

文章编号: 1007-130X(2003)04-0007-03

混沌加密图象算法^{*}

An Algorithm for Chaotically Encrypting Images

陶 栋, 李之棠

TAO Dong, LI Zhi-tang

(华中科技大学计算机学院, 湖北 武汉 430074)

(School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

摘 要: 本文利用变化了的 Logistic 系统, 在密码形成的初始参数驱动下, 对图象像素进行加密, 混沌加密图象。这个算法可以用于信息隐藏技术开始时对隐藏信息的加密处理, 提高信息隐藏技术的安全性。

Abstract: The paper uses the changed Logistic system to encrypt image pixels and chaotically encrypt images with the primary parameters formed by your password. The algorithm can be used to encrypt the hidden information when information hiding begins, in order to increase its security.

关键词: Logistic 系统; 混沌加密; 信息隐藏技术

Key words: Logistic system; chaotic encryption; information hiding

中图分类号: TP391.41; TP309

文献标识码: A

1 引言

随着网络时代的到来, 人们越来越多地利用网络来传递信息。信息安全问题越来越受到人们的关注。解密技术以及软硬件的发展严重威胁着加密技术的安全性。信息隐藏技术显示了它的优势。

信息隐藏技术是指将信息隐藏在数字化宿主信息(如文本、图象等)中的技术。

隐藏信息的安全性是评判隐藏技术的重要标准之一。隐藏之前对信息合理加密能够增强其安全性, 加密隐藏信息显然更符合当前需要。文献[1]中提到了置换图象像素地址的方法来置乱图象, 以达到保护图象信息的目的。但是, 这种方法

运算量比较大, 它要求对图象的所有象素点遍历一次, 同时还要考虑地址之间的相关性。根据对混沌算法的理解, 本文提出了混沌加密图象象素的方法, 此方法易实现、运算量小、效果好。

2 混沌加密图象象素的算法

2.1 混沌系统的介绍

混沌(Chaos)是一种复杂的非线性、非平衡的动力学过程, 其特点为: (1) 混沌系统的行为是许多有序行为的集合, 而每个有序分量在正常条件下, 都不起主导作用; (2) 混沌看起来似为随机, 但都是确定的; (3) 混沌系统对初始条件极为敏感, 对于两个相同的混沌系统, 若使其处于稍异的

* 收稿日期: 2002-09-30; 修订日期: 2002-12-24

基金项目: 武汉市科技计划资助项目(2000101111)

作者简介: 陶栋(1977-), 女, 江苏泰兴人, 硕士, 研究方向为网络安全; 李之棠, 教授, 博士生导师。

通讯地址: 430074 湖北省武汉市华中科技大学东 13 舍 523; Tel: (027) 87780353-819, 13036115096; E-mail: hustdong@hust.edu.cn

Address: School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, Hubei 430074, P.R.China

初态就会迅速变成完全不同的状态。

现介绍一个常用的混沌系统 Logistic:

$$X(n+1) = 1 - aX^2(n) \tag{1}$$

如果 $a = 1.945\ 68$, 初始条件为 $X(0) \in [0, 1]$ 时, $|X(n)|$ 在 $[0, 1]$ 之间混沌地变化。

2.2 混沌系统在加密图象(bmp)中的应用

在 bmp 图象中每个象素由三个字节组成, 它们的大小都在 $[0, 255]$ 之间变化, 混沌加密的结果仍然是存放在图象中的, 这就要求加密结果值也必须在 $[0, 255]$ 内。通常的方法是使用一个混沌值和图象的象素值做运算, 所得结果必然处于混沌状态。

我们用 Logistic 系统产生混沌值, 取 $a = 1.945\ 68$, 初始条件: $X(0) \in [0, 1]$, $a[i, j]$ 表示原图象象素值, $A[i, j]$ 表示加密后的象素值。具体操作如下:

$$X(n+1) = 1 - 1.945\ 68 * X^2(n) \tag{2}$$

$$A[i, j] = a[i, j] * |X[n]| \tag{3}$$

比较如图 1 所示的原图和如图 2 所示的加密图发现, 加密结果仍可看出原图的轮廓。研究后发现此系统并未使得象素值 $a[i, j]$ 加密后的值 $A[i, j]$ 在 $[0, 255]$ 之间变化, 实际变化范围是 $[0, a[i, j]]$ 。加密算法并没有解决象素局部性问题, 所以加密效果很不如人意。



图 1 原图



图 2 加密后图

下面的公式可以得到 $[0, 255]$ 之间混沌变化的序列:

$$X(n+1) = 255 - 1.945\ 68 * X^2(n)/255 \tag{4}$$

计算式 $(X[n] + a[j, k]) \bmod 255$ 可以得到一个藏有信息且混沌的序列。使用这种算法对图象 $(M * N)$ 进行加密, 只需产生 $M * N$ 个混沌值, 并与每个象素值相加取 255 的模。所以, 该算法的复杂度为 $O(n * m)$ 。下面我们使用这种算法对图象加密:

$$X(n+1) = 255 - 1.945\ 68 * X^2(n)/255 \tag{5}$$

$$T[i, j] = (X(n+1) + a[i, j]) \% 255 \tag{6}$$

图 4 是加密的结果(初值为 $X(0) = 94$), 图 3 为原图。结果并不理想, 我们仍能看到图象轮廓。取 $n = 589\ 824$, 对混沌序列 $|X(n)|$ 作统计, 统计结果如表 1 所示。由表 1 可得到图 5。



图 3 变化前

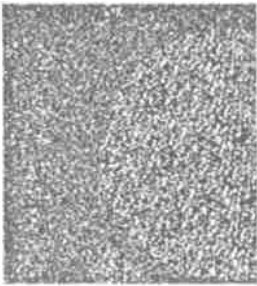


图 4 加密之后

表 1 当 $n = 589\ 824$ 时, 对混沌序列 $|x(n)|$ 的统计

项目	X(n) 值的范围					
	> 200	> 150	> 100	> 50	> 0	
X(n) 初值	0	219 164	122 884	80 600	74 697	92 479
	90	219 178	122 884	80 585	74 693	92 484
	30	256 770	142 656	38 157	28 649	123 592
	120	219 169	122 887	80 590	74 692	92 486
	160	219 166	122 877	80 599	74 704	92 478
	200	219 164	122 885	80 599	74 703	92 473
	240	219 179	122 894	80 570	74 701	92 480
所占比例	37. 16%	20. 84%	13. 66%	12. 66%	15. 68%	

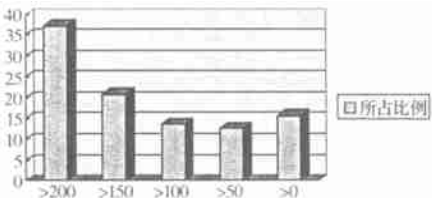


图 5 统计图

由此可见, 此序列不完全混沌, 在 $[200, 255]$ 区间比较密, 而在 $[50, 150]$ 区间上则比较稀疏, 其密度不及前者的 $1/2$ 。

分析原图: 圆圈外的主要颜色是 $(0, 64, 128)$ (RGB), 红色圆圈内颜色为 $(255, 0, 0)$, 这两种颜色相差比较大, 当使用混沌系统加密的时候, $(0, 64, 128)$ 区域就会更倾向于 $(R > 200; 64 > G > 13; 128 > B > 73)$, $(255, 0, 0)$ 区域会倾向于 $(R > 200; G > 200; B > 200)$ 。

显然, 这两个区域是不同的。对这两个区域抽样统计得表 2。

表 2 基本符合上面我们通过理论得到的估计, $(0, 64, 128)$ 区域加密后的象素值偏向于红色, 而 $(255, 0, 0)$ 区域加密后的象素值偏向于白色。

所以,加密后仍能看到轮廓。显然,图象的局部性已经明显减小,边缘界限很模糊。如果再对图二次混沌加密,选择不同的初值,得到图6。

表 2 抽样统计

	(255, 0, 0) 区			(0, 64, 128) 区		
	R	G	B	R	G	B
0	71	206	79	44	7	214
1	254	2	183	2	247	180
2	13	187	240	237	111	37
3	96	214	72	241	63	128
4	147	229	252	16	252	114
5	61	203	245	225	126	31
6	183	240	43	187	49	171
7	177	237	254	237	62	139
8	216	71	155	187	49	127
9	44	198	86	252	80	61
10	156	232	54	252	81	49
11	254	7	180	6	249	223
12	238	254	8	93	22	201
13	228	251	20	169	45	126
14	62	259	112	227	60	149
15	135	226	251	254	70	58
16	229	252	19	20	54	162

此时的原图已经基本上处于混沌状。但是,如果我们仔细看,还是可以看到一些很模糊的轮廓。但是,这已经难不住我们了,解决方法有两种:第一就是再换一个初值,混沌加密一次;还有就是在第二次混沌加密的时候,改变一下混沌加密的算法。修改后的算法中公式(5)不变,公式(6)改为

$$T = (X(n + 1) + a[j, k]/2) \% 255 \tag{7}$$

这种算法的弱点是,恢复的原图将会有误差 $C, |C| \leq 1$ 。图7为试验图,加密图象的恢复算法为加密算法的反过程:

```

if A[i, j] > X[n] then
a[i, j] = A[i, j] - X[n]
else
a[i, j] = A[i, j] + 256 - X[n]

```

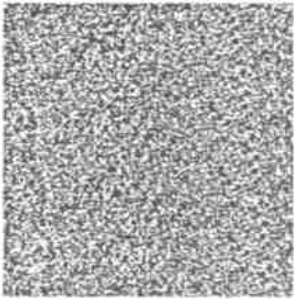


图 7 试验图

我们通过密钥产生混沌加密的初值,初值空间将决定加密的安全性。由上面的讨论可知,这个初值的范围为[0, 255]。现在我们来讨论初值

变化最小值,图象仍可被加密。
显然,一次加密的空间为(0.000 00, 255.000 00),其中最小单位是0.000 02。从我们加

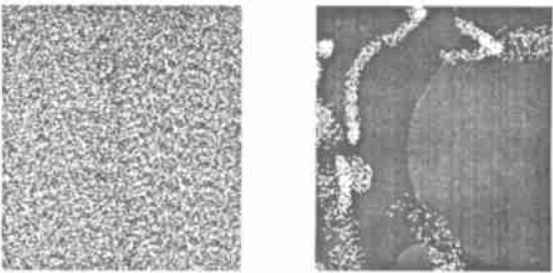


图 8 初始值增加 0.00002 后的解密图 图 9 初始值增加 0.00001 后的解密图

密两次的时候起密码空间就会呈平方递增,所以其安全性是相当可靠的。图 8 为初始值增加 0.000 02 后的解密图,图 9 为初始值增加 0.000 01 后的解密图。

解密过程中,如果初值变化 0.000 02,其解密后的图形就会变化很大。所以,我们发现了一个更好的加密算法,即将混沌加密算法和其提取算法相组合所形成的加密算法(组合时注意他们的初值不能相等,否则就相当于加密解密了)。该算法效果相当好,图 10 是其效果图。

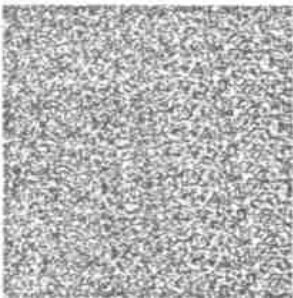


图 10 加密算法效果图

3 结束语

本文成功地运用混沌理论改进传统的混沌加密算法,使之能更好地应用于 bmp 格式的图象加密。该算法具有算法简单、运算量小、加密效果好和密钥的空间大等优点,将它运用于信息隐藏技术必将大大提高隐藏信息的安全性,

参考文献:

[1] 谢荣生,秦红磊,郝燕玲,等.混沌二维置换网络的设计及其在图象数字水印隐藏中的应用[A].信息隐藏(CIHW2000/2001)论文集[C].2001.88-96.
[2] 杨世平,牛海燕,田钢,等.用驱动参数法实现混沌系统的同步[J].物理学报,2001,50(4):619-623.
[3] 易开祥,石教英,孙鑫.数字水印技术研究发展[J].中国图象图形学报,2001,6(2):111-116.