基于混沌序列的图像加密解密算法

陈永红[1,2] 黄席樾[1]

(重庆大学自动化学院 重庆400044)[1] (重庆师范大学数学与计算机系 重庆400047)[2]

An Image Encryption and Decryption Algorithm Based on Chaos Sequence

CHEN Yong-Hong[1,2] HUANG Xi-Yue[1]

(Automatization College, Chongqing University, Chongqing 400044)[1]

(Department of Maths and Computer, Chongqing Normal University, Chongqing 400047)[2]

Abstract In this paper, an image encryption and decryption algorithm based on chaos sequence is proposed. This algorithm provides low computational complexity, high security and no distortion. Finally, experimental results are satisfactory.

Keywords Chaos, Chaos sequence, Encryption, Decryption

1 引言

混沌系统是一种高度复杂的非线性动态系统,具有对初始条件非常敏感的特性,由它产生的混沌序列具有随机特性。因此,常把混沌应用用于信息加密中。随着现代通信技术和网络技术的发展,尤其是电子商务的兴起,对信息加密提出了更高的要求。特别是对图像、声音等信息的加密尤为重要。

目前,对图像的加密还是基于传统的数据加密方式,没有利用图像本身的数据特性,因而存在一定的局限性。

文[1,2]提出的算法是先生成的实数值混沌序列,然后把实数值混沌序列转化为二进制序列,再利用该序列作为判断条件间接加密图像,其缺点是生成的实数值混沌序列在数字化的时候存在有限精度问题,从而使混沌序列存在退化和周期性,而且它是利用混沌序列间接加密图像,没有很好利用到混沌的特性。文[3,4]提出图像加密算法,但是没有相应明显的解密算法,并且已经有人提出该加密算法存在安全隐患。

文[5]提出了一种离散非线形的混沌系统,该系统是一维线形混沌映射的推广,其结果生成任意区间上的整数值混沌序列,但并没有对图像进行加密,只是混沌序列的生成方式。本论文中利用文[5]提出的混沌序列生成方式形成新的混沌映射,该混沌映射比文[5]提出的混沌映射复杂度更高,而且生成整数值混沌序列仍然具有混沌特性。然后用生成的混沌序列直接加密图像,既改变像素的灰度也改变像素的位置,易实现、计算花费少,加密的实验结果表明其保密性很好,加密后的图像可以完全正确地还原成原始图像。

2 混沌影射

在文[5]中提出了一个具有良好随机统计特性的一维非线形混沌影射,由它生成的混沌序列为某一区域上的整数值混沌序列,具有随机性,且对初值极其敏感。其定义如下:

$$x_{k+1}=f_a(x_k)=\begin{cases}\lceil (m/a)x_k\rceil & ,1\leqslant x_k\leqslant a\\ \lfloor m(m-x_k)/(m-a)\rfloor & ,a<x_k\leqslant m\end{cases} \quad (1)$$

其中 $x_k\in\{1,2,\cdots,m\}$,参数 $a\in\{1,2,\cdots,m\}$,$([z],[z]$分别表示不大于 z 的最大整数和不小于 z 的最小整数。

混沌影射(1)经过 n 次迭代后形成新混沌影射(2),如下所示,即为本文要运用的影射,同样具有上述混沌影射(1)的混沌特性,记为:

$$x_{k+1}=f_a^n(x_k) \quad (2)$$

当给定初始值 x_0,参数 a,m 的值和迭代次数 n 的值就确定了由混沌系统(2)生成混沌序列:$\{x_k;k=0,1,2,3\cdots\}$。该序列具有混沌特性,对初值条件 x_0 极为敏感。本文把参数 a 与 n 也作为初始条件,即把有序数组(x_0,a,n)一起作为密钥,则攻击混沌系统(2)成功的概率比只把 x_0 作为密钥时攻击成功的概率更小。

举例说明混沌影射(2)生成混沌序列的具体过程。例如:产生[1,371]的一个整数混沌序列,取参数 $m=371,a=205$,下表为混沌序列产生过程,表第一行为迭代次数 n,第一列为 x_k,表中为对应某一 x_k,n 的 x_{k+1}:

表1

	1	2	3	4	.	13	14
1	2	4	8	15	.	300	159
2	4	8	15	28	.	159	288
3	6	11	20	37	.	269	228
.	.	.	.	.	.	.	.
369	5	10	19	35	.	277	211
370	3	6	11	20	.	251	269
371	1	2	4	8	.	237	300

3 图像加密解密算法

本文用混沌系统(2)生成的混沌序列加密图像,既改变图像像素的位置,同时也改变图像像素的灰度值,该算法简洁、易实现。

3.1 加、解密算法设计

设原始图像为 I_R,用$(i,j,g(i,j))$表示这一张图像,(i,j)为某一像素标值,$g(i,j)$表示该像素的灰度值,这一张图像的大小为 $M\times N$ 个像素。其中$0\leqslant i\leqslant M-1,0\leqslant j\leqslant N-1,L$ 为该图像的灰度水平。

3.1.1 加密算法设计

Step 1:输入 M,N,原始图像 $I_R=(i,j,g(i,j))$。

陈永红 博士,主要研究方向为智能控制、计算机控制、信息安全技术等。黄席樾 教授,博士生导师,主要研究方向为智能控制、计算机控制等。

Step 2:输入一维混沌影射(2)的初始值 x_0,设置参数 a,m 的值和迭代次数 n 的值,用混沌影射(2)生成混沌序列:x_0,$x_1,x_2,\cdots,x_{M+N-1}$。

Step3:

```
for i=0 to M-1
    X_i=x_i mod N
    for j=0 to N-1
        if j+X_i≥N
            (i,j,g(i,j))→(i,j+X_i-N,g(i,j))
        else(i,j,g(i,j))→(i,j+X_i,(g(i,j))
    end
end
```

利用第二步生成的混沌序列将图像的每行像素右移(循环移动)变换到该行的另一位置,像素的灰度值不改变。变换得到的图像为:$(i,j,g_1(i,j))$。

Step4:

```
for j=0 to N-1
    Y_j=x_{M+j} mod M
    for i=0 to M-1
        if i+Y_j≥M
            (i,j,g_1(i,j))→(i+Y_j-M,j,g_1(i,j))
        else(i,j,g_1(i,j))→(i+Y_j,j,g_1(i,j))
    end
end
```

这一步在第三步得到的变换结果$(i,j,g_1(i,j))$的基础上,利用第二步生成的混沌序列将图像的每列像素向下移动(循环移动)变换到该列的另一位置,像素的灰度值不改变。变换得到的图像为:$(i,j,g_2(i,j))$。

Step 5:重新输入一维混沌影射(2)的初始值 x'_0,设置参数 a',m'的值和迭代次数 n'的值,用混沌影射(2)生成混沌序列:$x'_0,x'_1,x'_2,\cdots,x'_{M\times N-1}$。

Step 6:将第四步得到的结果$(i,j,g_2(i,j))$的每一像素的灰度值改变。

```
for i=0 to M-1
    for j=0 to N-1
        (i,j,g_2(i,j))→
                (i,j,(g_2(i,j)+x'_{i×N+j} mod L)
    end
end
```

得到加密图像的各个像素的新的灰度值 $g'(i,j)$,生成加密图像 $I_E=(i,j,g'(i,j))$。

Step 7:终止算法。

3.1.2 解密算法设计

Step1:输入 M,N 以及加密图像 I_E。

Step2:这一步与加密过程第五步正好一样,输入一维混沌影射(2)的初始值 x'_0,设置参数 a',m'的值和迭代次数 n'的值,用混沌影射(2)生成混沌序列:$x'_0,x'_1,x'_2,\cdots,x'_{M\times N-1}$。

Step3:

```
for i=0 to M-1
    for j=0 to N-1
        (i,j,g'(i,j))→
        (i,j,(g'(i,j)-x'_{i×N+j}) mod L)
    end
end
```

这一步是加密过程的第六步的逆过程,利用第二步生成的混沌序列将加密图像的每一像素的灰度值改变,还原成原来的相应灰度值。得到结果为:$(i,j,g_2(i,j))$。

Step4:输入一维混沌影射(2)的初始值 x_0,设置参数 a,m 的值和迭代次数 n 的值,用混沌影射(2)生成混沌序列:x_0,$x_1,x_2,\cdots,x_{M+N-1}$。这一步是加密过程的第二步的一致。

Step 5:

```
for j=0 to N-1
    Y_j=x_{M+j} mod M
    for i=0 to M-1
        if i-Y_j≤0
            (i,j,g_2(i,j))→(i-Y_j+M,j,g_2(i,j))
        else(i,j,g_2(i,j))→(i-Y_j,j,g_2(i,j))
    end
end
```

这一步是加密过程的第四步的逆过程,将图像$(i,j,g_2(i,j)$的每列像素向上移动(循环移动)变换到该列的另一位置,像素的灰度值不改变。得到的结果为:$(i,j,g_1,(i,j))$。

Step 6:

```
for i=0 to M-1
    X_i=x_i mod N
    for j=0 to N-1
        if j-X_i≤0
            (i,j,g(i,j))→(i,j-X_i+N,g(i,j))
        else(i,j,g(i,j))→(i,j-X_i,(g(i,j))
    end
end
```

这一步是加密过程的第三步的逆过程,将图像$(i,j,g_1(i,j)$的每列像素向下左移动(循环移动)变换到该列的另一位置,像素的灰度值不改变。得到的结果为:$(i,j,g(i,j))$。

得到解密图像的各个像素的新的灰度值,生成解密加密图像 $I_D=(i,j,g(i,j))=I_R$。还原图像。

Step 7:终止算法。

3.2 加密解密结构图

如图1所示,混沌系统(2)对于加密解密过程是完全一样的,也即混沌系统(2)的初始值 x_0,x'_0参数 a,a',m,m'的值和迭代次数 n,n'的值对于加密解密处理过程完全一样,从而保证加密前的图像和解密后的图像完全一致,即完全还原。

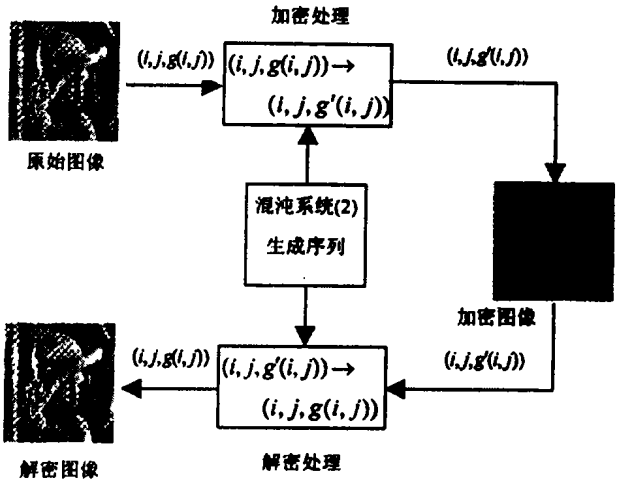

图1

4 算法分析

4.1 破解混沌影射(2)变得复杂

本论文不仅仅以混沌影射(2)的初始值 x_0,x'_0作为密钥,而是以数组$(x_0,a,n,m),(x'_0,a',n',m')$作为密钥,这就加大了破解加密后的图像的复杂度,比以前单以初始值 x_0,x'_0为密钥的破解难度更大。

4.2 破解加密图像变得复杂

对于图像每个像素,由于混沌系统(2)生成的混沌序列随机特性,通过变换可能在图像的任何位置,加密结果可能有$(M\times N)!$结果,每个像素可能的灰度值为 L 种,如果采用穷举法攻击需要计算$(M\times N)!\times L^{M\times N}$次,其破解成功的概率几乎为0。例如:一张原始图像 I_R,大小为 $M\times N$ 个像素,$M=256$,$N=256$,$L=16$采用穷举法攻击需要计算$(256\times 256)!$

(下转第143页)

表3 经 NDNA-GA 优化设计的 TS 模型控制器设计参数
（模型输出为2.5）

a_{ij} b_{ij}		$\mu_1(r)$	$\mu_2(r)$	$\mu_3(r)$
	a	0.000	−0.100	−0.500
	b	0.000	−0.700	−0.200
$\mu_1(e)$	0.000	0.250	0.000	0.017
	−0.400	0.150	0.183	0.183
$\mu_2(e)$	−0.400	0.233	0.050	0.033
	−0.800	0.083	0.133	0.150
$\mu_3(e)$	0.200	0.133	0.150	0.017
	−0.700	0.183	0.083	0.033

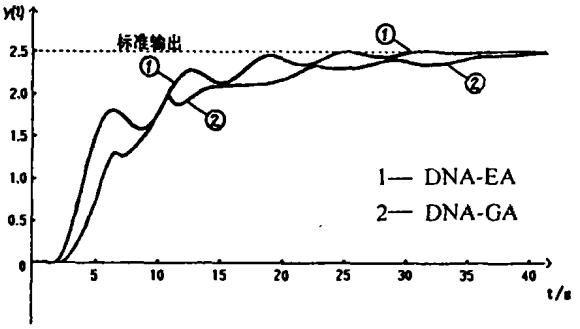

图2 经 DNA-GA 与 DNA-EA 优化设计的 TS 模糊控制器的仿真性能的比较

由图2可见：①两种算法均能在很短时间内收敛到标准（期望）值2.5，所以算法是有效的；②DNA-EA 在30代收敛，DNA-GA 在33代收敛，故 DNA-EA 收敛快；③DNA-EA 比 DNA-GA 响应（调整）时间短，上升时间快，超调量小，静态误差相同，几乎均为0，但 DNA-EA 振荡程度稍大。综上比较可知，DNA-EA 仿真性能优于 DNA-GA。因为 DNA-EA 的基因转移操作将适应度较优个体上的好的编码部分直接转移到较差适应度的个性上，算法频繁地作用于好的规则，促进了群体性能的提高，有利于全局最优解的搜索。DNA-EA 的细菌变异对于局部搜索也是很有效的，为了便于比较这两种算法，本文对此采用了相同的染色体结构（见图1），但这种结构较适于 DNA-GA 的遗传操作，而对于 DNA-EA 则欠佳，从而使 DNA-EA 的优点在本文中尚未能够得到充分体现。下一步的工作是改进 DNA 链结构，并采用框构变异以获得更好的算法优化解性能。基于 DNA 机理的学习算法，对解决特定复杂的实际问题已显示出了极大的潜力，进一步将研究其他一些基于 DNA 技术的软计算。

参 考 文 献

1 孙增圻，张再兴，邓志东编著. 智能控制理论与技术. 清华大学出版社，1997

2 高琳，许进，张世英. DNA 计算的研究进展与展望. 电子学报，2001，29(7)：973～977

3 Shi Y H，Eberhart R，Chen Y B. Implementation of evolu- tionary fuzzy systems. IEEE Tyans. Fuzzy Systems，1999，7(2)：109～119

4 Lim M H，Rahardja S，Gwee B H. A GA paradigm for lear- ning fuzzy rules. Fuzzy Sets & Systems，1996，82：177～186

（上接第140页）

$\times 16^{256\times256}$次，这几乎不可能攻击成功。

4.3 解密加密的图像无失真

由本文提出的加密解密算法知解密是加密的逆过程，该算法完全可以把加密图像还原成原始图像，即解密加密的图像完全可以还原成原始图像。

5 实验结果

为了验证上述算法的有效性，本文对一幅 Lena 图进行实验。在这个例子中 $M=257$，$N=361$。取混沌系统(2)的初始值 $x_0=35$，$x'_0=24$，设置参数 $a=94$，$a'=87$，$m=256$，$m'=241$迭代次数 $n=6$，$n'=5$数组(x_0,a,n,m)，(x'_0,a',n',m')作为密钥。加密解密结果如下。数组任意一个数值错误，解密的结果将不能还原成原始图像。例如：图2为原始图像，图3为加密图像，图4为密码正确的解密图像，图5为密钥错误（$x_0=34$）的解密图像，图6为密钥错误（$a=93$）的解密图像，图7为密钥错误（$n=5$）的解密图像。图8为密钥错误（$m=255$）的解密图像。

图2 图3 图4 图5

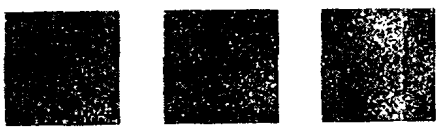

图6 图7 图8

结论 本文提出的混沌系统加密解密图像算法通过改变混沌影射的初始值、参数值以及增加迭代次数来增加混沌系统的复杂性，而且实际实现图像加密时，增加了破解加密图像的计算复杂度，从而保证了图像信息的保密性，设计简单且容易实现，计算量少，解密加密图像可以完全还原。计算机模拟结果表明该算法确实可行。

虽然本文只对一种类型的图像进行加密，但是很显然可以对其它任意类型的图像进行加密，只需要选取适当的参数即可。

参 考 文 献

1 Yen J-C，Guo J-I. A new chaotic key-based design for image encryption and decryption. IEEE International Symposium on Circuits and Systems，2000，IV：49～52

2 Fridrich J. Image encryption based on chaotic maps. IEEE，1997. 1105～1110

3 易开祥，孙鑫，石教英. 一种基于混沌序列的图像加密算法. 计算机辅助设计与图形学报，2000，12(9)：672～676

4 孙鑫，易开祥，孙优贤. 基于混沌系统的图像加密算法. 计算机辅助设计与图形学报，2002，14(2)：136～139

5 Masud N，Aihara K. Cryptosystems With Discretized Chaotic Maps. IEEE Trans Circuit and Systems，2002，49(1)：28～40

6 Yen J-C，Guo J-I. Efficient hierarchical chaotic image encryption alogorithm and its VLSI realistion. IEE proc.-vis Image Signal Process，2000，147(2)：167～175