基于 Logistic 映射的图像加密安全风险研究

章秀君[1],冯乔生[1],罗 可[1],方 正[2]
(1.云南师范大学 计算机科学与信息技术学院,云南 昆明 650092;
2.中国地质大学 工程学院,湖北 武汉 430074)

摘 要:通过分析 Logistic 映射所产生序列的随机特性,发现当 Logistic 映射用于图像加密时存在一些安全风险,即使 Logistic 映射的参数 $\mu \in (3.569\ 9\cdots,4]$ 时,此映射所产生的序列也并不总是呈现混沌状态,仍然存在一些周期窗口。为了避免当 Logistic 映射用于图像加密时的安全风险,提出了一些安全保障规则。

关键词:Logistic 映射;混沌序列;图像加密
中图分类号:TN911.73 **文献标识码**:A

Research of security risks in image encryption based on Logistic mapping

ZHANG Xiu Jun[1], FENG Qiao Sheng[1], LUO Ke[1], FANG Zheng[2]
(1.College of Computer Science and Information Technology, Yunnan Normal University, Kunming 650092, China;
2.Faculty of Engineering, China University of Geosciences, Wuhan 430074, China)

Abstract: The random features of the sequence generated by Logistic mapping are analyzed and the security risks are then found when a Logistic sequence is used for image encryption. Logistic sequence is not always chaotic even if the parameter $\mu \in (3.569\ 9\cdots,4]$ of Logistic mapping, there still exist a few periodic windows. Some rules are proposed in this paper for avoiding the security risks when Logistic mapping is used for image encryption.

Key words: logistic mapping; chaotic sequence; image encryption

随着互联网的发展,大量的敏感图像信息开始通过网络传输,同时也为不法分子利用网络获得未授权的信息提供方便,因此图像数据的安全变得更加严峻和必要。由于图像具有信息量大、相邻像素值相关性强等特点,传统的文本加密算法 DES、IDEA、RSA 等不能完全满足加密需要。

混沌理论的发展为图像加密提供了新思路。混沌是确定性系统,但由其产生的序列是伪随机的、不可预测的、在理想条件下具有无限大的周期,可以提供巨大的密钥空间、是非周期又不收敛的。更重要的是,混沌系统对初值变化极端敏感,即初始状态只有微小差别的两个同构混沌系统在短时间就会产生两组完全不同的、互不相关的混沌序列值。由于安全性高、加密速度快,基于混沌的图像加密技术得到了广泛的研究[1-9]。

目前按照变换方式的不同,基于混沌的图像加密可分为图像像素坐标变换和图像像素值变换加密方式两大类。其中,图像像素坐标变换的加密方式也称置乱方法,是通过一些混沌映射改变像素的坐标位置,从而使得图像杂乱无章,达到加密目的。用于这类的混沌映射主要有 Arnold 变换、Baker map[10]、Cat map[11]、Tent map 等。图像像素值变换的加密方式也称置混方法,是通过使用混沌系统生成伪随机流,将随机流直接掩盖明文,改变原图像各像素点的像素值,使攻击者无法辨认原始图像,从而达到对图像加密的目的。用于这类加密的混沌系统有 Logistic 映射、PWLCM 映射、Chebyshev 映射、Henon 映射、Lorenz 系统、Chen 系统等。Logistic 映射因具有实现简单的优势,可以设计出实现速度较快的密码系统而得到广泛的应用[2-5]。但 Logistic 映射不总是能产生混沌序列,如何保证 Logistic 映射产生出混沌序列是将 Logistic 映射用于图像加密的关键。另外,混沌系统是基

于实数集的，而加密在整型的离散集中进行，所以基于混沌的数字图像加密方法均需对混沌序列做取整形化处理，而这一处理会导致动力学特性的退化。因此，基于 Logistic 映射的图像加密还需要进一步的研究。本文通过分析 Logistic 映射所产生序列的随机特性，指出了这种混沌序列实际用于加密时存在的安全隐患问题以及避免这些加密安全隐患的规则。

1 Logistic 混沌映射

Logistic 映射是一种非常简单却被广泛应用的经典动力学系统，其模型可被定义如下：

$$x_{n+1}=f(x_n)=\mu x_n(1-x_n) \tag{1}$$

式中，$\mu\in(0,4]$，$x_n\in[0,1]$，解方程 $f(x_n)=\mu x_n(1-x_n)$ 得到 2 个平衡点：$x_1=0$，$x_2=1-1/\mu$。由于不动点线性部分的雅可比行列式 $J=\partial f/\partial x=\mu-2\mu x$，可知系统的稳定性取决于参数 μ。目前研究者已得出以下结论：

当 $1<\mu<3$，不管 x_0 取什么初值，在 $n\to\infty$，$x_n=1-1/\mu$ 是稳定的。

当 $3<\mu<3.449$，在 $n\to\infty$，式(1)存在 2 个平衡点。

当 $3.449<\mu<3.544$，在 $n\to\infty$，式(1)存在 4 个平衡点。

当 $3.544<\mu<3.564$，在 $n\to\infty$，式(1)存在 8 个平衡点。

随着 μ 值的增加，出现稳定的 $1,2,4,6,8,16,\cdots,2^n$ 周期点，但当 $\mu\in(3.569\ 9\cdots,4]$ 时则周期 2^n 轨迹不再存在，进入混沌区[2-3,6-7,12]。在这一混沌区具有对初值极端敏感和非周期等特点，所以常被研究者用来加密图像，并把初值 x_0 和参数 μ 用来当作密钥。

当 $\mu=4$ 时，式(1)进入最佳混沌状态而且序列值能填满[0,1]区间的实数，具有遍历性，是加密的最好参数取值[4]。

2 Logistic 混沌序列用于图像加密的安全隐患分析

2.1 Logistic 混沌序列的整型化问题

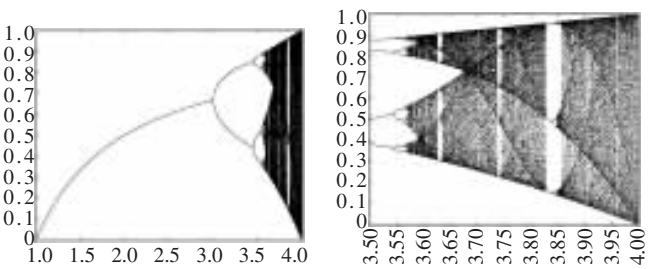
Logistic 产生的是 0~1 之间的实数，而图像值是一个整数。若先将图像像素值转为如参考文献[7]的实型，则会因为不同系统对浮点数运算的精度抖动，而出现在一个平台上加密无法在另一个平台解密的现象。若将实型混沌序列转为整型序列，则要将所有序列值扩大 K 倍。因为 Logistic 混沌序列很多小数点后前几个数都是相同的，如果扩大的倍数不够大，则混沌序列将丧失混沌性质，这时加密出来的图像是很不安全的。在 Logistic 模型中当 $\mu=4$ 时，完全呈现混沌状态而且序列值能填满[0,1]区间的实数，具有遍历性，是加密的最好参数取值[4]。但若在处理序列值实型转为整形时采用扩大倍数方式时，若扩大倍数 K 取值不够大，则加密效果极差。如图 1 加密效果对比中的图 1(a)是加密前的 Lena 原图，图 1(b)为 $\mu=4$、$K=100$ 时加密后的密图，从密图中仍可看到加密前 Lena 图的原始信息，并没有达到加密效果，此时混沌序列已丧失混沌特性。而当扩大倍数 K 的取值足够大时，则不会导致混沌特性丧失，如图 1(c)为 $\mu=4$、$K=10^5$ 的密图，它已是面目全非了，攻击者无法辨认原始图像，从而达到了对图像加密的目的。所以，参考文献[2]中将扩大倍数 K 作为密钥中的子密钥而又没有规定 K 的最小取值是不合理的做法，加密者可能会选到过小的 K 值而使混沌序列丧失混沌性，而导致加密算法的安全性无法得到保障。

(a)lena 原图　(b)$\mu=4$，$K=100$ 时密图　(c) $\mu=4$，$K=10^5$ 时密图

图 1 不同的整型化因子下的加密效果对比

2.2 Logistic 映射参数 μ 的取值与周期性窗口

目前学者认为，当 μ 进入 $(3.569\ 9\cdots,4]$ 区间时，Logistic 序列就进入混沌区[2-3,6-7,12]，但本文通过实验发现，当 μ 取 3.835 时只有 3 个稳定值，取 3.845 时有 6 个稳定值，经大量实现测试发现，μ 在 [3.828,3.875] 之间取值均存在周期性，μ 取 3.583、3.63、3.74 等也出现周期性。图 2(a)表示序列值 x_n 与参数 μ 在 1~4 之间的分岔图，此图还看不出参数 μ 在 $(3.569\ 9\cdots,4]$ 区间有周期窗口，但从图 2(b)x_n 值与参数 μ 在 3.5~4 之间的分岔图中则可清楚地看到：当 μ 进入 $(3.569\ 9\cdots,4]$ 区间内 μ 的取值处确实出现了一些周期性很强的窗口，即周期窗口。所以，虽然 $\mu\in(3.569\ 9\cdots,4]$ 属于混沌区域内，但并不意味着在这一区域仅存在混沌轨迹[10]，μ 在窗口中的取值使 Logistic 映射所产生的序列是周期性序列而不是混沌序列，因此，将该序列用于数字图像加密时会严重影响到加密的效果，算法加密的安全性完全无法保障，对图像进行置混后得到的加密图像都还可以看到原始图像的情况。如图 3 是采用了参考文献[2]中用到密码反馈机制的较好加密算法对 Lena 进行加密的密图，从密图仍可识别原图为 Lena 图。所以用 Logistic 映射加密图像时把 μ 作为子密钥是不合理的。



(a)μ 在 1~4 之间的分岔图　(b)μ 在 3.5~4 之间的分岔图

图 2 Logistic 映射分岔图

3 Logistic 映射用于图像加密规则

针对上述问题，本文给出避免加密安全隐患的 3 条规则：

μ=3.835 时密图　μ=3.828 时密图　μ=3.583 时密图

图 3　μ 取到周期点时加密效果图

规则 1：不能把参数 μ 作为密钥。2006 年，ALVAREZ G 和 LI Shu Jun 针对混沌密码学的安全要求提出了具有代表性的 17 条建议规则[13]中指出：密钥空间 κ 中的所有选择都应是有效的密钥，密钥空间 κ 应明确规定而且应避免非混沌区域。而本文上面已说明 $\mu \in (3.569\ 9\cdots, 4]$ 区间内存在着一些周期窗口，而 μ 的取值为实型，无法将所有呈现出周期性的点彻底排除在外。所以，为了保证算法的安全性不能把 Logistic 映射的参数 μ 作为密钥，加密算法应该确定 μ 的取值，保证整个映射具有很好的混沌特性。

规则 2：如果要把扩大倍数 K 作为密钥的一部分，为保证原混沌序列不丧失混沌学特性，应先求出 K 的最小取值 K_{min}，加密时明确规定 K 取值的下限为 K_{min}。

求解 K_{min} 的主要算法如下：

(1)确定式(1)中的 μ 值(保证该取值不在非混沌区)得到：

$$x_{n+1}=4x_n(1-x_n) \tag{2}$$

(2)用式(2)生成的混沌序列 1：

$x_0, x_1, x_2 \cdots x_i, x_j, \cdots x_n$

(3)排序得到序列 2：

$y_0, y_1, y_2, \cdots y_i, y_j, \cdots y_n$

(4) $y_k - y_{k+1}, k=0, 1, 2, \cdots, n$，即求序列 2 中两相邻值之差最小的值 min。

(5)计算出 min 的小数点到小数点后第 1 个非零数之间的零的个数 m，则 K_{min} 就为 10^{m+1}。

规则 3：用 Logistic 映射对图像进行置混加密时，应该与置乱方法结合。

随着计算机计算速度的增加，密码学的安全要求也越来越高，为了能抵抗蛮力攻击，密钥空间 κ 应该大于 2^{100} [13]。而若单独用 Logistic 映射进行加密，经上述分析不能把参数 μ 作密钥，就大大减小了密钥空间。若只用初值 x_0 作为密钥，从理论上有无限大的密钥空间，但由于当前计算机有效位数的限制，若取 15 位有效数的话，其密钥空间为 10^{15} 约为 $2^{50}<2^{100}$，无法满足当前的安全要求。所以用 Logistic 映射对图像进行置混加密时，应该与置乱方法结合来增加密钥空间以保障加密算法的安全性。本文建议与一些相对简单的置乱方法，如 Arnold 变换、Baker map 变换、Cat map 变换等相结合。因为现代密码学要求在不损失安全的前提下，加密系统的设计应尽可能地满足低成本和执行速度快的要求[11]。

本文总结了 Logistic 映射目前已有的一些结论，分析了在采用 Logistic 映射对图像进行加密时常被很多文献所忽略的一些安全隐患问题，并通过实验证实了这些安全隐患所带来的危害性。同时给出了避免加密安全隐患的 3 条规则，这 3 条规则对基于 Logistic 映射的数字图像加密能起到保证加密安全的作用。

参考文献

[1] PENG Jun, ZHU Shang. A novel scheme for image encryption based on piecewise linear chaotic map [C]. 2008 IEEE Conference on Cybernetics and Interlligent Systems, 2008: 1012-1016.

[2] 彭成等，柳林.基于混沌序列的压缩图像加密算法[J].计算机工程，2008，34(20):177-179.

[3] 刘树堂，孙福艳.基于空间混沌的图像加密设计[J]. 中国科学，2009，39(3):387-393.

[4] HONGE R, ZHENWEI S. A chaotic algorithm of image encryption based on dispersion sampling [C]//proceedings of the 8th International Conference on Electronic Measurement and Instruments, 2007:836-839.

[5] ZHANG Yun Peng, ZUO Fei, ZHAI Zheng Jun, et al. A new image encryption algorithm based on multiple chaos system [J]. International Symposium on Electronic Commerce and Security10.1109/ISECS, 2008, 142.

[6] 贺文华，朱从旭.基于双混沌映射的快速图像加密新算法[J].计算机工程与应用，2008，44(7):152-154.

[7] HONG Lian Xi, LI Chuan Mu. A novel color image encryption approach based on multi-chaotic system [C]//proceedings of the 2nd International Conference on Anti-counterfeiting, Security and Identification, 2008:223-226.

[8] PISARCHIK A, CARMONA N F, VALADEZ M C. Encryption and decryption of images with chaotic map lattices [J]. Chaos, 2006, 16(3).

[9] 蔺兢，吴立伟.基于混沌的图像空域复合加密方法的研究[J].电脑开发与应用，2008，21(9):29-31.

[10] SALLEH M, BRAHIM S I, ISNIN I F. Enhanced chaotic image encryption algorithm based on chaotic maps [C]. IEEE Conf Circuits and Syst, 2003:508-511.

[11] CHEN Guan Rong, MAO Yao Bin, CHARLES K C. A symmetric image encryption scheme based on 3D chaotic catmaps[J]. Chaos, Solitons & Fractals, 2004, 21(3):749-761.

[12] 丁文霞，卢焕章.基于混沌系统的独立密钥 DES 数字图像加密算法[J].计算机应用研究，2006(2):113-115.

[13] ALVAREZ G, LI S. Some basic cryptographic requirements for chaos-based cryptosystems [J]. chaos, 2006, 16: 2129-2151.

(收稿日期：2009-10-12)

作者简介：

章秀君，女，1984 年生，硕士研究生，主要研究方向：图像加密、信息安全。

冯乔生，男，1961 年生，教授，主要研究方向：机器视觉、虚拟现实技术。