文章编号：1000-8608(2016)06-0650-07

基于污染二维混沌动力系统的加密算法

王丽燕*，柳　扬

（大连大学 信息工程学院，辽宁 大连　116622）

摘要： 首先定义了污染动力系统，将二维 Henon 动力系统用二维 Logistic 动力系统进行污染，用这个污染的二维混沌动力系统构造序列密码体系. 这种算法可以产生两列密钥，从而有效地解决了输出结果对密钥低 bit 位变化敏感度较低的问题. 计算机模拟实验和游程测试、相关性分析、灵敏度分析、平衡度检验等安全实验分析结果表明，密文、明文和密钥之间具有高度的非线性和敏感性，算法的密钥空间巨大，可以有效防止统计攻击、唯密文攻击和穷举攻击.

关键词： 污染动力系统；二维 Henon 动力系统；二维 Logistic 动力系统；序列密码

中图分类号： TN918　　**文献标识码：** A　　**doi：** 10.7511/dllgxb201606014

0　引　言

序列密码具有易于计算机实现和错误扩散率较低等特点，一直是密码学中重要的研究课题. Matthews 于 1984 年第一次提到了“chaotic encryption”[1]. 1991 年，由 Habutsu 等提出的迭代加密模式，提供了密码算法研究的新方法，成为早期混沌密码学研究的典型代表[2]. 虽然该算法后来被 Biham 证明存在安全问题[3]，但是基于混沌系统设计密码算法的思想却得到了学术界的认可，开启了混沌密码的研究热潮. 周红等利用逐段线性映射的段数为参数的混沌系统，得到在[－1，1]上为均匀分布、自相关函数为 δ 形态的前馈型流密码[4-5]. 桑涛等采用“逐段二次方根”动力系统，得到均匀的不变分布、自相关函数为 δ 形态的反馈型流密码，避免了文献[4-5]中所采用的“逐段线性”动力系统自身的缺欠[6]. 孙枫等利用一种具有遍历性的动力系统，给出了具有“复杂性高、抗破译性强”等优点的分组密码置换网络的设计[7]. 王相生等通过增强混沌映射的参数来改良系统的混沌状态分布[8]. 翁贻方和鞠磊分别利用 Logistic 动力系统和 Lorenz 系统设计密码体系[9]，得出利用 Logistic 映射具有更快的运算速度，利用 Lorenz 系统安全性更高的结论. 李红达等利用移位寄存器和明文的模运算结果，选择 $f_0(x)=\sqrt{|2x-1|}$ 和 $f_1(x)=1-\sqrt{|2x-1|}$ 这两个非线性映射中的一个进行迭代，迭代轨迹点的位置作为密文的加密算法[10-11]. 尽管现已存在许多使用混沌动力系统为序列密码加密的算法[12-14]，但有些仍存在对混沌映射密钥低 bit 位变化敏感度较低的问题，并有学者提出了相对应的攻击方案[15-18]. 金晨辉在文献[19]中给出了文献[7]已知明文攻击和唯密文攻击的破译方法. 之后在文献[20]和[21]中又指出文献[4]和文献[6]中加密算法存在的问题，给出了先对高位密钥进行攻击，再对低位密钥进行攻击的分割攻击方案. 为了解决由单一的混沌系统而造成的“前若干 bit 位的变化对密钥的变化并不敏感”的安全性问题，王丽燕等构造将可变参数的分段线性动力系统的参数和输入都由二维 Logistic 映射迭代结果控制的复合加密算法[22]. 孙小雁等利用添加离散化的 Logistic混沌扰动的方法，来削弱三角形体系中变量间存在的线性关系[23]. 文献[24]给出了一对互补、具有可变参数、不变分布密度、自相关函数为 δ 形态、遍历的分段非线性动力系统，构造的双重

收稿日期： 2016-01-19；　**修回日期：** 2016-09-02.
基金项目： 国家自然科学基金资助项目(71072161).
作者简介： 王丽燕*(1963-)，女，博士，教授，E-mail：wly1963@163.com；柳　扬(1979-)，女，博士生，E-mail：lykx2001@163.com.

加密算法增长了输出序列的周期，并提高了系统的非线性. 张顺等利用 DNA 编码分组、随机替换分组以及超混沌系统构造加密算法[25]. Merah 等利用二维 Henon 映射及其同步映射构造实时密码系统[26].

为增强混沌动力系统的敏感性，本文借用污染分布的思想，给出污染动力系统的定义，将二维 Henon 动力系统用二维 Logistic 动力系统进行污染，讨论污染后动力系统的简单性质. 基于该污染的二维混沌系统产生两列密钥流对明文进行加密，通过游程测试、相关性分析、灵敏度分析、平衡度检验等计算机模拟实验对安全性进行验证.

1　混沌动力系统

1.1　污染混沌动力系统

定义 1　设 f_1 和 f_2 是两个动力系统，称 $f=\alpha f_1+(1-\alpha)f_2$ 为污染动力系统，其中 $\alpha(0<\alpha<1)$称为污染系数.

1.2　污染二维混沌动力系统

二维 Logistic 映射动力学方程为

$$\begin{aligned} x_{n+1}&=\mu\lambda_1 x_n(1-x_n)+\gamma y_n\\ y_{n+1}&=\mu\lambda_2 y_n(1-y_n)+\gamma x_n \end{aligned} \tag{1}$$

其中 λ_1、λ_2、γ、μ 是参数. 当 $\mu=4$ 时，表 1 列出了系统会出现混沌现象的不同条件[12].

表 1　二维 Logistic 映射混沌条件

Tab. 1　Chaotic condition of two-dimensional Logistic mapping

γ	λ_1	λ_2
0.1	[0.65,0.90]	[0.65,0.90]
[0.20,0.45]	0.8	0.2
[0.30,0.54]	0.7	0.3
[0.40,0.57]	0.6	0.4

图 1 分别给出了两种参数取值条件下的分叉情况.

二维 Henon 映射的动力学方程为

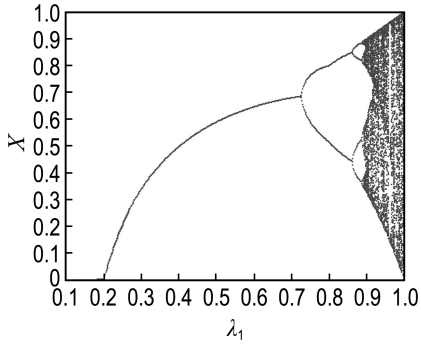
$$\begin{aligned} u_{n+1}&=1-pu_n^2+v_n\\ v_{n+1}&=qu_n \end{aligned} \tag{2}$$

其中 p、q 为参数. 图 2 给出了 $p=1.4$，$q=0.3$ 条件下的混沌状态图.

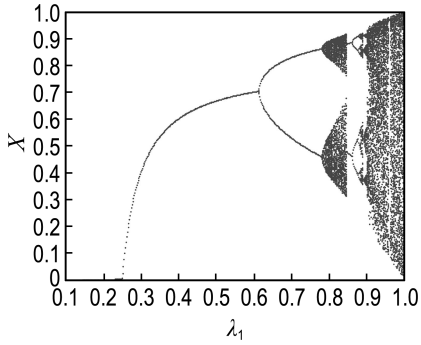
将二维 Henon 映射用二维 Logistic 映射进行污染，得到污染动力系统：

$$\begin{pmatrix} x_{n+1}\\ y_{n+1}\end{pmatrix}=\alpha\begin{pmatrix}\mu\lambda_1 x_n(1-x_n)+\gamma y_n\\ \mu\lambda_2 y_n(1-y_n)+\gamma x_n\end{pmatrix}+(1-\alpha)\begin{pmatrix}1-px_n^2+y_n\\ qy_n\end{pmatrix} \tag{3}$$

其中 $0<\alpha<1$.



(a) λ_1，$\lambda_2=1-\lambda_1$，$\lambda=0.3$



(b) $\lambda_1=\lambda_2$，$\lambda=1-\lambda_1$

图 1　Logistic 映射分叉图

Fig. 1　Branch chart of Logistic mapping

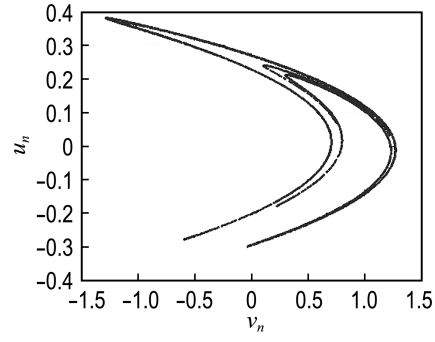
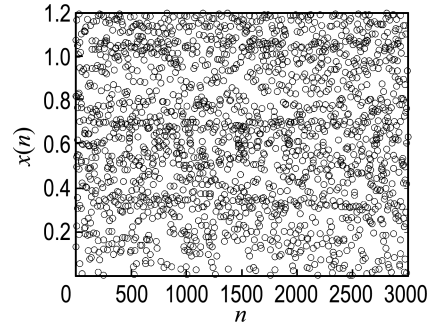


图 2　Henon 映射的吸引子

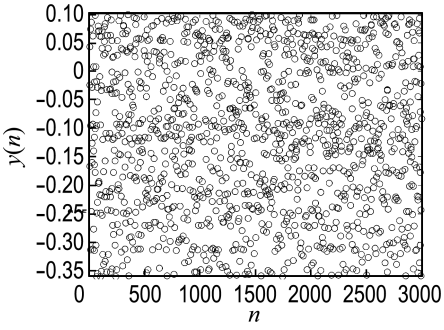
Fig. 2　Attractor of Henon mapping

利用 Matlab 计算，得到 Jacobi 矩阵的特征值的绝对值为 1.871 9>1，根据差分方程组计算 Lyapunov 指数定义[13]，可知式(3)的 Lyapunov 指数大于零，说明污染的二维动力系统(3)为混沌动力系统. 系统输出的 $x(n)$和 $y(n)$的值如图 3

所示，容易看出输出值服从均匀分布.



(a) $x(n)$



(b) $y(n)$

图 3 $x(n)$和 $y(n)$在其区间的分布

Fig. 3 The distribution of $x(n)$ and $y(n)$ in their domains

2 序列密码的加密与解密算法

2.1 加密算法

加密过程如图 4 所示.

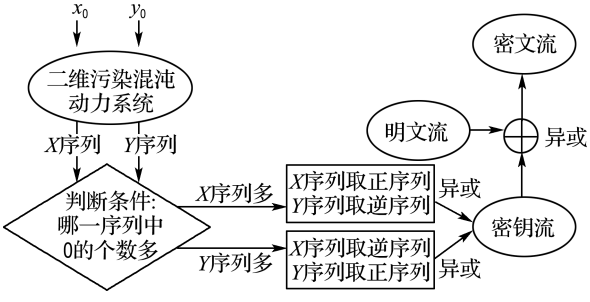


图 4 加密过程

Fig. 4 Encryption process

具体加密算法如下：

(1)通过 ASCII 码把明文转化为十六位二进制序列$\{m_1m_2m_3\cdots m_n\}$，其中 $m_i(i=1,2,3,\cdots,n)$为 0 或者 1.

(2)确定密钥. 给二维污染混沌动力系统(3)中的参数 μ、γ、λ_1、λ_2、p、q、α 取值，选定迭代初始值 x_0、y_0，迭代得到两个混沌序列$\{x(i)\}(i=1,2,3,\cdots,n)$和$\{y(j)\}(j=1,2,3,\cdots,n)$.

(3)由离散化算子 $T_k(x(i))=[10^k x(i)]\bmod 2$ 和 $T_k(y(j))=[10^k y(j)]\bmod 2$，计算得到两个密钥序列$\{k(i)\}$和$\{k(j)\}$，其中 $k(i)=T_k(x(i))(i=1,2,3,\cdots,n)$，$k(j)=T_k(y(j))(j=1,2,3,\cdots,n)$.

(4)比较两个密钥序列$\{k(i)\}(i=1,2,3,\cdots,n)$和$\{k(j)\}(j=1,2,3,\cdots,n)$中 0 的个数，个数多的取正序列，个数少的取逆序列，然后将这两个序列异或，得到新的密钥序列$\{k(l)\}(l=1,2,3,\cdots,n)$.

(5)将密钥序列$\{k(l)\}(l=1,2,3,\cdots,n)$与明文序列$\{m_1m_2m_3\cdots m_n\}$进行异或运算，得到密文二进制序列$\{c_1c_2c_3\cdots c_n\}$.

(6)由密文序列 $C=c_1c_2c_3\cdots c_n$ 的 ASCII 值得到最终的密文.

类似地可以给出解密算法.

2.2 算法仿真

“二维污染混沌动力系统”明文的二进制序列为

01001110100011000111111011110100011011
00011000010110011111010011011011011111
01110110110010001100010100101010100001
01001010011011011111001111101101111110
11011111

不同条件下得到的密文如下：

(1)若取 $\mu=4$，$\gamma=0.52$，$\lambda_1=0.7$，$\lambda_2=0.3$，$p=1.4$，$q=0.3$，$\alpha=0.02$，$x_0=0.131\ 4$，$y_0=0.112\ 3$，$j=4$，得到的密文为

耗 M?@? M<佃€?➛塻

(2)若取 $\alpha=0.02+10^{-11}$，其他条件与(1)相同，密文为

??Y 訊??瞹 x)串妠?

(3)若取 $y_0=0.112\ 3+10^{-11}$，其他条件与(1)相同，密文为

7」 喰 l 欽溙 J`?,蚋拆−？

(4)若取 $x_0=0.131\ 4+10^{-11}$，其他条件与(1)相同，密文为

?-T 砸弦]J?煄⊥h 鐏

(5)若取 $x_0=0.131\ 4+10^{-11}$，$y_0=0.112\ 3+10^{-11}$，其他条件与(1)相同，密文为

?(!!u_2 轟?,K?f?

(6)若取 $j=7$，其他条件与(1)相同，密文为

颯;w 蕈?.D[G}?嗦<q?

(7)若取 $x_0=0$，$y_0=0$，其他条件与(1)相同，密文为

蔰┐ 革繩藍\贈 o~ ?

(8)若取 $\gamma=0.52+10^{-7}$，$x_0=0$，$y_0=0$，$j=$

4，其他条件与(1)相同，密文为

奋洼 Nw 鈥?4!/滦 B 笈 l?

图 5 给出了以上 8 种条件下密文用 0-1 序列的图形化表示，显然，密钥的细微改变将会导致密文的显著改变.

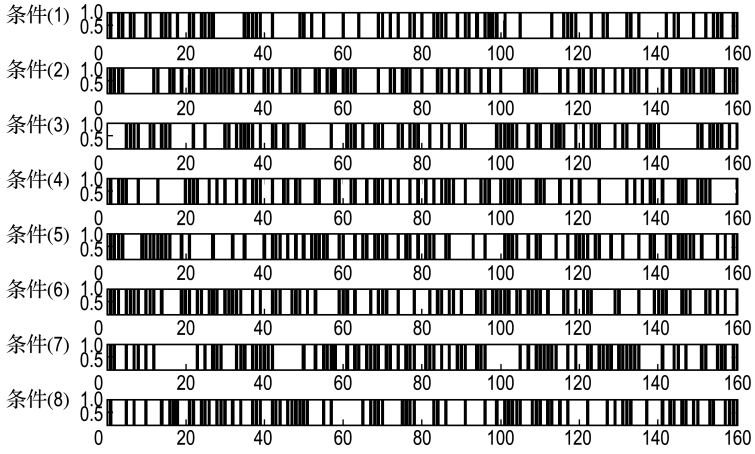


图 5　不同条件下密文信息的二进制序列图

Fig. 5　The binary sequence diagrams of the ciphertext information under different conditions

如果使用正确的解密密钥，可以输出正确的明文；否则无法得到正确的明文. 例如在条件(1)中，解密时，如果使用正确的密钥可以得到正确的明文. 如果两列密钥序列顺序判断错误，得到明文为“儓 2 哄 s 艽慄 a 倡-➢l2 蔓 1”；如果 $x_0=0.131\ 4$ 改为 $x_0=0.131\ 4+10^{-11}$，其他条件不变，得到明文为“A?@黩 9??➢%━衽?-”.

3　安全性分析

3.1　游程测试[13]

游程是指序列中由相同 bit 所构成的不间断的子序列. 该测试可以判断其是否为随机序列.

具体测试方法如下：

步骤 1　计算 $f=\sum_j \varepsilon_j \Big/ n$. 其中 n 为序列长度，ε_j 为 bit 值.

步骤 2　判断. 若 $\left|f-\frac{1}{2}\right|\geqslant\tau$，可以断定算法产生的序列随机性较差；若 $\left|f-\frac{1}{2}\right|<\tau$，转步骤 3. 其中 τ 在游程测试中取定为 $\tau=2/\sqrt{n}$.

步骤 3　计算统计值 $V_n=\sum_{k=1}^{n-1} r(k)+1$. 其中 $r(k)=\begin{cases}1; & \varepsilon_k=\varepsilon_{k+1}\\ 0; & \varepsilon_k\neq\varepsilon_{k+1}\end{cases}$.

步骤 4　计算判断标准 P：

$$P=\operatorname{erfc}\left(\frac{|V_n-2nf(1-f)|}{2\sqrt{2n}f(1-f)}\right)$$

其中 f 通过步骤 1 计算得到，函数 $\operatorname{erfc}(z)=\frac{2}{\sqrt{f}}\int_z^{\infty} \mathrm{e}^{-\mu^2}\,\mathrm{d}\mu$.

如果 $P<0.01$，断定测试的序列随机性较差；反之，断定序列具有较好的随机性.

若选取 $\mu=4$，$\gamma=0.52$，$\lambda_1=0.7$，$\lambda_2=0.3$，$p=1.4$，$q=0.3$，$\alpha=0.02$，$x_0=0.131\ 4$，$y_0=0.112\ 3$，$j=4$，$n=160$，计算得到 $x(n)$ 序列和 $y(n)$ 序列的 P 都为 1.99，远大于 0.01. 因此，可以认为混沌序列是随机序列.

3.2　相关性分析

如果明文表示为 $\{m_1m_2m_3\cdots m_n\}$，密文表示为 $\{s_1s_2s_3\cdots s_n\}$，其中 m_i 和 s_i 只取 0 或 1，$i=1,2,3,\cdots,n$，称 $R(\mu,\gamma,\lambda_1,\lambda_2,p,q,\alpha,x_0,y_0,j,n)=\frac{1}{n}(\#\{s_i|s_i=m_i,1\leqslant i\leqslant n\}-\#\{s_i|s_i\neq m_i,1\leqslant i\leqslant n\})$ 为明文和密文之间的相关度[27].

本文选取长度 $n=10\ 000$ 的 0 序列作为明文，以动力系统(3)参数值 $\mu=4$，$\gamma=0.52$，$\lambda_1=0.7$，$\lambda_2=0.3$，$p=1.4$，$q=0.3$，$\alpha=0.02$，$x_0=0.131\ 4$，$y_0=0.112\ 3$，$j=4$ 为例，对明文进行加密，相关度情况如图 6 所示.

显然随着 n 的增大，相关度逐渐趋近于 0，说明密文与明文几乎不相关.

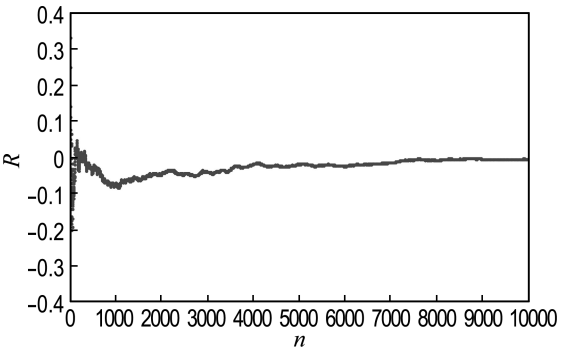


图 6 明文与密文的相关度

Fig. 6 The correlation between the plaintext and ciphertext

3.3 灵敏度分析

如果明文表示为$\{m_1 m_2 m_3 \cdots m_n\}$，密文表示为$\{s_1 s_2 s_3 \cdots s_n\}$，其中 m_i 和 s_i 只取 0 或 1，$i=1,2,3,\cdots,n$，称

$$L(\mu,\gamma,\lambda_1,\lambda_2,p,q,\alpha,x_0,y_0,j,n)=\frac{1}{n}\#\{s_i \mid s_i \neq m_i, 1\leqslant i\leqslant n\}$$

为明文与密文间的灵敏度[27].

仍以长度 $n=10\ 000$ 的 0 序列作为明文，动力系统(3)参数值 $\mu=4,\gamma=0.52,\lambda_1=0.7,\lambda_2=0.3,p=1.4,q=0.3,\alpha=0.02,x_0=0.131\ 4,y_0=0.112\ 3,j=4$ 为例，对明文进行加密，密文与明文间的灵敏度情况如图 7 所示.

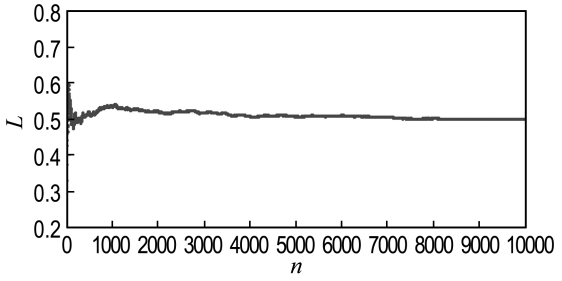


图 7 灵敏度分析图

Fig. 7 Sensitivity analysis chart

图 7 表明，相比明文，大致 50% 的密文序列将会改变.

3.4 密文的平衡度检验

$E(n)=\dfrac{n_0-n_1}{n}$ 称为密文的平衡度[27]. 其中，n_0 表示密文的二进制序列中 0 的个数，n_1 表示密文的二进制序列中 1 的个数，n 为密文的二进制序列总个数. 平衡度可以检验密文中 0 与 1 的个数是否相等，0 与 1 的个数越接近，密文的随机性就越好，抵御统计分析的能力越强.

仍以长度 $n=10\ 000$ 的 0 序列作为明文，动力系统(3)参数值 $\mu=4,\gamma=0.52,\lambda_1=0.7,\lambda_2=0.3,p=1.4,q=0.3,\alpha=0.02,x_0=0.131\ 4,y_0=0.112\ 3,j=4$ 为例，对明文进行加密，密文序列中 0-1 平衡度如图 8 所示.

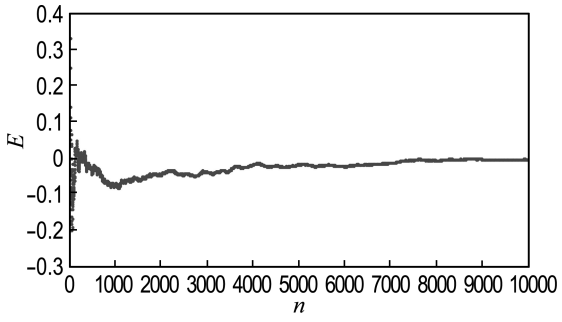


图 8 平衡度分析图

Fig. 8 Balance analysis chart

图 8 的结果表明，序列位数越多，平衡度的值就越趋近于 0，说明序列中 1 和 0 的个数几乎相等.

3.5 密钥空间分析

本文选取的密钥是污染二维混沌动力系统随机产生的初值 x_0、y_0 和离散化算子以及污染系数 α，假设计算的精度为 10^{-5}，采用本算法形成的密钥空间至少为 10^{20}. 实际上，动力系统本身的参数 μ、γ、λ_1、λ_2、p、q 只要在可以形成混沌的范围内取值，都可以作为密钥. 而且计算机的计算精度远远超过 10^{-5}，这样密钥空间将大大超过 10^{20}. 本算法足够抵抗由于密钥空间不大而形成的穷举攻击.

4 结 语

本文给出污染混沌动力系统的概念，并用污染系数 α 将二维 Henon 动力系统用二维 Logistic 动力系统进行污染，并进一步用污染后的多参数动力系统构造序列密码的加密算法. 所进行的各项性能分析，如随机性分析、相关性分析、灵敏度分析、0-1 平衡度检验等都表明污染的混沌映射具有良好统计特性，而且密钥空间巨大，可以有效防止统计攻击、唯密文攻击和穷举攻击.

参考文献：

[1] Matthews R A J. On the derivation of a "chaotic" encryption algorithm [J]. **Cryptologia**, 1984, **8**(1):

29-41.

[2] Habutsu T, Nishio Y, Sasase I, *et al*. A secret key cryptosystem by iterating a chaotic map [C] // Davies D W, ed. **Advances in Cryptology - EUROCRYPT ′91, LNCS 547**. Berlin: Springer-Verlag, 1991:127-140.

[3] Biham E. Cryptanalysis of the chaotic map cryptosystem suggested at EUROCRYPT′91 [C]// **EUROCRYPT′91 Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques**. Berlin: Springer-Verlag, 1991:532-534.

[4] 周　红,罗　杰,凌燮亭. 混沌非线性反馈密码序列的理论设计和有限精度实现[J]. 电子学报, 1997, **25**(10):57-60.
ZHOU Hong, LUO Jie, LING Xie-ting. Generating nonlinear feedback stream ciphers via chaotic systems [J]. **Acta Electronica Sinica**, 1997, **25**(10):57-60. (in Chinese)

[5] 周　红,俞　军,凌燮亭. 混沌前馈型流密码的设计[J]. 电子学报, 1998, **26**(1):98-101.
ZHOU Hong, YU Jun, LING Xie-ting. Design of chaotic feed forward stream cipher [J]. **Acta Electronica Sinica**, 1998, **26**(1): 98-101. (in Chinese)

[6] 桑　涛,王汝笠,严义埙. 一类新型混沌反馈密码序列的理论设计[J]. 电子学报, 1999, **27**(7):47-50.
SANG Tao, WANG Ru-li, YAN Yi-xun. The theoretical design for a class of new chaotic feedback stream ciphers [J]. **Acta Electronica Sinica**, 1999, **27**(7):47-50. (in Chinese)

[7] 孙　枫,秦红磊,徐耀群,等. 基于混沌的分组密码置换网络的设计[J]. 中国工程科学, 2000, **2**(9): 47-49.
SUN Feng, QIN Hong-lei, XU Yao-qun, *et al*. Design of block cipher substitution network on chaos [J]. **Engineering Science**, 2000, **2**(9):47-49. (in Chinese)

[8] 王相生,甘骏人. 一种基于混沌的序列密码生成方法[J]. 计算机学报, 2002, **25**(4):351-356.
WANG Xiang-sheng, GAN Jun-ren. A chaotic sequence encryption method [J]. **Chinese Journal of Computers**, 2002, **25**(4):351-356. (in Chinese)

[9] 翁贻方,鞠　磊. 基于混沌的序列密码加密算法[J]. 计算机工程, 2002, **28**(11):79-80, 83.
WENG Yi-fang, JU Lei. Chaotic stream cipher encryption algorithms [J]. **Computer Engineering**, 2002, **28**(11):79-80, 83. (in Chinese)

[10] 李红达,冯登国. 基于复合离散混沌动力系统的序列密码算法[J]. 软件学报, 2003, **14**(5):991-998.
LI Hong-da, FENG Deng-guo. Stream cipher algorithms based on composite nonlinear discrete chaotic dynamical systems [J]. **Journal of Software**, 2003, **14**(5):991-998. (in Chinese)

[11] 李红达,冯登国. 复合离散混沌动力系统与序列密码体系[J]. 电子学报, 2003, **31**(8):1209-1212.
LI Hong-da, FENG Deng-guo. Composite nonlinear descrete chaotic dynamical systems and stream cipher systems [J]. **Acta Electronica Sinica**, 2003, **31**(8):1209-1212. (in Chinese)

[12] Gotz M, Kelber K, Schwarz W. Discrete-time chaotic encryption systems. I. Statistical design approach [J]. **IEEE Transactions on Circuits and Systems. I. Fundamental Theory and Applications**, 1997, **44**(10):963-970.

[13] Kocarev L. Chaos-based cryptography: A brief overview [J]. **IEEE Circuits and Systems Magazine**, 2002, **1**(3):6-21.

[14] XIANG Tao, Wong Kwor-kwo, LIAO Xiao-feng. A novel symmetrical cryptosystem based on discretized two-dimensional chaotic map [J]. **Physics Letters A**, 2007, **364**(3-4):252-258.

[15] Alvarez G, Montoya F, Romera M, *et al*. Cryptanalysis of a chaotic encryption system [J]. **Physics Letters A**, 2000, **276**(1-4):191-196.

[16] 张　斌,金晨辉. 对迭代型混沌密码的逆推压缩攻击[J]. 电子学报, 2010, **38**(1):129-134,140.
ZHANG Bin, JIN Chen-hui. Inversion and compression attacks to iterative chaotic ciphers [J]. **Acta Electronica Sinica**, 2010, **38**(1):129-134,140. (in Chinese)

[17] 汪海明,李　明,金晨辉. 对 XW 混沌密码算法的分割攻击[J]. 计算机应用研究, 2010, **27**(7):2625-2628.
WANG Hai-ming, LI Ming, JIN Chen-hui. Divide-and-conquer attack on XW chaotic cipher [J]. **Application Research of Computers**, 2010, **27**(7): 2625-2628. (in Chinese)

[18] 尹汝明,袁　坚,山秀明,等. 混沌密码系统弱密钥随机性分析[J]. 中国科学:信息科学, 2011, **41**(7):777-788.
YIN Ru-ming, YUAN Jian, SHAN Xiu-ming, *et al*. Weak key analysis for chaotic cipher based on randomness properties [J]. **Science in China: Information Sciences**, 2011, **41**(7): 777-788. (in Chinese)

[19] 金晨辉. 一个基于混沌的分组密码算法的分析[J]. 中国工程科学, 2001, **3**(6):75-80.
JIN Chen-hui. Analysis of a block cipher based on chaos [J]. **Engineering Science**, 2001, **3**(6):75-80. (in Chinese)

[20] 金晨辉,高海英. 对两个基于混沌的序列密码算法的分析[J]. 电子学报, 2004, **32**(7):1066-1070.
JIN Chen-hui, GAO Hai-ying. Analysis of two stream ciphers based on chaos [J]. **Acta Electronica Sinica**, 2004, **32**(7):1066-1070. (in Chinese)

[21] 金晨辉,杨 阳,祁传达. 对混沌序列密码的相关密钥攻击[J]. 电子与信息学报, 2006, **28**(3):410-414.
JIN Chen-hui, YANG Yang, QI Chuan-da. A related-key attack on chaotic stream ciphers [J]. **Journal of Electronics & Information Technology**, 2006, **28**(3):410-414. (in Chinese)

[22] 王丽燕,李永华,贾思齐,等. 一种基于复合混沌动力系统的序列密码算法[J]. 大连理工大学学报, 2012, **52**(5):730-735.
WANG Li-yan, LI Yong-hua, JIA Si-qi, *et al*. A stream cipher algorithm based on composite chaotic dynamical systems [J]. **Journal of Dalian University of Technology**, 2012, **52**(5):730-735. (in Chinese)

[23] 孙小雁,张焕国,张茂胜,等. Logistic混沌扰动三角形密码体制[J]. 计算机应用与软件, 2014, **31**(9):268-271.
SUN Xiao-yan, ZHANG Huan-guo, ZHANG Mao-sheng, *et al*. Triangular cryptosystem with Logistic chaos disturbance [J]. **Computer Applications and Software**, 2014, **31**(9):268-271. (in Chinese)

[24] 王丽燕,许佳佳,李海燕. 基于两个离散混沌动力系统的序列密码算法[J]. 大连理工大学学报, 2014, **54**(5):581-588.
WANG Li-yan, XU Jia-jia, LI Hai-yan. A stream cipher algorithm based on two discrete chaotic dynamical systems [J]. **Journal of Dalian University of Technology**, 2014, **54**(5):581-588. (in Chinese)

[25] 张 顺,高铁杠. 基于类DNA编码分组与替换的加密方案[J]. 电子与信息学报, 2015, **37**(1):150-157.
ZHANG Shun, GAO Tie-gang. Encryption based on DNA coding, codon grouping and substitution [J]. **Journal of Electronics & Information Technology**, 2015, **37**(1):150-157. (in Chinese)

[26] Merah L, Ali-Pacha A, Naima H-S. Real-time cryptosystem based on synchronized chaotic system [J]. **Nonlinear Dynamics**, 2015, **82**(1-2):877-890.

[27] 廖晓峰,肖 迪,陈 勇,等. 混沌密码学原理及其应用[M]. 北京:科学出版社, 2009.
LIAO Xiao-feng, XIAO Di, CHEN Yong, *et al*. **Theory and Applications of Chaotic Cryptography** [M]. Beijing:Science Press, 2009. (in Chinese)

Encryption algorithm based on contaminated two-dimensional chaotic dynamic system

WANG Li-yan*, LIU Yang

(College of Information Engineering, Dalian University, Dalian 116622, China)

Abstract: An algorithm to construct a stream cipher system is presented by defining a contaminated dynamic system, in which the two-dimensional Henon dynamic system is contaminated by the two-dimensional Logistic dynamic system. By generating two columns of keys, this algorithm can effectively solve the problem that the output is not very sensitive to the change of the low bit of the input. The results of safety tests, such as computer simulation, runs test, correlation analysis, sensitivity analysis and balance test, etc. show the highly nonlinearity and sensitivity among ciphertext, plaintext and the key. Also the large key space of this algorithm can effectively prevent the statistical attacks, ciphertext only attacks and exhaustive attacks.

Key words: contaminated dynamic system; two-dimensional Henon dynamic system; two-dimensional Logistic dynamic system; stream cipher