文章编号: 1001- 2486(2007) 03- 0045- 05

对一种混沌加密图像方法的破译研究*

黎 全[1], 赵 凯[2], 邓正才[1], 何焰兰[1], 吕治辉[1], 黄水花[1]
(1. 国防科技大学 理学院, 湖南 长沙 410073; 2. 西安交通大学 材料科学与工程学院, 陕西 西安 710049)

摘 要: 介绍了利用混沌映射系统进行保密通信的理论依据。分析了一种利用混沌动力学方程所形成的混沌序列来对图像进行加密的方案, 并用程序语言予以实现。针对这种一维混沌加密算法, 在加密方程、参数和初始值完全未知的前提下, 运用相空间重构法和穷举法对其进行了破译研究并成功将其破译。总结了加密和破译方法的优缺点, 提出了一种抗破译能力更强的加密方案。

关键词: 混沌; 时间序列; 破译; 相空间重构; 自相关函数; 穷举法
中图分类号: TP391 文献标识码: A

Research on Deciphering Method of a Kind of Chaotic Encrypting Picture

LI Quan[1], ZHAO Kai[2], DENG Zheng-cai[1], HE Yan-lan[1], LV Zhi-hui[1], HUANG Shui-hua[1]
(1. College of Science, National Univ. of Defense Technology, Changsha 410073, China;
2. School of Material Science and Engineering, Xi' an Jiaotong University, Xi' an 710049, China)

Abstract: The chaotic encryption system which makes use of chaos mapping system to carry on the secret correspondence is introduced. The method which makes use of the chaos dynamics equation to carry on encrypting to pictures is put forward and realized with the program. For the one-dimension chaotic encryption method, it is successfully deciphered by the phase-space reconstruction theory and exhaustive method with the encryption function, parameter and the original value completely unknown. In the end, the advantages and the disadvantages of the encrypting and deciphering methods are discussed and a kind of encrypting project which is more difficult to be deciphered is put forward.

Key words: chaos; time series; decipher; phase-space reconstruction; autocorrelation function; exhaustive method

1983 年, 美国加州大学伯克利分校的 Tang 等学者率先探讨了混沌理论在安全通信中引用的可能性。美国麻省理工学院、加州大学伯克利分校、瑞士联邦工学院等研究机构于 1992~ 1993 年各自采用掩盖、混沌开关、混沌调制等方法验证了混沌保密机的可行性。1993 年, IEEE 的高级会员 Douglas. R. Frey 提出数字或准混沌保密通信这一重要概念, 开辟了数字混沌保密通信领域[1-2]。混沌安全通信现已成为一个令人激动和富有挑战性的热门话题, 大量的新思想和算法不断涌现。在实际应用中, 由于运算速度的限制, 一维混沌系统加密是常用的方法, 然而对其保密性缺乏理论探讨, 也难以有针对性地提出改进方案, 本文基于这种现状结合相空间重构和穷举法对一维混沌加密系统进行了破译研究。

1 混沌在图像加密中的应用

1.1 混沌加密的理论依据

混沌的自相似性, 使得局部选取的混沌密钥集在分布形态上都与整体相似。混沌系统对初始状态高度的敏感性, 复杂的动力学行为, 分布上不符合概率统计学原理, 使混沌系统难以预测[3-5]。由于混沌迭代序列信号具有高度随机性, 经过一定处理后的混沌信号具有准周期运动的特点, 可以高效产生密钥流。但更重要的是, 通过混沌系统对初始值和参数的敏感依赖性, 可以提供数量众多的密钥。

* 收稿日期: 2007- 01- 20
基金项目: 国家自然科学基金资助项目(10504043)
作者简介: 黎全(1976—), 男, 讲师, 博士。

Logistic 混沌系统是一种经典的混沌映射。其中以虫口模型为例,它的映射公式为:

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

当取 $x_0 = 0.314$, $u = 3.8$ 时,选取其前 300 个点,得到的混沌时间序列图如图 1 所示。

由图 1 中可以看出,Logistic 系统虫口模型序列的数值分布在0~ 1,是数据起伏非常大的准周期运动,非常适合用来加密。

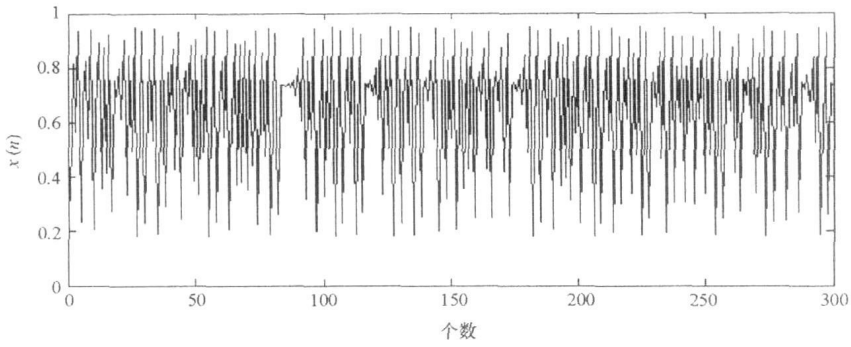

图 1 逻辑映射时间序列图

Fig. 1 Time series of logistic mapping system

1.2 图像加密

利用 Logistic 系统中的虫口模型公式,以列为顺序,对图像的像素值乘以对应的混沌序列值进行加密。取参数 $x_0 = 0.618$, $u = 3.825$ 对图像进行进行加密和解密,其效果如图 2 和图 3。

图 2 原图

Fig. 2 Original picture

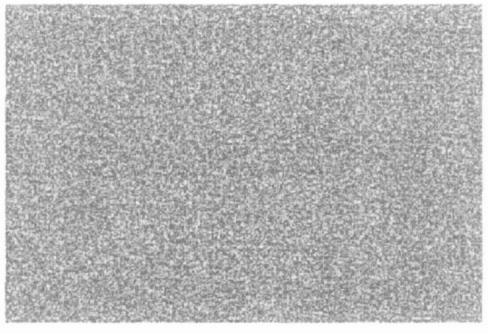

图 3 加密后图像

Fig. 3 Encrypted picture

这是一种利用混沌动力学系统所形成的单变量时间序列来进行加密的方法。本文主要工作就是对这种加密方法进行破译。

2 相空间重构

2.1 相空间重构原理

由于混沌加密是图像像素与对应的混沌序列值进行运算而形成密文,明文图像的像素值的起伏比较缓和,混沌序列的起伏却比较大(如图 1 所示),所以相乘所形成的密文的像素值在数据特征上必然保留着所使用的混沌方程的特点。只要将密文的相空间图重构出来,然后和各种混沌动力学方程的原始相空间图进行比对,找出动力学特征最相似的那一个,就可以确定加密者使用的是哪一种动力学方程。

要恢复原系统的相空间图,应首先对系统输出的单一变量的时间序列进行相空间重构。20 世纪 80 年代,Takens 在 Whitney 早期拓扑学方面工作的基础上,提出著名的 Takens 定理[6]。该定理是相空间重构的理论基础,揭示了某些非线性系统的动力学机制。Takens 研究的是一族时滞坐标映射,它是对实验中得到的单一观测量的时间序列进行重构。Takens 定理表明,可以寻求合适的嵌入维,并在嵌入维空间中恢复诸如吸引子等规则性的轨迹。这个过程实际上就是相空间重构[7-9]。将长度为 N 的单变量时间序列 $x_1, x_2, x_3, \cdots, x_N$ 通过延迟时间 τ 生成 N_m 个 m 维向量,构造出 m 维相空间,每一个 m 维向量都是重构相空间中的点 $Z_1, Z_2, Z_3, \cdots, Z_{N_m}$。

$$\begin{cases} \boldsymbol{Z}_1 = (x_1, x_{1+\tau}, x_{1+2\tau}, \cdots, x_{1+(m-1)\tau}) \\ \boldsymbol{Z}_2 = (x_2, x_{2+\tau}, x_{2+2\tau}, \cdots, x_{2+(m-1)\tau}) \\ \vdots \\ \boldsymbol{Z}_{N_m} = (x_{N_m}, x_{N_m+\tau}, x_{N_m+2\tau}, \cdots, x_N) \end{cases} \tag{2}$$

这样 $\boldsymbol{Z}_n$ 就可以用来表示系统在各时刻的动力学状态, 其中 $N_m = N-(m-1)\tau$。嵌入维数 m 和延迟时间 τ 是两个决定重构相空间质量的重要参数。

可以将式(2)中对应的列向量记为:

$$\boldsymbol{y}_n = (x_{1+n\tau} \quad x_{2+n\tau} \quad x_{3+n\tau} \quad \cdots \quad x_{N_m+n\tau})^{\mathrm{T}} \tag{3}$$

则以 y_n 和 $y_{n+\tau}$ 分别为横坐标和纵坐标, 做出其图形, 即为取延迟时间为 τ 时该时间序列所重构的相空间图。

2.2　线性自相关函数法确定 τ

延迟时间 τ 是相空间重构过程中的一个重要参数, 选择的延迟时间如果太大, 时间序列的任意两个相邻延迟坐标点将毫不相关, 不能反映整个系统的特性, 而延迟时间选择过小的话, 时间序列的任意两个相邻延迟坐标点又非常接近, 将会导致数据的冗余。自相关函数能够提供信号自身与它的延迟时间由冗余到不相关的关系, 从而来选取合适的延迟时间。

记 $\bar{x} = \frac{1}{N}\sum_{n=1}^{N} x_n$, 则

$$C_L(\tau) = \left[\sum_{n=1}^{N-\tau}(x_n - \bar{x})(x_{n+\tau} - \bar{x})\right] \Big\backslash \sum_{n=1}^{N-\tau}(x_n - \bar{x})^2 \tag{4}$$

$C_L(\tau)$ 被称为线性自相关函数。延迟时间 τ 的选取原则是让时间序列内元素之间的相关性减弱, 同时又要保证时间序列包含的原系统的信息不会丢失。研究表明, 当线性自相关函数 $C_L(\tau)$ 的值第一次为 0, 或者第一次接近于零时, 所对应的延迟时间 τ 比较合适[10]。

3　实 验

3.1　重构加密方程

下面以所截获的密文为研究对象, 首先选取其前 500 个像素点, 来进行线性自相关函数 $C_L(\tau)$ 的计算, 其计算结果如表 1。

表 1　线性自相关函数 $C_L(\tau)$ 值的变化

Tab. 1　Numerical variety of linear autocorrelation function $C_L(\tau)$

τ	1	2	3	4
$C_L(\tau)$	−0.4573	0.0226	0.3832	−0.1483

计算表明 $\tau=2$ 时, $C_L(\tau)$ 的值第一次接近于零, 为 0.0226。故只有当取 $\tau=2$ 时重构出的相空间图才能最好地保持原系统的动力学特征。为了更简单地重构, 选取 $m=2$, $\tau=2$, 利用所截获的密文的前 500 个点可以重构出它的相图, 如图 4, 当取 $\tau=2$ 时, 各混沌系统的原始相空间图如图 5~9。

根据与所画出的各系统的原始相空间图进行相关性分析, 可以发现图 4 与图 7(即通过密文重构出的相空间图与 Logistic 混沌系统的虫口模型的原始相空间图) 的图像相关度最大, 也就是说它们拥有最相似的动力学特征。由此可以断定加密所使用的混沌动力学系统公式为 Logistic 混沌系统的虫口模型映射公式:

$$x_{n+1} = ux_n(1-x_n) \tag{5}$$

3.2　确定参数与初值范围

在加密算法中, 是以列为顺序对各像素点的像素值乘以对应的混沌序列值, 从而形成了密文。那么

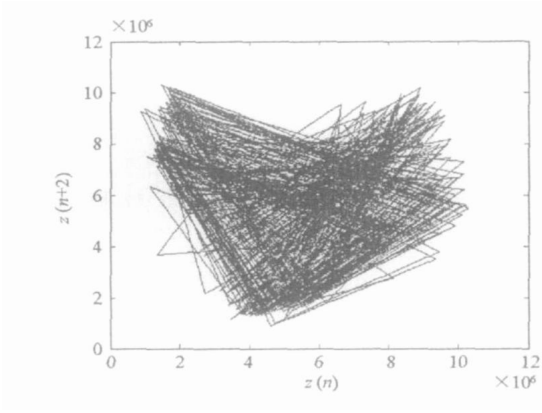

图 4 通过密文重构出的相空间
Fig. 4 Phase-space reconstruction by cryptograph

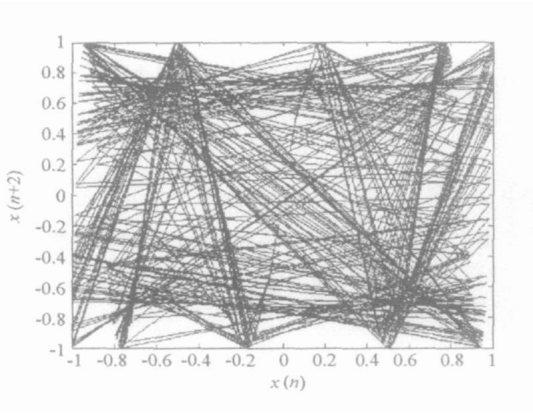

图 5 立方映射系统的相空间
Fig. 5 Phase-space of cubic mapping

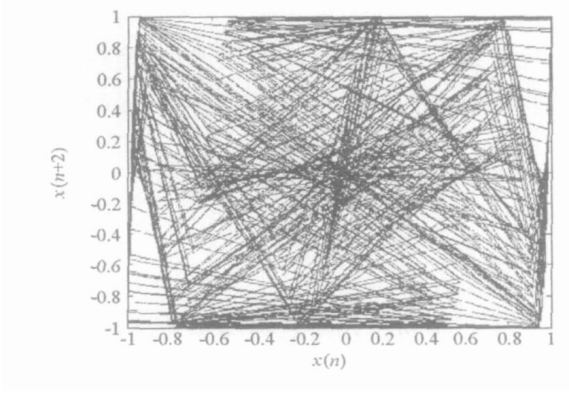

图 6 Chebyshev 系统的相空间
Fig. 6 Phase-space of Chebyshev mapping

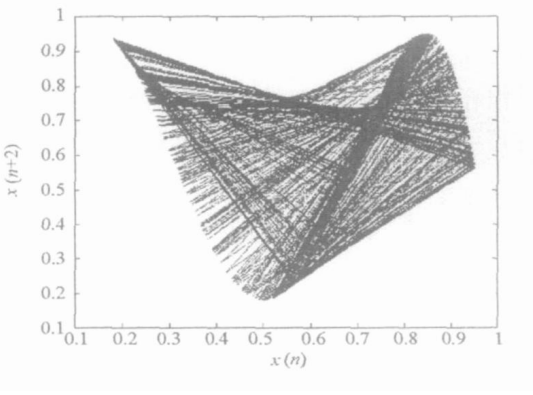

图 7 Logistic 系统虫口模型的相空间
Fig. 7 Phase-space of mapping $x_{n+1}= ux_n(1- x_n)$

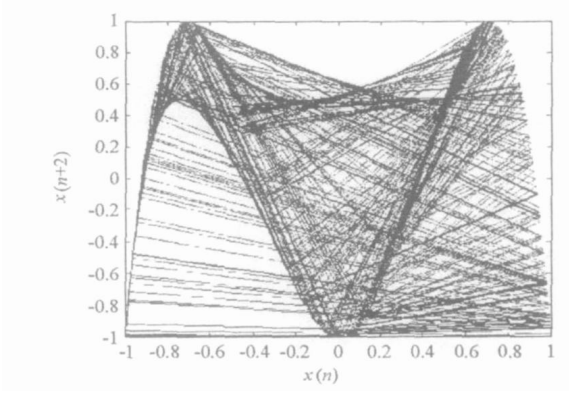

图 8 Logistic 映射 $x_{n+1}= 1- ux_n^2$ 的相空间
Fig. 8 Phase-space of mapping $x_{n+1}= 1- ux_n^2$

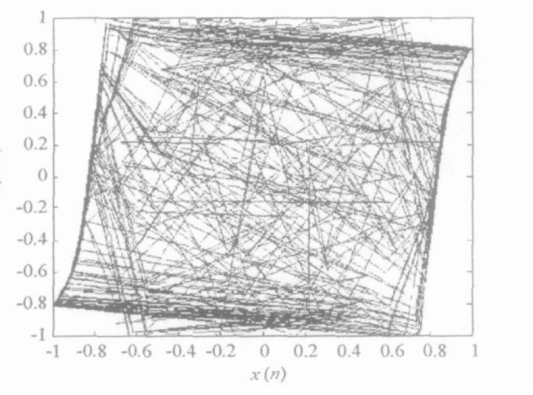

图 9 ICMIC 映射的相空间
Fig. 9 Phase-space of ICMIC mapping

就可以将明文图像中连续着的三个像素点的值分别记为: y_n, y_{n+1}, y_{n+2}(其中 n 代表像素点的顺序), 则与其对应相乘的混沌序列值可以记为: x_n, x_{n+1}, x_{n+2}。同样将在密文图像上读取的在位置上与明文相对应的连续着的三个像素点的值记为: z_n, z_{n+1}, z_{n+2}。依据加密原理可以得到关系式:

$$\begin{cases} y_n x_n = z_n \\ y_{n+1} x_{n+1} = z_{n+1} \\ y_{n+2} x_{n+2} = z_{n+2} \end{cases} \tag{6}$$

已知 $x_{n+1}= ux_n(1- x_n)$, 由于明文图像的像素值是渐变的, 所以可以近似地认为 $y_n \approx y_{n+1} \approx y_{n+2}$, 联立解方程组, 得到计算 u 的公式:

$$u=\frac{z_n^2 z_{n+2}-z_{n+1}^3}{z_n z_{n+1}(z_n-z_{n+1})} \tag{7}$$

可以看到, 利用这个公式, 只要在密文图像上连续地选取三个像素点的值, 就可以计算出一个 u 值。在所截获的密文图像上, 本文随机选取了 10 处连续的三个像素点, 利用式(7)进行数据处理, 得到 10 个 u 的值, 如表 2 所示。

表 2　实验得到的 10 个 u 参数样本

Tab. 2　10 numerical samples of the parameter u

3.794177	3.802357	3.856016	3.795449	3.831886
3.821270	3.804458	3.860728	3.787859	3.855792

从计算出的这组数据中, 可以发现所计算出的 u 的值在 3.787859~3.860728 之间波动。这也就是我们所确定的加密时所取的 u 的范围, 均值为 $\bar{u}=3.820999$。

在确定的 u 的大致范围以后, 就可以利用 u 的值来确定初始值 x_0 的大致范围。对于明文图像中的前两个点的加密过程, 同样可以得到如下关系式:

$$y_0 x_0=z_0,\quad y_1 x_1=z_1 \tag{8}$$

由于明文像素值是渐变的, 假设 $y_0\approx y_1$ 成立, 再将 $x_1=ux_0(1-x_0)$ 代入式(8), 则可以推导出计算初始值 x_0 的公式

$$x_0=1-z_1\backslash uz_0 \tag{9}$$

3.3　利用穷举法破译

使用以上方法, 从 $\bar{u}=3.820999$ 开始在区间[3.787859, 3.860728]内以 10^{-6} 为步长进行搜索, 直到所选取的几个像素组合符合渐变要求, 则表明破译成功。这就是穷举法确定参数 u 和初始值 x_0 的思路过程。实验中经过 10 000 次搜索, 耗时约 100s, 当取到 $x_0=0.618000$ 与 $u=3.825000$ 时, 将其共同代入解密程序中运行后得到了清晰的明文图像, 如图 10 所示。

图 10　破译图像

Fig. 10　Deciphering picture

4　结束语

简单的一维混沌加密方法是实际应用中易于实现且应用较多的方法, 本文针对这种图像加密模式结合相空间重构和穷举法进行了破译研究, 取得了较好的效果。同时应指出影响该破译方法效率的因素主要取决于运算器的精度。提高保密性方法有多种, 我们认为即使仍然采用一维混沌系统进行加密, 如果采取以下两种简单的改进方法也能大大提高保密性能: (1)同一系统变参数加密; (2)分时映射多刀开关法, 即在不同的时间域内使用不同的映射关系式。这两种方法能极大地增加破译的难度, 而对通信方运算难度和速度的影响很小。

参 考 文 献:

[1] Pareek N K, Patidara V, Sud K K. Discrete Chaotic Cryptography Using External Key[J]. Physics Letters A, 2003, 309: 75-82.

[2] Baptista M S. Cryptography with Chaos [J]. Physics Letters A, 1998, 240: 50-54.

[3] 郝柏林. 从抛物线谈起——混沌动力学引论[M]. 上海: 上海科技教育出版社, 1995.

[4] Gleick J. 混沌学——一门新学科[M]. 张彦, 等译. 北京: 社会科学文献出版社, 1992.

[5] 关新平, 范正平, 等. 混沌控制及其在保密通信中的应用[M]. 北京: 国防工业出版社, 2002.

[6] Edpr E P. Chaos and Order in the Capital Market [M]. New York: John Wiley & Sons, Inc., 1996.

[7] 王卫宁, 等. 股票价格波动的混沌行为分析[J]. 数量经济技术经济研究, 2004(4): 141-147.

[8] 吕金虎, 路军安, 陈士华. 混沌时间序列分析及其应用[M]. 武汉: 武汉大学出版社, 2002.

[9] 马军海. 复杂非线性系统的重构技术[M]. 天津: 天津大学出版社, 2005.

[10] 马红光, 等. 相空间重构中嵌入维和时间延迟的选择[J]. 西安交通大学学报, 2004, 38: 335-338.