文章编号:1001 - 9081(2010)11 - 3038 - 02

基于分段非线性混沌映射的流密码加密方案

罗松江,朱路平
(仲恺农业工程学院 信息学院,广州 510225)
(luosongjiang@126.com)

摘 要:基于分段非线性混沌映射设计了一种流密码加密方案。用 Logistic 映射的输出作为分段非线性映射的分段参数,以 Henon 映射输出的混沌序列经运算后得到迭代次数,分段非线性混沌映射的输出与明文相加取模后生成密文。仿真实验和安全性分析表明,该方案的密钥空间大,对明文和密钥敏感,能有效抵抗穷举攻击、差分攻击和统计攻击,且实时性较好。

关键词:多混沌系统;流密码;加密
中图分类号: TP309;TP301.6 **文献标志码**:A

Stream cipher encryption scheme based on piecewise nonlinear chaotic map

LUO Song-jiang, ZHU Lu-ping
(*School of Information, Zhongkai University of Agriculture and Engineering, Guangzhou Guangdong* 510225, *China*)

Abstract: A stream cipher encryption scheme was designed based on piecewise nonlinear chaotic map. The control parameter and iteration numbers of piecewise nonlinear chaotic map was produced by Logistic map and Henon map after the computation, and its outputs were added to the plaintext with modulus to obtain the ciphertext. The simulation and security analysis indicate that the proposed scheme possesses large key space, and has high sensitivity to plaintext and key. It can fight against brute-force attack, differential attack, and statistical attack efficiently, which also has excellent real-time characteristics.

Key words: multi-chaotic system; stream cipher; encryption

0 引言

利用混沌系统的确定性、长期不可预测性和对初值的敏感性来构造各种混沌密码算法已引起人们广泛的研究兴趣[1-6]。然而,由于用计算机实现混沌系统时的动力学特性退化问题,用单一混沌系统实现的密码算法是不够安全的。因此,用传统加密和混沌加密级联[2]、高维混沌系统[3]或多混沌系统[4]实现密码算法是提高密码系统安全性的有效措施。

本文提出一种基于分段非线性混沌映射的流密码加密方案。方案中用 Logistic 映射的输出作为分段非线性混沌映射的分段参数,用 Henon 映射迭代产生的混沌序列经运算后得迭代次数,分段非线性映射的输出与明文相加取模后生成密文。以图像加密为例进行了仿真实验和安全性分析。

1 混沌流密码加密方案设计

1.1 分段非线性混沌映射

分段非线性混沌映射方程为[5]:

$$\varphi(x,\alpha) = \frac{\alpha^2 F}{1+(\alpha^2-1)F} \tag{1}$$

$$F = \begin{cases} x/p, & 0 \leqslant x \leqslant p \\ (x-p)/(1-p), & p < x \leqslant 1 \end{cases} \tag{2}$$

其中:α 为控制参数,分段参数 $p \in [0,1]$。相应的不变测度为[5]:

$$\mu(x,\alpha,p) = \frac{1-\alpha}{\ln\left(\frac{1-p}{\alpha-p}\right)} \times \frac{1}{(\alpha-p)+(1-\alpha)x};\ \alpha > p$$

当 $p = 0.1$ 时,分段非线性混沌映射的分形图见图 1。

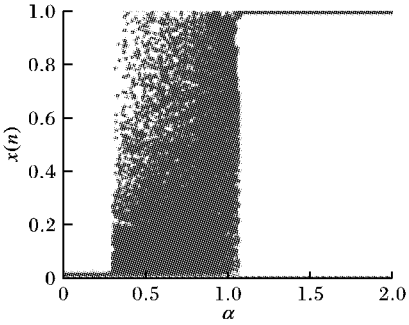


图 1 分段非线性混沌映射的分形图

1.2 流密码加密算法

流密码加密方案如图 2 所示。

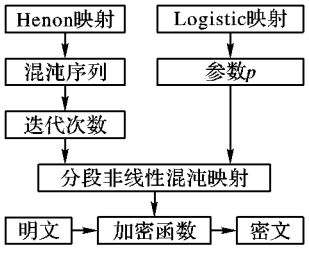


图 2 加密算法框图

设明文长度为 h。由 Logistic 映射:$y_{n+1} = \mu y_n(1-y_n)$,$\mu = 4$,给定初值 $y(0)$,迭代得 $y_i \in [0,1]\ (i = 1,2,\cdots,h)$,以此作为分段非线性混沌映射的参数 p_i,显然,p_i 为一混沌序列;再由 Henon 映射:$z_n = 1 + bz_{n-2} - 1.4z_{n-1}^2$,$b = 0.3$,给定初

收稿日期:2010 - 04 - 07;**修回日期**:2010 - 07 - 10。 **基金项目**:仲恺农业工程学院校级科研项目(G3100018)。
作者简介:罗松江(1973 -),男,湖南隆回人,讲师,博士,主要研究方向:混沌保密通信。

值 $z(0)$,得 $z(i) \in [0,1]$ $(i = 1,2,\cdots,h)$。通过式(3)得到分段非线性混沌映射的迭代次数:

$$m_i = 3 + \text{round}(h \times z_i) \bmod 20;\ i = 1,2,\cdots,h \tag{3}$$

给定控制参数 α 和初值 $x(0)$,对每一个分段参数 p_i,迭代分段非线性混沌映射 m_i 次,得到混沌密钥流 k_i $(i = 1,2,\cdots,h)$。

加密函数定义为:

$$C_i = \left(\left\lfloor k_i \times 10^{14} \right\rfloor + P_i\right) \bmod 256 \tag{4}$$

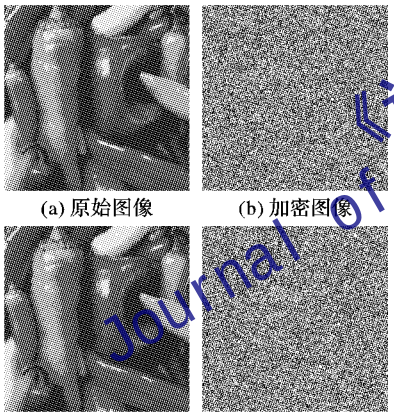
解密过程类似于加密过程。在得到和加密过程同样的密钥流后,解密函数定义为:

$$P_i = \left(C_i - \left\lfloor k_i \times 10^{14} \right\rfloor\right) \bmod 256 \tag{5}$$

该流密码加/解密方案中应用了3个混沌映射。通过分段参数和迭代次数的混沌变化,增强了由分段非线性混沌映射迭代得到的密钥流的安全性,同时一次一密的特点也增加了攻击的难度。

2　算法仿真

对分辨率为 512 × 512 像素的 Peppers. tif 灰度图像进行算法仿真实验。仿真环境为:PC 机的 CPU 为 P4 2.4 GHz,512 MB 内存,80 GB 硬盘空间,软件用 Matlab 7.1 实现。混沌系统的初值分别取 $x(0) = 0.1$, $y(0) = 0.2$, $z(0) = 0.3$,控制参数 $\alpha = 0.4$。仿真结果见图 3。



(a) 原始图像　(b) 加密图像

(c) 正确解密图像　(d) 错误解密图像

图 3　图像的仿真结果

用本文算法与文献[4]的算法进行加解密速度比较,实验结果如表 1 所示。仿真时也可采用离线生成密钥流的方法进一步提高加/解密速度,说明该方案有较好的实时性。

表 1　加解密速度比较

图像及大小	本文算法		文献[4]算法	
	加密时间/s	解密时间/s	加密时间/s	解密时间/s
Boats (256 × 256)	0.039	0.033	0.048	0.039
Peppers (512 × 512)	0.068	0.061	0.085	0.074

3　安全性分析

3.1　密钥空间分析

加密方案的安全性依赖于密钥的安全。本文研究的流密码加密方案的可能密钥为:混沌系统的初值 $x(0)$、$y(0)$ 和 $z(0)$;混沌系统的参数 α、μ 和 b;分段非线性混沌映射的迭代次数 m。仿真实验表明,仅改变上述任何密钥的一位,都会导致解密图像的完全不可辨识。如将 Logistic 映射的初值由 0.2 变为 0.200 000 000 001,相应的解密结果如图 3(d)所示。可见,该加密方案的密钥空间足够大且对密钥敏感,可抵御可能的穷举攻击。

3.2　抗统计攻击分析

Shannon[7] 建议通过加强扩散和混淆抵抗基于统计分析的攻击,文献[7]中的统计分析表明,扩散与混淆特性对统计分析具有较强的抵抗力。从原始图像与加密图像的直方图(见图 4)可看出,加密图像的直方图具有较好的均匀特性,攻击者难以利用像素灰度值的统计特性恢复原始图像,说明该流密码加密方案具有抗统计攻击的能力。

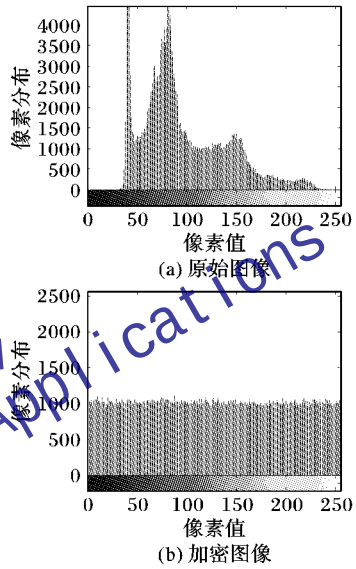


图 4　直方图分析

3.3　抗差分攻击分析

攻击者可能通过对明文图像做微小修改来观察解密结果的变化,并可能由此发现原始图像和解密图像的联系来得到正确解密结果。但若加密过程中明文图像的微小变化即导致密文图像的较大变化,则这种差分攻击的效果就会大大降低。

通常用两个参数来描述这种变化,即像素数目改变率(Number of Pixels Change Rate, NPCR)和归一化平均改变强度(Unified Average Changing Intensity, UACI)[6]。设原始图像的相应加密图像为 C_1,改变原始图像的一个像素灰度值后得到的加密图像为 C_2,令 C_1 和 C_2 在像素点 (i,j) 处的灰度值分别为 $C_1(i,j)$ 和 $C_2(i,j)$,有:

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases}$$

NPCR 和 *UACI* 定义为:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{m \times n} \times 100\%$$

$$UACI = \frac{1}{m \times n} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%$$

其中 m 和 n 分别为图像的水平像素数目和垂直像素数目。可见 *NPCR* 反映两图像间不同像素的多少,*UACI* 反映两图像间灰度差值的情况。对两幅完全随机的图像,*NPCR* 和 *UACI* 的理论值分别为99.609375% 和33.46354%[6]。设原始图像的

(下转第 3043 页)

结果表明本文算法只需要很小的位图,甚至不需要位图;即使需要位图,相对于负载来说它的大小也可以忽略不计。

表 1　测试图像的位图大小和负载

负载(比特/像素)	丽娜($T=16$)			狒狒($T=32$)		
	阈值		位图	阈值		位图
	T_n	T_p	比特	T_n	T_p	比特
100 Kb/0.38	2	1	0	−2	2	0
150 Kb/0.57	−3	3	0	−6	5	2
200 Kb/0.76	−5	5	0	−9	8	115
220 Kb/0.83	−6	6	2	−15	15	1 253
230 Kb/0.87	−8	7	6	−25	25	5 602
250 Kb/0.95	−12	12	9	—	—	—

表 2　丽娜图像用不同算法嵌入的容量和失真度对比

容量/(比特/像素)	失真度		
	本文算法	文献[4]算法	文献[8]算法
0.10	57.35	53.68	48.89
0.20	52.86	47.67	44.93
0.30	48.75	45.03	42.31
0.40	46.35	43.84	39.87
0.50	43.67	41.63	37.85
0.60	42.71	36.87	34.86
0.70	38.90	36.21	34.64
0.80	37.56	35.67	32.57
0.90	36.83	34.53	32.74
1.00	—	—	—

4　结语

本文的可逆水印算法是一些高效算法和一些性能良好的新技术的综合。使用一种新的基于高效排序的全邻预测算法:一个经过排序以后的预测误差集合,可以在保持很低的失真度的情况下嵌入数据。实验的结果表明,本文算法优于 Thodi、Vasiliy Sachnev 等人[4,8]的算法。在可逆水印中增加嵌入容量,以及减少失真度方面进行了一些有益的研究和探索。

参考文献:

[1] BARTON J M. Method and apparatus for embedding authentication information within digital data: US, 5646997[P], 1997-07-01.

[2] TIAN J. Reversible watermarking by difference expansion [C]// Multimedia and Security Workshop at ACM Multimedia. New York: ACM Press, 2002: 19-22.

[3] ALATTAR A M. Reversible watermark using difference expansion of triplets [C]// ICIP 2003: 2003 IEEE International Conference on Image Processing. Washington, DC: IEEE, 2003: I-501-4.

[4] SACHNEV V, KIM H J, NAM J, *et al*. Reversible watermarking algorithm using sorting and prediction [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2009, 19(7): 989-999.

[5] THODI D M, RODRIGUEZ J J. Reversible watermarking by prediction-error expansion [C]// 6th IEEE Southwest Symposium on Image Analysis and Interpretation. Washington, DC: IEEE, 2004: 21-25.

[6] CHANG C C, LU T C. A difference expansion oriented data hiding scheme for restoring the original host images [J]. The Journal of Systems & Software, 2006, 79(12): 1754-1766.

[7] KAMSTRA L, HEIJMANS H. Reversible data embedding into images using wavelet techniques and sorting [J]. IEEE Transactions on Image Processing, 2005, 14(12): 2082-2090.

[8] THODI D M, RODRIGUEZ J J. Expansion embedding techniques for reversible watermarking [J]. IEEE Transactions on Image Processing, 2007, 16(3): 721-730.

[9] YANG BIAN, MARTIN S, WOLFGANG F, *et al*. Integer DCT-based reversible watermarking for images using companding technique [C]// Proceedings of the SPIE, 2004, 5306: 405-415.

[10] WANG XIAOTONG, SHAO CHENGYONG, XU XIAOGANG, *et al*. Reversible data-hiding scheme for 2-D vector maps based on difference expansion [J]. IEEE Transactions on Information Forensics and Security, 2007, 2(3): 311-320.

[11] 张志明,周学广. 采用奇异值分解的数字水印嵌入算法[J]. 微计算机信息, 2006, 7(2): 69-71.

[12] LEE S, YOO C D, KALKER T. Reversible image watermarking based on integer-to-integer wavelet transform [J]. IEEE Transactions on Information Forensics and Security, 2007, 2(3): 321-330.

[13] 陈开英,胡永健,李建伟. 利用差值扩展进行可逆数据隐藏的新算法[J]. 计算机应用, 2008, 28(2): 455-459.

[14] 田华伟,赵耀,倪蓉蓉. 一种抵抗插值误差的数字水印方法[J]. 解放军理工大学学报:自然科学版, 2009(3): 242-247.

(上接第 3039 页)

第一个像素的灰度值为 p_1,改变其值为 p'_1,即 $p'_1=(p_1+100) \bmod 256$,其他像素的灰度值保持不变。得到两幅相应的加密图像,计算其 *NPCR* 和 *UACI* 分别为 99.51% 和 33.38%,非常接近其理论值,说明该加密方案有较强的抵御差分攻击的能力。

4　结语

本文提出了一种新的基于分段非线性映射的混沌流加密方案,该方案以 Logistic 映射的输出作为分段参数,以 Henon 映射的输出经运算后得到迭代次数,分段非线性映射的输出与明文相加取模后得到密文,提高了密文的不可预测性。安全性分析表明该方案的密钥空间大,可抵抗利用统计特性、差分特性进行的攻击,并具有较好的实时性。

参考文献:

[1] ZHANG LINHUA, LIAO XIAOFENG, WANG XUEBING. An image encryption approach based on chaotic maps[J]. Chaos Solitons and Fractals, 2005, 24(3): 759-765.

[2] 丘水生,陈艳峰,吴敏,等. 一种新的混沌加密系统方案原理[J]. 电路与系统学报, 2006, 11(1): 98-103.

[3] XIANG T, WONG K W, LIAO X F. Selective image encryption using a spatiotemporal chaotic system [J]. Chaos, 2007, 17(2): 1-12.

[4] 李恩,吴敏,熊永华. 一种基于双混沌映射的加密算法设计与应用[J]. 计算机应用研究, 2009, 26(4): 1512-1514.

[5] BEHINA S, AKHSHANI A, AHADPOUR S, *et al*. A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps [J]. Physics Letters A, 2007, 366(4/5): 391-396.

[6] KWOK H S, TANG W S. A fast image encryption system based on chaotic maps with finite precision representation [J]. Chaos, Solitons and Fractals, 2007, 32(4): 1518-1529.

[7] SHANNON C E. Communication theory of security system [J]. Bell System Technical Journal, 1949, 28(1): 656-715.