一种改进的 Arnold Cat 变换图像置乱算法

张 健[1],于晓洋[2],任洪娥[1]
ZHANG Jian[1],YU Xiao-yang[2],REN Hong-e[1]

1.东北林业大学 信息与计算机工程学院,哈尔滨 150040
2.哈尔滨理工大学 测控技术与通信工程学院,哈尔滨 150040
1.Information and Computer Engineering College,Northeast Forestry University,Harbin 150040,China
2.College of Measurement-Control Tech. & Comm. Engineering,Harbin University of Science and Technology,Harbin,150040,China
E-mail:zhangjianok00@163.com

ZHANG Jian,YU Xiao-yang,REN Hong-e.Improved image scrambling algorithm of Arnold Cat transformation.Computer Engineering and Applications,2009,45(35):14-17.

Abstract: Arnold Cat transformation is a classical algorithm of image scrambling.However,it has some disadvantages,such as small key quantities and not better visual effect.At the same time,it only changes the position of pixel point and the pixel value is fixed.So,the attacker may break down it through the statistics.Aimming at the disadvantages,an improved scrambling algorithmm of Arnold Cat transformation using chaotic map is put forward.The experiment results show that the key quantities and scrambling effect are improved obviously,and the security of image encryption is increased.

Key words: image scrambling;Arnold Cat transformation;chaotic map;even scrambling

摘 要: Arnold Cat 变换是经典的图像置乱算法,但其存在密钥量小,置乱视觉效果差的缺点。同时置乱仅仅是重新排列图像各像素点的位置,像素值并没有发生改变,这样攻击者就可以通过统计分析等手段进行破译。针对 Arnold Cat 变换的不足,运用混沌理论,提出了一种基于均匀性的改进 Arnold Cat 变换置乱算法。仿真实验证明改进的算法具有密钥量大、置乱视觉效果好、图像的位置和像素值均发生本质改变等优点,增加了图像加密的安全性。

关键词:图像置乱;Arnold Cat 变换;混沌映射;均匀置乱
DOI:10.3778/j.issn.1002-8331.2009.35.005 **文章编号:**1002-8331(2009)35-0014-04 **文献标识码:**A **中图分类号:**TP391

1 引言

随着网络与多媒体技术的飞速发展,数字图像正逐渐成为人们进行信息交流的重要载体。随着人们对信息安全性要求的提高,数字图像加密技术在多媒体通信中获得了广泛的应用[1]。经典的图像加密算法包括 Arnold Cat 变换[2]、面包师变换[3]、Hilbert 变换[4]和 Zigzag 变换[5]等,其中以 Arnold Cat 变换应用最为广泛,置乱效果相对最好,但 Arnold Cat 变换的密钥量较小、视觉效果还不够理想。同时,这些应用数学变换的图像加密算法都是从位置上进行置乱,图像的像素值并没有发生变化,即灰度直方图没有变化,这样攻击者就可以通过统计分析等手段进行破译。从图像置乱的实质出发,提出均匀置乱的概念,并结合 Lu 混沌映射,在 Arnold Cat 变换的基础上,提出一种图像置乱算法,通过实验来验证算法的可行性和有效性。

2 Arnold Cat 变换

Arnold Cat 变换,也叫猫脸变换,其表达式如(1)所示:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod(N) \quad (1)$$

式中:x_n,y_n是一个 $N\times N$ 图像的原始像素点位置,x_{n+1},y_{n+1}是置乱后的像素点位置,a 和 b 是系统的参数,取正整数。当 $a=1$,$b=1$ 时,是标准的 Arnold Cat 变换。mod 是取模,即求余,目的是为了保证变换后像素点仍落在原先的图像区域内。应用 Arnold Cat 变换进行图像置乱,置乱一次的效果并不理想,而需要反复迭代多次才能达到相对较好的置乱效果。Arnold Cat 变换中的密钥量是参数 a 和 b,以及加密时迭代的次数 λ。由于其加密相对简单,带来了置乱效果不够理想以及密钥量小的缺点(后面有详细分析)。为此,在 Arnold Cat 变换的基础上,提出了均匀置乱的定义。

3 均匀置乱

图像可以看作是由若干个像素点集合所构成,每个像素点集合包含若干个像素点。或者说每个像素点都具有其确定的像素值,若干个像素点按照一定的位置关系集合在一起形

基金项目:教育部春晖计划(No.Z2007-1-15014)。
作者简介:张健(1980-),男,博士,讲师,主要研究领域为信息安全;于晓洋(1962-),男,博士生导师,教授,主要研究领域为图像处理,信息安全;任洪娥(1962-),女,博士,教授,主要研究领域为图像处理。
收稿日期:2009-09-17 **修回日期:**2009-10-12

成图像信息。之所以能分辨出不同图像或同一幅图像的不同部分，是由于构成图像的若干集合所表现出的信息不同。然而，图像位置置乱的实质就是要降低像素点位置之间的相关性直至无关，从而破坏这些集合所表现出的信息，实现图像置乱的目的。

为有效说明置乱的实质，提出“块”的概念。

定义 1 在大小为 $M\times N$ 的图像中，以像素点 $f(i,j)(1\leqslant i\leqslant M,1\leqslant j\leqslant N)$ 为中心的 $m\times n$ 个相邻像素组成的一个邻域，称之为块($0\leqslant m\leqslant M,0\leqslant n\leqslant N$)。

根据块的定义，图像可以看作是由任意形状和数量的块集合所组成，为便于讨论问题，将图像及图像中的每个分块都规定为正方形。

有了这一分块前提，那么原始图像各块的相邻像素在置乱后图像中如何分布才能保证最佳置乱效果，是需要进一步讨论的问题。为此，给出了均匀置乱的定义。

定义 2 原始图像中每块含有 $n\times n$ 个点，如果这些点分别出现在置乱后图像的 $n\times n$ 个块中，不管这些点在置乱后图像各块中出现的顺序如何，只要保证每块中各含有一个点，就称为均匀置乱。

均匀置乱提供了一种进行图像位置置乱的思想，将图像分块并进行均匀置乱是实现图像位置置乱的一种有效途径。如果置乱过程中按块实现了均匀置乱，则就分块层面而言达到了像素间的相关性降到最低。

4　基于 Lu 混沌映射的改进 Arnold Cat 变换图像置乱算法

4.1　基于均匀置乱的改进 Arnold Cat 变换图像置乱算法

在 Arnold Cat 变换的基础上，将其变形为公式(2)。

$$\begin{cases}\begin{bmatrix}F_x'\\F_y'\end{bmatrix}=\left\{\begin{bmatrix}1 & a_1\\ b_1 & a_1b_1+1\end{bmatrix}\begin{bmatrix}F_x\\F_y\end{bmatrix}\bmod(N)\right\}^{n1}\\ \begin{bmatrix}F_x''\\F_y''\end{bmatrix}=B\times\left\{\begin{bmatrix}1 & a_i\\ b_i & a_ib_i+1\end{bmatrix}\cdot\begin{bmatrix}F_x'-1\\F_y'-1\end{bmatrix}\bmod\left(\frac{N}{B}\right)\right\}^{n2}+\begin{bmatrix}k_1\\k_2\end{bmatrix}\end{cases}\tag{2}$$

式中：N 代表图像的大小为 $N\times N$；F_x 和 F_y 分别表示原图像的像素点横纵坐标；F_x' 和 F_y' 分别表示对原图做整体置乱后的像素点横纵坐标；F_x'' 和 F_y'' 分别表示再进行分块置乱后的像素点横纵坐标；B 是原始图像的分块数；a_1，b_1，a_i，b_i 为每一个分块的参数，$i\in(1,B^2)$，取值为正整数；(k_1,k_2) 为原图像分块矩阵的位置坐标；n_1 和 n_2 为迭代次数。

可以将 a_1、b_1、a_i 和 b_i 都作为密钥，由于原始图像分为很多块，每一块的 a_i、b_i 都不同，所以，该算法的密钥量是足够大的。

由于每个分块的 a_i 和 b_i 都不同，置乱的时候就需要记住每个分块的 a_i 和 b_i 值，这显然是不切实际的。为解决这一问题，可以引入混沌映射以实现。

混沌系统最显著特性就是初始敏感性，即初值的微小变化将对结果产生巨大的影响。采用如式(3)所示的三维 Lu 混沌映射[6]：

$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=-xz+cy\\ \dot{z}=xy-bz\end{cases}\tag{3}$$

式中：(x,y,z) 为系统轨迹；(a,b,c) 为系统参数。当 a=36，b=3，c=20 时，系统有一个奇怪吸引子，处于混沌状态。如果给定 Lu 的初值 x_0，y_0，z_0，让系统迭代 k 次，则会产生三个序列$(x_1,x_2,\cdots,x_k)$，$(y_1,y_2,\cdots,y_k)$，$(z_1,z_2,\cdots,z_k)$。这些序列数值在计算机精度范围内是不重复的序列，通过对序列的每个值进行放大、取整、取余等数学变化，可以将前两个序列作为式(2)的每个分块的 a_i 和 b_i 值。这样，不需记住每个分块的 a_i 和 b_i 值，而只需给出 Lu 混沌映射的初始值即可，并利用混沌映射的初值敏感性达到保密的效果。通过将 Arnold Cat 变换和混沌映射的结合，既实现了图像位置的均匀置乱，又增大了算法的密钥量，同时算法具有很好的灵活性和实用性。

Arnold Cat 位置均匀置乱算法可以很好地实现图像的位置置乱，并且其安全性也得到了足够的保证。但是位置置乱后，图像各像素点的像素值并没有发生改变，所以图像的灰度直方图并没有改变。而攻击者可以通过对灰度直方图进行分析，这给安全带来一定的隐患。为了进一步提高安全性，同时考虑均匀置乱图像置乱算法的完整性，在 Arnold Cat 位置置乱的基础上，再将图像的像素值进行置乱，从而形成双重加密。为此，通过 Lu 混沌映射可以实现像素值置乱。

4.2　基于 Lu 混沌映射的改进 Arnold Cat 变换图像置乱算法

采用扩散函数来进行像素值置乱，其表达式如式(4)所示。

$$v_k'=v_k+Z^2\bmod 256\tag{4}$$

式中：v_k 是指每个像素的像素值，v_k' 为置乱后的像素值，Z 取决于 Lu 混沌映射产生的第三个序列 z。该种扩散函数结构简单、扩散速度非常快。

对 Lu 混沌序列的$(z_1,z_2,\cdots,z_k)$，取其从百分位开始的三个数字组成十进制数构成序列。即对于 $z(i)=0.b_1b_2b_3b_4b_5\cdots$，序列 Z 由式(5)得到：

$$Z(i)=100b_1+10b_2+b_3\quad i=0,1,2\cdots\tag{5}$$

在扩散函数中引入了伪随机序列，这样克服了在已知扩散函数时，通过简单的逆运算就可恢复原图像灰度直方图的缺陷。

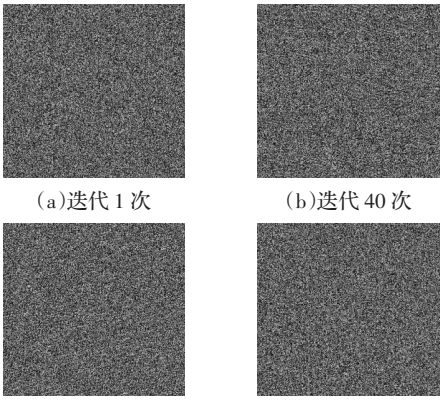
5　实验及分析

为验证所提出的改进 Arnold Cat 变换图像置乱算法的有效性，针对不同典型图像、采用不同参数进行了大量的实验，以经典 256×256 的 Lena 图像为例进行说明。原始图像如图 1 所示。实验中，Arnold Cat 变换的初始值 a=1、b=1；Lu 混沌映射的初值 x_0=−7.042，y_0=4.658，z_0=8.263。

图 1　原始图像

5.1 视觉效果分析

当迭代次数分别为 $n_1=n_2=1$、$n_1=n_2=40$、$n_1=n_2=50$、$n_1=n_2=192$ 时,置乱后的图像如图 2(a)、(b)、(c)、(d)所示。显然,他们均达到比较好的置乱效果,而且不同迭代次数的置乱效果在视觉上无差别。

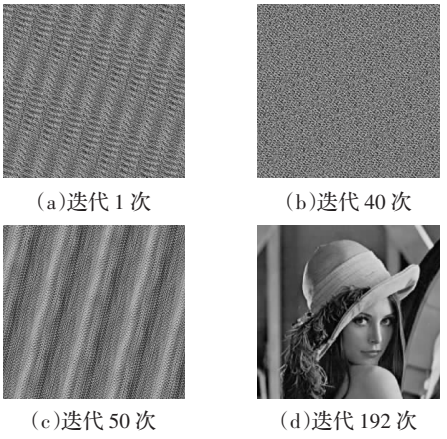


(a)迭代 1 次 (b)迭代 40 次

(c)迭代 50 次 (d)迭代 192 次

图 2 位置置乱后的图像

为了与 Arnold Cat 变换进行对比,将 Arnold Cat 变换迭代相同次数,得到的置乱效果如图 3(a)、(b)、(c)、(d)所示。



(a)迭代 1 次 (b)迭代 40 次

(c)迭代 50 次 (d)迭代 192 次

图 3 Arnold Cat 置乱后的图像

通过对比分析可以得出如下结论:

(1)Arnold Cat 变换不是迭代一次就可以达到好的效果,需要迭代多次,直到出现好的置乱效果。而 Arnold Cat 位置均匀置乱算法一次就可以达到近似理想的状态,多次置乱与一次置乱效果没有太大分别,所以该算法效率显著提高;

(2)Arnold Cat 变换的置乱效果并不是迭代次数越多效果越好,而是一个"好坏交替"的过程,这给观察、判断带来了一定的难度,每次置乱都要去判断效果。而 Arnold Cat 位置均匀置乱算法不管置乱多少次,都能得到类似的置乱效果,无需判断;

(3)对不同的图像,Arnold Cat 变换置乱次数相同,置乱的效果也会不同,即算法极大地依赖于原始图像。而 Arnold Cat 位置均匀置乱算法与原始图像无关,不管什么图像,都能实现其均匀置乱,通用性强;

(4)Arnold Cat 变换具有周期性,迭代某一次后又会恢复到原始图像。而 Arnold Cat 位置均匀置乱算法对整幅图像而言,不存在周期性。

所以,在视觉效果上,改进后的 Arnold Cat 变换图像置乱算法要明显优于 Arnold Cat 变换。

5.2 密钥量分析

由式(1)可以看出,用 Arnold Cat 变换来进行图像置乱,其密钥量取决于参数 a、b 和迭代次数 λ。

首先对 Arnold Cat 变换中 a 和 b 的密钥量进行分析,由式(1)可以得出:

$$\begin{cases} x_{n+1}=(x_n+a\times y_n)\bmod N \\ y_{n+1}=(b\times x_n+a\times b\times y_n+y_n)\bmod N \end{cases} \tag{6}$$

由式(6)得:

$$x_{n+1}=(x_n \bmod N+(a\times y_n)\bmod N)\bmod N=$$
$$(x_n \bmod N+(a \bmod N\times y_n \bmod N)\bmod N)\bmod N \tag{7}$$

由于 x_n 和 y_n 是图像的位置坐标,每一次迭代都是一个固定的值,所以 x_{n+1} 的值取决于 $a \bmod N$ 的变化,而 $a \bmod N=(a+N)\bmod N$,所以 a 的取值范围为 $a\in[1,N]$,同理 b 的取值范围也为 $b\in[1,N]$。以大小为 256×256 的图像为例,当固定 $a=1$,$b\in[1,\infty]$,则迭代至恢复原图像周期数 T 与参数 b 的关系如图 4 所示,其数据如表 1 所示。

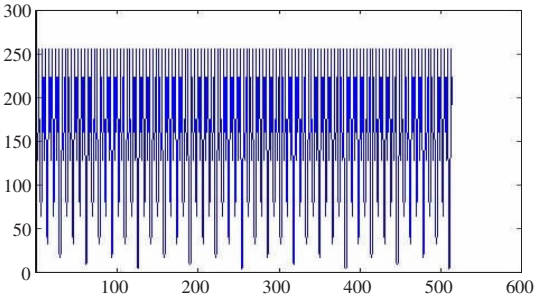


图 4 周期 T 与参数 b 的关系图

表 1 周期数 T 与参数 b 的关系

b	1	2	3	4	5	6	7	8	9	10	…
T	192	128	192	256	96	64	96	256	192	128	…
b	41	42	43	44	45	46	47	48	49	50	…
T	192	128	192	256	48	32	48	256	192	128	…
b	100	101	102	103	104	105	106	107	108	109	…
T	256	96	64	96	256	192	128	192	256	48	…
b	257	258	259	260	261	262	263	264	265	266	…
T	192	128	192	256	96	64	96	256	192	128	…
b	297	298	299	300	301	302	303	304	305	306	…
T	192	128	192	256	48	32	48	256	192	128	…
b	513	514	513	769	770	771	1 025	1 026	1 027	1 281	…
T	192	128	192	192	128	192	192	128	192	192	…

由图 4 和表 1 可以看出,当 a 值一定时,随着 b 的取值不同,Cat 变换的周期 T 呈周期性,其循环周期为 256,也就是说攻击者知道 a 的取值,利用穷举攻击无需知道 b 值,只要计算 256 次就可以恢复出原始图像。同样经实际计算可知当 b 值一定时,随着 a 的取值不同,映射的周期 T 亦呈现周期性,其循环周期亦为 256。

所以,如果将 Cat 变换的参数 a 和 b 作为密钥的话,其密钥量为 N^2,例如,对于大小为 256×256 的图像,密钥量 $key=256^2$。从安全性角度考虑,其密钥量太小、安全性难以得到保证。

表 2　周期值与周期出现的次数关系

序数	1	2	3	4	5	6	7	8	1
周期 T	192	128	256	96	64	48	32	24	192
周期 T 出现的次数	8 192	16 384	16 384	4 096	10 240	2 048	3 584	1 024	8 192
序数	9	10	11	12	13	14	15	16	9
周期 T	16	12	8	6	4	3	2	1	16
周期 T 出现的次数	1 408	512	608	384	536	128	7	1	1 408

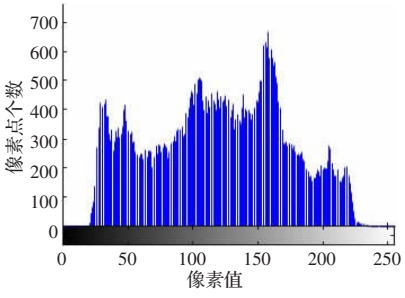


图 5　原始图像的灰度直方图

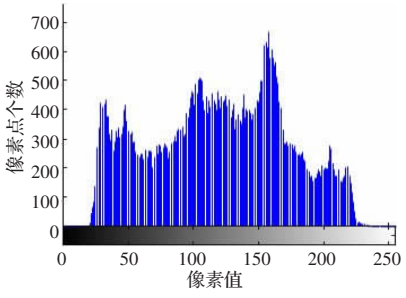


图 6　位置置乱后的灰度直方图

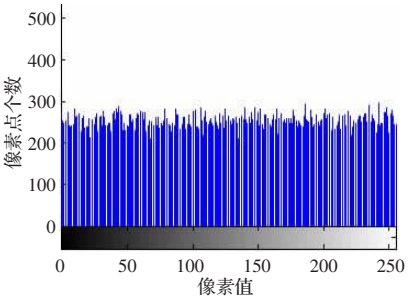


图 7　像素值置乱后的灰度直方图

再对 Arnold Cat 变换中迭代次数 λ 的密钥量进行分析。对于一幅图像,如果 a 和 b 的值给定,其迭代至恢复到原始图像的周期是一个定值,例如对于大小为 256×256 的图像,当 a=1、b=1 时,其迭代至恢复到原始图像的周期 T=192。那么对 $a\in$[1,256]和 $b\in$[1,256]进行全排列周期实验,其所有的周期值与周期出现的次数的关系如表 2 所示,无论 a 和 b 的取值如何,周期的值就为表中的 16 个值。

在知道 a 和 b 值的前提下,如果要对迭代次数进行破解,只需对表 2 列出的 16 个值进行最小公倍数迭代即可恢复原始图像。而这 16 个值的最小公倍数[192,128,256,96,64,48,32,24,16,12,8,6,4,3,2,1]=768。如果把迭代次数作为密钥,其密钥量仅为 768。

所以,Arnold Cat 变换的总密钥量 $key=256^2\times768\approx5\times10^7$,这显然还是非常小,不能抵抗穷举攻击。所以 Cat 变换密钥量小、安全不高。

现对提出的改进 Arnold Cat 变换图像置乱算法进行分析。由前可知,可以将 a_1、b_1、a_i 和 b_i 都作为密钥。对于大小为 256×256 的原始图像,分成 16×16 块,每一块都有一个 a 和 b 值。按照前述进行计算,每块中恢复到原始图像的最小公倍数是[16,12,8,6,4,3,2,1]=48。那么,总密钥量 $key=(16\times16\times48)^{256}>>10^{1\,000}$,这个数量级是不能用穷举方法攻击的。

所以,在视觉效果上,改进后的 Arnold Cat 变换图像置乱算法要明显优于 Arnold Cat 变换。

5.3　灰度直方图分析

在位置置乱的基础上,应用公示(4)进行像素值置乱,其效果如图 5、图 6 和图 7 所示。其中,图 5 是原始图像的灰度直方图,图 6 是位置置乱后的灰度直方图,图 7 是像素值置乱后的灰度直方图。从图中可以看出,经过位置置乱后的灰度直方图并没有发生变化,这样攻击者可以通过统计等手段进行破译,给安全带来了一定的隐患。而经过像素值置乱之后,其灰度直方图发生巨大变化,基本上呈现出均匀分布,根本无法找出原始图像的像素值信息。所以,经过像素值置乱可以进一步提高安全性,实现双重加密的目的。

6　结论

通过对图像置乱实质的分析,提出了位置均匀置乱的概念,并利用 Arnold Cat 变换,结合混沌理论提出了一种图像置乱算法。通过大量实验分析表明提出的算法具有密钥量大、置乱效果好、像素值分布均匀等优点,具有可行性和有效性。

参考文献:

[1] Kwok H S,Tang W K S.A fast image encryption system based on chaotic maps with finite precision representation[J].Chaos,Solitons & Fractals,2007,32(4):1518-1529.

[2] 陈铭.基于 Arnold 变换的图像信息伪装算法[J].计算机应用研究,2006(1):235-237.

[3] 熊昌镇.K 进制面包师变换及其在数字图像加密中的应用[J].北方工业大学学报,2004,16(1):6-11.

[4] 林雪辉.基于 Hilbert 曲线的数字图像置乱方法研究[J].中国体视学与图像分析,2004,9(4):224-227.

[5] 马文涛.一种基于 Zigzag 变换及混沌序列的图像加密方法研究与实现[J].现代电子技术,2008(5):104-109.

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