一类改进型基于混沌的图像置乱网络设计

刘云江 刘向东
(鞍山科技大学图形图象与网络研究所,辽宁鞍山 114002)
王光兴
(东北大学信息科学与工程学院,沈阳 110004)

摘 要 基于混沌映射的图像置乱是图像加密的一种常用方法。为了增加图像置乱网络的复杂度和提高网络运行的速度,提出了一种改进型基于混沌的图像置乱网络。该网络首先对混沌映射区间进行二次划分,然后在二次划分的区间上将混沌映射的迭代值动态量化为置乱图像的坐标,从而不仅克服了有限精度下混沌轨道遍历混沌映射区间的时间复杂度高的问题,而且减少了搜寻新坐标的迭代次数。另外,还通过计算机实验,对置乱网络的遍历时间复杂度及其置乱性质进行了分析。结果表明,这种置乱网络不仅提高了算法的运行速度,而且增加了密钥参数和密钥空间,具有良好的置乱性质,可以有效地保障加密图像的安全性。

关键词 混沌 置乱网络 区间分割
中图法分类号: TP309.7 TP391.41 **文献标识码**: A **文章编号**: 1006-8961(2004)03-0360-05

The Design of A Class of Modified Chaotic Picture Scrambling Networks

LIU Yun-jiang, LIU Xiang-dong
(*Institute of Graphics, Images & Network, Anshan University of Science & Technology, Anshan Niaoning* 114002)
WANG Guang-xing
(*School of Information Science & Engineering, Northeastern University, Shenyang* 110004)

Abstract The picture scrambling algorithms based on chaos are frequently-used for images secure communications. In this paper, a new modified method of chaotic picture scrambling network is proposed by the chaotic mapping interval twice division and the chaotic orbits dynamic quantification. The new scrambling network adds the complexity and speeds up the computation of the network, since it overcomes the disadvantage that it need large number of computation to make the chaotic orbits ergods the whole chaotic mapping interval under the finite computational accuracy, reduces the computation. The paper also analyzed the time complexity and the scrambling performance of the new networks by computer experiments. The results show that this picture scrambling network has good scrambling capability and guarantees the security of the encrypted images effectively because it can work quickly with large cryptographic keys space.

Keywords chaos, scrambling network, interval division

1 引 言

随着 Internet 技术与多媒体技术的飞速发展,多媒体通信逐渐成为人们进行信息交流的重要手段,由于数字图像是通信中重要的信息载体,因此数字图像加密技术在多媒体通信和保密通信中有重要意义。

数字图像置乱加密技术目前主要有如下 3 种:(1)基于图像像素点坐标的空间域和频域变换加密;(2)基于图像色度域变换的加密;(3)基于图像空间域和色度域变换的加密。其中基于图像空间域变换的数字图像置乱是一种常见的图像加密方法,其图像置乱要求为置乱后的图像具有较低的可懂度;置乱后的图像要具有一定的安全性,能抗一定程度的破译攻击;解密后的图像能准确表达原始图像的内容。文献[1~3]给出了几种基于几何运算和空间域变换的图像置乱变换算法。

众所周知,混沌现象是非线性动态系统中出现的确定性伪随机过程,即混沌系统具有对初始条件的极端敏感性,由于其可产生大量的具有非周期性

基金项目:辽宁省自然科学基金(2001102099);国家博士后基金
收稿日期:2002-12-10;改回日期:2003-08-01

和宽谱性的类随机信号,因而适合应用于密码体系的设计。1989 年,英国数学家 Matthews 首先提出了应用混沌理论进行加密的方法[4],之后应用混沌理论进行加密体系的设计有了巨大的发展,文献[5,6]分别提出采用参数化的二维混沌映射在空间域对图像的各像素重新进行排列加密的方法,文献[7]采用一维混沌映射在空间域对图像的像素点进行置乱加密。文献[8]采用混沌映射构造了空间域的置换矩阵和色度域的加密矩阵来进行置乱和加密。本文正是基于此思想,在文献[7]的基础上给出了一种改进算法,其不仅大大减少了混沌映射的迭代次数,而且提高了图像加密解密算法的运算速度,同时增加了算法的密钥参数、密钥空间和算法的复杂度。

2　图像置乱网络的设计

采用一维 Logistic 映射

$$x_{n+1}=1-2x_n^2 \quad x([-1,1] \tag{1}$$

来产生混沌序列,其中,x_n 为第 n 次迭代值。理论上,由式(1)的 Logistic 映射生成的混沌序列在混沌映射区间$[-1,1]$具有遍历性,同时由于此 Logistic 映射还具有 δ 函数的自相关函数和零的互相关函数,因而可以作为良好的图像置乱网络的像素点坐标产生器。利用混沌信号产生图像像素点坐标的过程,实质上就是将实值混沌信号转换为符号序列的过程,即

(1) 将混沌映射区间$[-1,1]$划分为 q_1 个相邻的连续子区间,记为第 1 次划分,使得点 x_n 落入各个子区间的概率相等。记第 1 次划分点依次为 d_0,$d_1,\cdots,d_q$,映射(式(1))的轨道点分布的概率密度为

$$\rho(x)=1/(\pi\sqrt{1-x^2}) \quad x\in[-1,1] \tag{2}$$

易知,第 1 次划分,各划分点为

$$d_k=-\cos(k\pi/q_1) \quad k=0,1,2,\cdots,q_1 \tag{3}$$

对于一个二维 $M\times N$ 像素的图像,文献[7]的图像置乱网络的置乱算法是:首先在混沌映射区间$[-1,1]$分别取 $q_1=M$ 和 $q_1=N$,由式(3)来生成两种第 1 次划分,然后在两种划分上分别采用一个 Logistic 映射进行迭代,并对生成的遍历这 $M\times N$ 个区间的两个混沌序列分别进行 M 值和 N 值量化来产生像素点的行列坐标,最后根据此坐标依次对像素点重新进行排列来生成加密图像。

周期点稠密是混沌系统的内在规律性,但以这些周期点为初值的混沌映射,其迭代生成的混沌序列对混沌区间不具有遍历性,并且在实际应用中都是在有限精度下来实现混沌映射,而对于 M、N 较大的情况下,则对任一初值均不能保证混沌映射的遍历性。本文在文献[7]的基础上,采用了对混沌映射区间进行动态二次划分的改进算法,即对于混沌映射区间的第 1 次划分,本文选取任意 $q_1>1$ 的整数由式(3)来生成两个一样的第 1 次划分。为说明方便,将其中一个称为行划分,另一个称为列划分。

(2) 在行、列划分的第 1 次划分的每个区间内再划分 q_2 个相邻的连续子区间,记为第 2 次划分,同样使得点 x_n 落入各个子区间的概率相等,其中对应$[d_k,d_{k+1}]$区间的 q_2 个划分点依次记为 $d_k^{(0)},d_k^{(1)},\cdots,d_k^{(q_2)}$,其中,$d_k^{(0)}=d_k$,$d_k^{(q_2)}=d_{k+1}$,易知第 2 次划分各划分点为

$$d_k^{(m)}=-\cos((k\times q_2+m)\pi/(q_1\times q_2)) \tag{4}$$
$$k=0,1,\cdots,q_1-1 \quad m=0,1,\cdots,q_2$$

对于一个二维像素的图像,在行、列划分的第 1 次划分的每个子区间上分别取 $q_2=M$ 和 $q_2=N$ 再由式(4)进行第 2 次划分。为说明方便,约定第 1 次划分的子区间$[d_k,d_{k+1}]$称为第 k 个转轮,行划分上的每个转轮内的 M 个相邻的连续子区间对应像素点的 M 个行坐标,同理,列划分上的每个转轮内的 N 个相邻的连续子区间则对应像素点的 N 个列坐标。第 k 个转轮内的每个小区间所对应像素点的坐标循环右移一格称为第 k 个转轮转动一格,图 1 给出了行划分上第 k 个转轮转动一格,后每个小区间对应像素点坐标的状态。

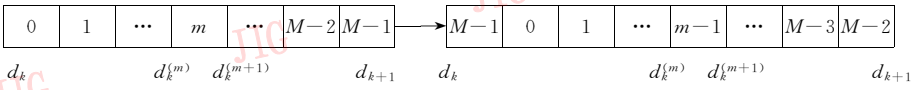


图 1　第 k 个转轮转动一格后,转轮内的每个小区间对应像素点的坐标重新分配示意图

在二次划分的区间上,通过对混沌映射的迭代值进行动态量化来生成坐标值,解决了如下两个问题:

(1) 针对有限精度下,混沌序列对混沌区间不具有遍历性的性质,提出了一种能重构原图像全部坐标的方法。通常随着迭代值来驱动每个转轮的转动,可导致第 2 次划分的每个小区间对应的坐标值

是变化的，这样即使迭代值对混沌区间不具有遍历性，但由于经动态量化后也能重构原图像的全部坐标值，从而克服了文献[7]不具有遍历性的缺点。

(2) 提高了算法的速度。混沌映射的相邻迭代值之间存在一定的相关性，即对迭代值在一次划分的区间上进行普通量化生成的符号序列汉明相关大[9]，文献[9]给出了改善生成符号序列汉明相关性的量化算法。本文算法也改善了符号序列的汉明相关性，即同样随着每个转轮的转动，迭代值落入第 2 次划分每个小区间的对应坐标值是变化的，并使生成的相邻坐标值之间相关性减弱，这样由于减少了搜寻新坐标值的迭代次数，从而提高了算法的速度。

生成加密图像的算法如下：

(1) 赋初值 $g_{\mathrm{row},k}=0, g_{\mathrm{column},k}=0, k=0,1,2,\cdots,q_1-1$；$\boldsymbol{V}_{\mathrm{row}}=\{\}$，$\boldsymbol{V}_{\mathrm{column}}=\{\}$；$I=0, J=0$；其中 $g_{\mathrm{row},k}$、$g_{\mathrm{column},k}$ 分别标志行、列划分上的每个转轮的状态；$\boldsymbol{V}_{\mathrm{row}}$ 为行坐标集合，$\boldsymbol{V}_{\mathrm{column}}$ 为列坐标集合；I、J 分别标志原图像像素点坐标，i、j 分别标志加密图像像素点坐标；

(2) 生成像素点的行坐标 在行划分区间上进行 Logistic 映射迭代，如迭代值 $x_n\in[d_k^{(m)}, d_k^{(m+1)}]$，则 $g_{\mathrm{row},k}=g_{\mathrm{row},k}+1$，$i=|m-g_{\mathrm{row},k}| \bmod M$；若 $i\in\boldsymbol{V}_{\mathrm{row}}$，则 $\boldsymbol{V}_{\mathrm{row}}=\boldsymbol{V}_{\mathrm{row}}\cup\{i\}$，并生成行坐标 i，转步骤(3)；若 $i\notin\boldsymbol{V}_{\mathrm{row}}$，则继续执行步骤(2)；

(3) 生成像素点的列坐标 在列划分区间上进行 Logistic 映射迭代，如迭代值 $x_n\in[d_k^{(m)}, d_k^{(m+1)}]$，则 $g_{\mathrm{column},k}=g_{\mathrm{column},k+1}$，$j=|m-g_{\mathrm{column},k}| \bmod N$；若 $j\notin\boldsymbol{V}_{\mathrm{column}}$，则 $\boldsymbol{V}_{\mathrm{column}}=\boldsymbol{V}_{\mathrm{colunn}}\cup\{j\}$，生成列坐标 j，转步骤(4)；若 $j\in\boldsymbol{V}_{\mathrm{column}}$，则继续执行步骤(3)；

(4) 对原图像置乱 $B[i,j]=A[I,J]$，转步骤(5)；

即将原图像像素点 $A^{[I,J]}$ 移动到加密图像的 $B[i,j]$ 像素点上。

(5)
$$\begin{cases} J=J+1,\text{转步骤(3)} & I<M, J<N-1 \\ \boldsymbol{V}_{\mathrm{column}}=\{\}, I=I+1, J=0,\text{转步骤(2)} & I<M, J=N-1 \\ \text{转步骤(6)} & I=M \end{cases}$$

(6) 算法结束；

重新排列原图像像素点可以有多种方法，例如，按行优先遍历原图像像素点、按列优先遍历原图像像素点、按对角线优先遍历原图像像素点、按行优先隔点遍历原图像像素点等。本文算法选取的是按行优先遍历原图像像素点。

解密算法：只有第(4)步不同于加密算法，为 $A[I,J]=B[i,j]$，即将加密图像 $B[i,j]$ 像素点移动到解密图像的像素点 $A[I,J]$ 上。其他各步骤与加密算法相同。

3 衡量图像置乱的性能指标

本文选取和文献[7]相同的如下图像置乱性能指标：

(1) 时间特性

对于一个二维 $M\times N$ 像素的图像，L 为生成加密图像全部像素点坐标的两个 Logistic 映射的迭代总次数，显然迭代次数 L 越小，算法的运算速度越快。

(2) 不动点

如果原图像像素点经过置乱网络置乱后，像素点的行列坐标值没有发生变化，则称此像素点为不动点。若不动点的数目 k 越少，则说明置乱的效果越好，保密性也就越高。

(3) 自然序

如果相邻的像素点，其置乱后的行列地址虽然都发生变化，但仍然相邻，称之为自然序。自然序包括行自然序、列自然序、斜自然序、圆自然序。若置乱后图像的自然序越少，则置乱的效果越好，保密性也就越高。

(4) 二阶距[7]

$$\tau^{(2)}=\sum_{I=1}^{M}\sum_{J=1}^{N}((I-i)^2+(J-j)^2) \tag{5}$$

式(5)中，I，J 为原图像像素点的坐标，i，j 为经置乱后加密图像像素点的坐标。若二阶距 $\tau^{(2)}$ 越大，则说明经置乱后像素点总体的位移越大，即与原图像越不相关，置乱效果越好。

4 混沌二维图像的置乱性质

为了和文献[7]对比，在对二维 $M\times N$ 大小的图像置乱网络置乱性质进行统计分析时，采用和文献[7]相同的图像置乱性能指标和相同的初始条件，两个 Logistic 映射的初始值分别为 $x_0=i/100$ 和 $y_0=j/100$ 的 99×99 个点，其中 $0<i<100$、$0<j<100$。第 1 次划分取 $q_1=3$，第 2 次划分分别取 $q_2=M$ 和 $q_2=N$。

(1) 时间特性

表 1，表 2 中，$L_{\max}$ 为 L 的最大值，$L_{\min}$ 为 L 的最小值，$\bar{L}$ 为 L 的平均值，$\bar{L}=\bar{k}MN$。从表 1，表 2 可以

看出,本文算法的混沌映射平均迭代次数为 $M\times N$ 的 3.3～4.8 倍,因迭代次数比文献[7]算法大大减少,故算法运行的速度有很大提高。

表 1　文献[7]的时间(迭代次数)特性统计分析表

M	N	$L_{\max}$(次)	$L_{\min}$(次)	$\bar{L}$(次)	$\bar{k}$(个)
32	8	6990	1478	2910	11.4
	16	15080	3559	6610	12.9
	32	29974	8789	14706	14.9
64	8	14305	3769	6619	12.9
	16	30451	8638	14816	14.4
	32	60665	20737	32627	15.9
	64	119671	48218	71769	17.5

表 2　本文算法的时间(迭代次数)特性统计分析表

M	N	$L_{\max}$(次)	$L_{\min}$(次)	$\bar{L}$(次)	$\bar{k}$(个)
32	8	1069	665	839	3.3
	16	2241	1562	1877	3.7
	32	4814	3765	4294	4.2
64	8	2320	1438	1726	3.4
	16	4546	3292	3787	3.7
	32	9693	7739	8623	4.2
	64	21732	18335	19753	4.8

(2) 不动点

表 3 中数据说明,置乱后图像中不动点的个数仅占整个图像像素点的 0.1%～0.4%,可见达到了很好的置乱效果。

表 3　本文算法置乱图像不动点个数 k 统计分析表

M	N	$k_{\max}$(个)	$k_{\min}$(个)	$\bar{k}$(个)	$\lambda_{\max}$(个)	$\bar{\lambda}$(个)
32	8	10	0	1.220	0.0391	0.00476
	16	11	0	1.143	0.0214	0.00223
	32	10	0	1.146	0.0097	0.00112

表中,$\lambda_{\max}=\dfrac{k_{\max}}{M\times N}$,$\bar{\lambda}=\dfrac{\bar{k}}{M\times N}$。

(3) 自然序

表 4　本文算法置乱图像自然序 n 统计分析表

M	N	$n_{\max}$(个)	$\bar{n}$(个)	$\lambda_{\max}$(个)	$\bar{\lambda}$(个)
32	8	1.562	0.856	0.173	0.095
	16	0.773	0.483	0.086	0.054
	32	0.406	0.253	0.045	0.028

表 4 中,$\lambda_{\max}=\dfrac{n_{\max}}{9}$,$\bar{\lambda}=\dfrac{\bar{n}}{9}$,它们分别表示置乱图像的一个 3×3 方阵内出现自然序点的可能性大小。从表 4 可以看出,由于经置乱网络置乱后 3×3 方阵内出现的自然序个数只占整个数据点的 9%以下,且相邻的数据点基本都被拆散,从而达到了很好的置乱效果。

(4) 二阶距

表 5 中,$\tau_{\max}^{(2)}$、$\tau_{\min}^{(2)}$、$\bar{\tau}^{(2)}$ 分别是置乱后由式(5)计算得到的所有置乱图像的二阶距的最大值、最小值、平均值。

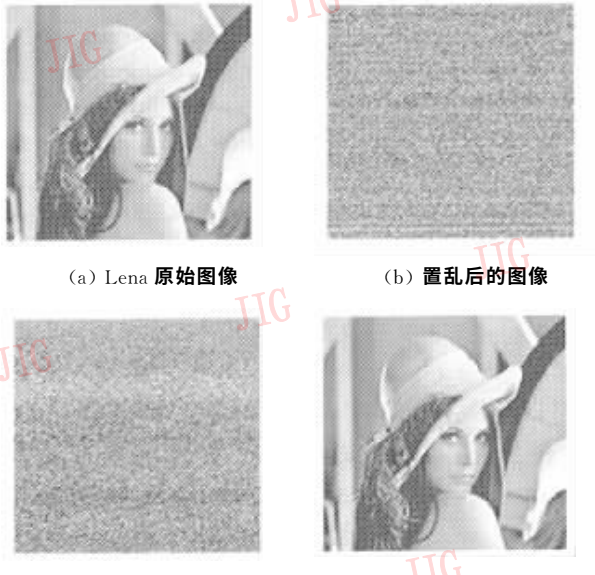
表 5　本文算法置乱图像二阶距统计分析表

M	N	$\tau_{\max}^{(2)}$	$\tau_{\min}^{(2)}$	$\bar{\tau}^{(2)}$
32	8	82250	26116	46691
	16	181820	66384	109406
	32	500604	200000	348635

从以上 5 个表中可以看出,图像置乱的性能指标——不动点、自然序、二阶距基本与文献[7]的指标相当,而本文算法的时间特性、复杂度却比文献[7]大大改善。

5　计算机模拟与结果分析

图 2 是利用本文提出的混沌置乱网络对 Lena 图像(256×256)加密置乱和解密的实验结果。两个 Logistic 映射的初始值分别为 0.2 和 0.3,第 1 次划分 $q_1=3$,第 2 次划分 $q_2=256$。图 2(a)是原图,图 2(b)是用置乱网络置乱后的图像,由该图可以看出,该图未保留原图像的任何轮廓;图 2(c)是在列划分的初始状态下将第 1 个转轮转动一格后的状态作为解密的初始状态而得到 的解密结果,由图 2(c)可见,转轮的初始状态略有不同,也无法正确解密出原图像;图 2(d)为密钥正确时解密出的图像,由图 2(d)可以看出,解密图像和原图像完全相同。



(a) Lena 原始图像　(b) 置乱后的图像

(c) 密钥略有不同时的解密结果　(d) 密钥正确时的解密结果

图 2　混沌置乱网络加密、解密实验结果

6 结 论

以上的模拟和分析结果表明，本文提出的混沌置乱网络比文献[7]的置乱网络在算法的运算速度上有了很大提高。在生成像素点的行列坐标过程中，由于每个转轮的转动是由混沌映射迭代驱动的，因而增加了算法对混沌映射初始值的敏感度。另外由于初始值、行列划分上的转轮数、每个转轮的初始状态、对原图像像素点的遍历方式等都可以是密钥，因而比文献[7]增加了密钥个数和密钥空间，这样就满足了图像置乱网络的密钥量要足够大、置乱网络要足够复杂、算法的运行速度要快等的要求。计算机模拟结果显示，该置乱网络置乱效果好，是一种适合于实际应用的良好的图像置乱算法。

参 考 文 献

1 卢朝阳，周幸妮. 一种新的数据信息置乱算法[J]. 计算机工程与科学，1998，**20**(3)：28～31.

2 吴旻升，王介生，刘慎权. 图象的排列变换[J]. 计算机学报，1998，**21**(6)：514～519.

3 丁玮，齐东旭. 数字图象变换及信息隐藏与伪装技术[J]. 计算机学报，1998，**21**(9)：838～843.

4 Matthews R. On the derivation of a ‘chaotic’ encryption algorithm[J]. Cryptologia，1989，**13**(1)：29～42.

5 Shi C，Bhargava B. Light-weight MPEG video encryption algorithm[A]. In：Proceedings of the International Conference on Multimedia’98[C]，New Delhi，India，1998：55～61.

6 Josef Scharinger. Fast encryption of image data using chaotic Kolmogorov flows [A]. In：Proceedings of Electronic Imaging’97，Security and Watermarking of Multimedia Contents [C]，San Jose，CA，USA，1997，**3022**：278～289.

7 秦红磊，郝燕玲，孙枫. 一种基于混沌的图象置乱网络的设计[J]. 计算机工程与应用，2002，**38**(7)：104～106.

8 孙鑫，易开祥，孙优贤. 基于混沌系统的图象加密算法[J]. 计算机辅助设计与图形学学报，2002，**14**(2)：1～4.

9 凌聪，孙松庚. 用于跳频码分多址通信的混沌跳频序列[J]. 电子学报，1999，**27**(1)：67～69.

刘云江 1970 年生，鞍山科技大学讲师，2003 年获鞍山科技大学硕士学位。主要研究领域为混沌分形信号处理、计算机图形、图像。

刘向东 1967 年生，大连民族学院计算机科学与工程系教授，2000 年获东北大学信息科学与工程学院博士学位。主要研究领域为混沌分形信号处理、计算机图形、图像。

王光兴 1937 年生，东北大学教授，博士生导师，国务院学科评议组成员。主要研究方向为网络与多媒体通信技术及信号处理。