsymbol{R}_j$:$[0,1]\to\{0,1\}$,$R_j(x)=\lfloor x\times 2^j\rfloor \bmod 2$,$j\in N$。

3.2.2　自适应图像置乱

自适应图像置乱可先将矩阵分割成上下或左右对称的两部分。现以上下部分的分割方法为例来说明置乱的过程。

(1)先按矩阵元素大小求出上半部分的一个遍历矩阵,且遍历矩阵的每一元素与下半部分矩阵的元素是一一对应的;

(2)根据所求的遍历矩阵对下半部分矩阵按遍历矩阵确定的顺序进行置乱;

(3)用同样的方法重复步骤(1)和(2),对已置乱的下半部分再求遍历矩阵,再根据遍历矩阵对上半部分进行置乱。

这里用复合混沌系统生成的置乱密钥串来控制这个置乱过程。置乱密钥串 $\boldsymbol{C}$ 中的值,用 0 代表上下置乱,用 1 代表左右置乱,这样就可以根据 $\boldsymbol{C}_i$ 的值选择进行左右置乱还是上下置乱。依次迭代置乱直到 $\boldsymbol{C}$ 的最后一位。置乱流程如图 4 所示,图中 $\boldsymbol{C}=\{0111\cdots\}$。

解密的过程则是加密的逆过程。根据置乱密钥串 $\boldsymbol{C}$ 的值,反过来依次解密。以置乱密钥串 $\boldsymbol{C}=\{0111\}$ 为例,解密顺序 $\boldsymbol{C}_r=\{1110\}$(下角 r 代表 reverse),直到解密到 $\boldsymbol{C}_r$ 的最后一位。从上下置乱转换到左右置乱,本文采用了矩阵的转置操作再做上下置乱,并使得上下与左右置乱都只调用同一个模块,这就大大加快了算法的运算速度。

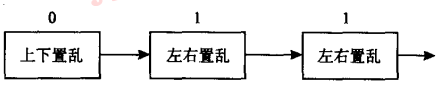


图 4　图像置乱过程

Fig. 4　Image scramble

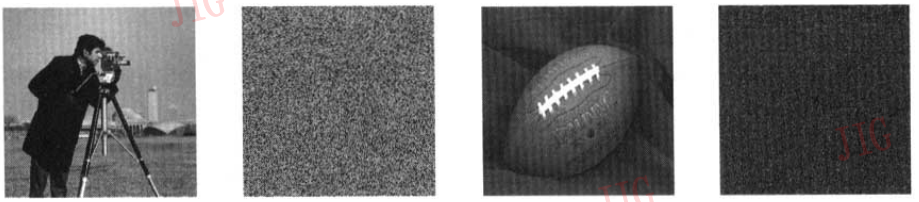
4　结果及结论

4.1　实验结果

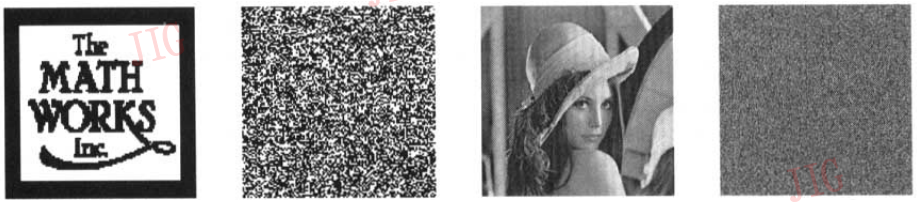
假定用户给定一个私有的加密密钥 $\boldsymbol{M}=$'zishiyingjiami',并先把每个字母转化为 ASCII 码,以得到一个 ASCII 码串:'122,105,115,104,105,121,105,110,103,106,105,97,109,105';然后将其转化为二进制串,联合起来就构成 $\boldsymbol{M}=\{M_i\}$。若 $\boldsymbol{M}$ 的二进制位数不够 128bits,则在后面用 0 和 1 均匀补齐,直到 128bits。设一个 8bits 的 LFSR 的初始值为 10101100,复合混沌系统中初始值 $x_0=0.87654321$,用其对图像进行加密,加密结果如图 5 所示。经过若干次迭代加密置乱,无论是二值图像

还是灰度图像或者 RGB 图像，其得到的结果都是均匀的，并且，已无法从置乱图像中辨认出原始图像的信息。

解密过程主要是先得到正确的加密密钥，然后用置乱的逆过程进行解密即可得明文。在得到加密密钥的过程中，M，x_0 及 LFSR 初始值的任意一个值的哪怕是微小的偏差，都将极大地影响解密的结果。例如，在得到 M 和 $x_0=0.87654321$ 情况下，如果取 LFSR 的初始值为 11101100，则图 5(b)和图 5(d)的错误解密图像如图 6(a)、图 6(b)所示。已知 M 和 LFSR 的初始值为 10101100 的情况下，如果取 $x_0=0.87654322$，那么，图 5(f)和图 5(h)的错误解密图像如图 6(c)、图 6(d)所示。从解密结果来看，哪怕加密参数中的任意一个，其值有一点微小的变化，即使已知本文算法，都无法正确解密还原正常图像。正确的解密结果和图 5 的原图一致。



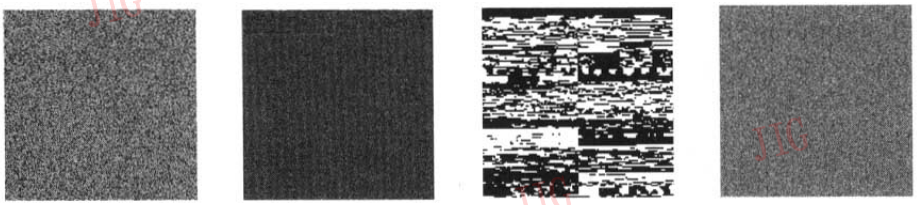
(a)原图 (b)图 5(a)加密图像 (c)原图 (d)图 5(c)加密图像



(e)原图 (f)图 5(e)加密图像 (g)原图 (h)图 5(g)加密图像

图 5 图像加密结果

Fig. 5 Results of image encryption



(a)图 5(a)的错解 (b)图 5(c)的错解 (c)图 5(e)的错解 (d)图 5(g)的错解

图 6 错误的解密图像

Fig. 6 Wrong results of decryption

4.2 结 论

通过大量实验证明，本文该算法具有速度快、加密效果好、安全性高的特点。混沌函数以及具体的置乱方法都有较大的可选择余地，可根据用户需要进行选定。一个好的密码体制在于即便知道算法，仍然难以在有限资源的情况下破解[6,7]。M，x_0 及 LFSR 的初始值，任意一个值的改变均会影响到加密结果，因而使得穷举攻击在实际上不能实现。加密系统对密钥非常敏感，在解密时，即使有细微的差别也将解密不出原始图像。

由于置乱密钥串是通过复合离散混沌动力系统生成的，因此具有独立同分布的特性。即使分析出 C 的统计特性也无法得到密文。如果以大于 128bits 的组合密钥对图像进行加密，尤其是对于信

息量大的图像,则在仅仅知道密文的情况下,攻击是很难的。即使在已知某一加密参数的情况下,也需要付出相当大的代价。当整个密钥组合的长度大于128bits时,就可以使生日攻击等非法操作成为不可能。

参考文献(References)

1 Qiao L T, Nahrstedt L. Camparison of MPEG encryption algorithms [J]. Computer & Graphics, 1998, **22**(4):437 ~ 448.

2 Chen G, Zhao X Y, Li J L. A self-adaptive algorithm on image encryption[J]. Journal of Software, 2005, **6**(11):562 ~ 568.

3 Yuan J. Developments and analysis of chaotic applications [J]. Journal of Nature (Science and Technology Developments), 2002, **17**(6):318 ~ 322.

4 Hu G J, Feng Z J. Security analysis of a kind of discrete chaotic encryption systems[J]. Journal of Electron and Information, 2003, **25**(11):1514 ~ 1518.

5 Li Hong-de, Feng Deng-guo. Composite nonlinear discrete chaotic dynamical systems and stream cipher systems[J]. Acta Electronica Sinica, 2003, **31**(8):1209 ~ 1212. [李红达,冯登国. 非线性离散混沌动力学系统[J]. 电子学报, 2003,**31**(8):1209 ~ 1212.]

6 Zhang Zhao-zhi. Foundations of cryptography[M]. Beijing: Beijing University of Posts and Telecommunications Press, 2004. [章照止. 现代密码学基础[M]. 北京:北京邮电大学出版社,2004.]

7 Zhang Huan-guo, Liu Yu-zheng. Introduction of cryptography[M]. Wuhan: Wuhan University Press, 2003. [张焕国,刘玉珍. 密码学引论[M]. 武汉:武汉大学出版社,2003.]