第 57 卷 第 10 期 2008 年 10 月
1000-3290/2008/57(10)/6132-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.10,October,2008

基于混沌系统互扰的流密码设计*

向 菲† 丘水生

(华南理工大学电子与信息学院,广州 510640)

(2008 年 1 月 17 日收到;2008 年 5 月 14 日收到修改稿)

提出了一种新的流密码设计方案,利用两个混沌系统产生的序列进行序列值和控制参数的互扰,得到新的密钥流序列.对互扰序列和 Logistic 序列进行 NIST 测试,证明新的流密码设计方案产生的互扰序列的密码学特性要好于单一混沌系统产生的密钥流序列.提出适用于混沌伪随机序列稳定性测试的 k 错近似熵定义,并将其应用于测试互扰序列及 Logistic 序列,结果显示,互扰序列的稳定性要好于 Logistic 序列.将互扰序列用作图像的加密和解密,仿真结果显示,互扰序列能够有效且安全地掩盖明文信息.

关键词:混沌系统,互扰序列,密钥流

PACC:0545

1. 引 言

由于混沌系统具有确定性、有界性、对初始条件的敏感性、拓扑传递性和混合性、宽带性、快速衰减的自相关性、长期不可预测性和伪随机性[1],使它能够满足保密通信及密码学的基本要求.因此,当前很多研究者都把混沌系统应用于保密通信和信息安全领域[2,3],研究集中在使用混沌系统构造伪随机数发生器的相关算法及性能分析[4—6].大多数混沌系统在有限精度条件下实现,它们的性质会与其理论结果发生偏移,从而许多基于混沌系统的加密系统无法实现.Borcherds 等人[7]指出有限精度混沌系统出现的短周期行为难以进行精确的分析.Lin 等人[8]认为应当增大系统的实现精度来克服数字化混沌系统产生的问题.Herdari-Bateni 等人[9]建议通过混沌系统级联来获得更大的周期.周红等人[10]提出了用 m 序列的扰动来实现有限精度混沌系统的方法.Sang 等人[11]提出用一类扰动来扩展混沌密钥流的短周期,并给出了扩展周期的理论值的下界.

本文提出用两个混沌系统实施互扰来克服有限精度效应,以 Logistic 映射为例,测试了两个 Logistic 映射实施互扰后的初值敏感性、分布特性、自相关特性和互相关特性.并且对比了扰动前后序列的伪随机特性,提出了测试序列稳定性的方法,并对扰动前后序列进行稳定性测试,定量地说明了互扰方案能有效地解决有限精度造成的混沌动力学特性退化问题.

2. 混沌系统互扰方案

不失一般性,考虑两个混沌系统:

$$x(t+1) = F(x(t)),$$
$$y(t+1) = G(y(t),\phi),$$

其中,F 为主混沌系统,G 为扰动混沌系统.G 产生扰动向量对主混沌系统 F 的输出形成扰动,同时主混沌系统 F 的输出去扰动 G 的控制参数 ϕ.扰动的结构如图 1 所示.

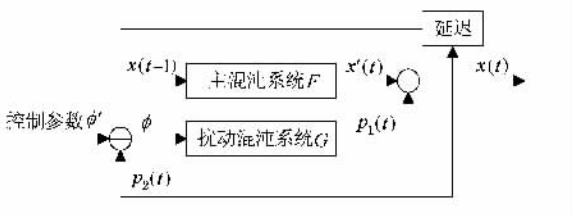

图 1 混沌系统互扰实现结构

扰动混沌系统 G 通过如下方法形成扰动向量:

$$p_1(t) = y(t) \times 10^{l} \times 10^{-n_1} \times \delta(t - k \cdot \Delta_1), \quad (1)$$

扰动过程为

* 国家自然科学基金(批准号:60372004)和广东省自然科学基金(批准号:06025729)资助的课题.

† E-mail:fayexiang@hotmail.com

$$x(t) = p_1(t) + x'(t).$$

主混沌系统 F 通过如下方法对扰动混沌系统 G 的控制参数形成扰动：

$$p_2(t) = x(t) \times 10\rfloor \times 10^{-n_2} \times \delta(t - k \cdot \Delta_2), \quad (2)$$

扰动过程为

$$\phi = \phi' + p_2(t),$$

其中“ $\rfloor$ ”表示向下取整，n_1 和 n_2 表示扰动位数，Δ_1 和 Δ_2 表示扰动间隔，k 为正整数. 系统最终的输出为 $x(t)$，即为流密码加密系统的密钥流.

根据文献[11]，一个好的扰动应当满足以下原则：1）具有均匀分布；2）不会使原有的混沌序列的良好的统计学特性退化，所以扰动信号的幅度应当远小于混沌信号的幅度，在数值上由信噪比进行衡量：

$$\mathrm{SNR} = 10\log_{10}\left(\frac{M_c}{M_p}\right), \quad (3)$$

其中，M_c 表示混沌信号的最大幅度，M_p 表示扰动信号的最大幅度. 因此，SNR 应当远大于 1；3）扰动时间应当远小于系统的运行时间. 基于这些原则，文献[10,11]都提出用 LFSR 作为扰动源. 本文提出用混沌系统作为扰动源，因为用混沌序列做扰动源除了满足以上原则外，相对于 m 序列还具备以下优点：1）主混沌系统和扰动混沌系统可以采用同一种或不同种混沌系统，易于产生和实现；2）混沌系统的初始条件比 LFSR 的初始条件要多得多，密钥空间大大增加，保密性得到加强.

3. 流密码密钥序列的检验

3.1. 伪随机特性检验

美国国家标准技术研究所(NIST)制定了一套随机序列的测试标准[12]，该标准共包含 16 项指标，从不同角度检验被测序列在统计特性上相对于理想随机序列的偏离程度.

本文主要选用如下几个测试及选择的理由如下：

1）单比特频数测试（the frequency/monobit test）该测试检验序列中 0 和 1 的个数所占的比例. 只有通过这个测试，才能进行随后的各项测试，要求被测序列的长度 $n \geqslant 100$.

2）游程测试（the runs test）　该测试的目的是检验序列中连续的 0 和 1 的长度相对于理想随机序列的偏离程度，要求被测序列的长度 $n \geqslant 100$.

3）离散傅里叶变换测试（the discrete Fourier transform test）　该测试计算序列傅里叶频谱中的峰值，以检验被测序列中与理想随机序列间不同的周期特性，要求被测序列的长度 $n \geqslant 1000$.

4）近似熵测试（the approximate entropy test）该测试计算两个相邻长度的序列重叠块发生的频率相对于理想随机序列的偏差. 文献[13]指出，线性复杂度表征的是能够产生该序列的最短线性反馈寄存器长度，而混沌伪随机序列是通过混沌系统的迭代，并由其演化轨迹得到的，用线性复杂度来衡量混沌伪随机序列的复杂度是不合适的，因此提出利用混沌运动产生信息量的大小来度量混沌伪随机序列的复杂度，用近似熵作为判断复杂度大小的准则，要求被测序列的距离向量的维数与序列长度的关系为 $m < \log_2 n\rfloor - 2$.

5）累积和测试（the cumulative sums test）　该测试评价被测序列的累积量偏移程度是否与理想随机序列相一致，测试分为从前往后测试（cum-sum forward）和从后往前测试（cum-sum reverse），要求被测序列的长度 $n \geqslant 100$.

被测序列随机性的优劣是通过测试结果 P[12] 来体现的，$P \in [0,1]$，如果 $P \geqslant 0.01$，则测试通过，且 P 越大，被测序列的伪随机特性越好.

3.2. 稳定性检验

序列的稳定性问题是指改变被测有限序列的相应一些元素后，序列的复杂度的变化问题[14]. 文献[14]中用线性复杂度的稳定性来衡量密钥流的稳定性，具体指标为重量复杂度或 k 错线性复杂度. 但在实验中发现，对于较短的二值序列，k 错线性复杂度并不能很好的区分序列的稳定性. 因此本文引入以下指标：

定义　设 s^N 是 $GF(2)$ 上的一个 N 长序列. s^N 的重量近似熵(weight approximate entropy)定义为

$$ApEn_k(m)(s^N) = \min_{W_H(t^N)=k} ApEn(m)(s^N + t^N), \quad (4)$$

其中 $W_H(t^N)$ 表示 t^N 的 Hamming 重量，即 t^N 的非零分量个数，$ApEn(m)(s^N)$ 表示序列 s^N 向量维数为 m 的近似熵. 重量近似熵也是原序列改变 k 位后得到的序列的近似熵的最小值，所以，它也可以被称为 k 错近似熵（k-error approximate entropy）.

被测序列的稳定性优劣通过原序列近似熵与 k 错近似熵之间的偏离程度来衡量，即用指标

$$R_{ApEn} = \frac{ApEn(m)(s^N) - ApEn_k(m)(s^N)}{ApEn(m)(s^N)} \times 100\% \quad (5)$$

测量被测序列近似熵的稳定性.

4. 仿真结果及分析

以最简单的 Logistic 映射为例,考察此方案的可行性.主混沌系统 F 和扰动混沌系统 G 均使用 Logistic 映射:$x(t+1) = F(x(t)) = 4x(t)(1 - x(t))$, $y(t+1) = G(y(t), \phi) = \phi y(t)(1 - y(t))$, 其中,$3.57 \leqslant \phi \leqslant 4$.仿真用 Matlab 7.1 实现,方案中参数 $x(1) = 0.001$, $n_1 = n_2 = 8$, $\Delta_1 = \Delta_2 = 10$.

从图 2 可知,互扰序列具有良好的对初值敏感性,均匀分布特性,二值自相关函数,零互相关函数,满足作为一个流密码密钥流的特性.

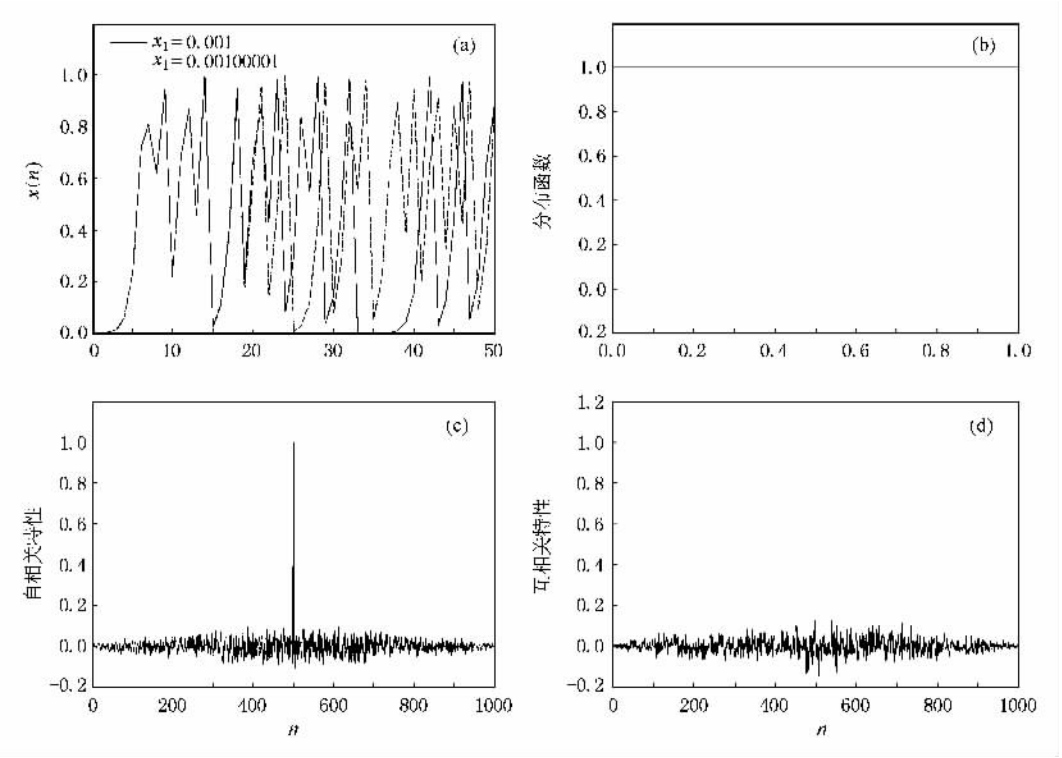

图 2 互扰序列的特性 (a)初值敏感性;(b)均匀分布性;(c)自相关性;(d)互相关性

根据(1),(2)和(3)式,可得到信噪比 SNR = 70.46,说明扰动没有使原混沌序列良好的统计学特性退化.由 $\Delta_1 = \Delta_2 = 10$ 可知,扰动时间大概占系统运行时间的 1/10,远小于系统的运行时间.以上条件都满足文献[11]所提出的一个好的扰动应当满足的原则.

4.1. 伪随机特性的比较与分析

为了定量地考察互扰序列的伪随机特性,在相同条件下,通过迭代得到未经过扰动的 Logistic 序列,将两种序列量化为二进制序列,用 3.1 节中测试进行检验.结果如表 1 所示.

表 1 互扰序列与 Logistic 序列伪随机特性比较

P-value	互扰序列 ($\Delta = 1000$)	互扰序列 ($\Delta = 100$)	互扰序列 ($\Delta = 10$)	Logistic 序列
单比特频数测试	0.412216	0.271332	0.920344	0.984043
近似熵测试 ($m = 2$)	0.532653	0.119281	0.608184	0.084931
离散傅里叶变化测试	0.436178	0.795208	0.697031	0.217619
游程测试	0.159481	0.233165	0.904562	0.075077
累积和测试(前向)	0.214793	0.277729	0.722386	0.393883
累积和测试(后向)	0.787595	0.407891	0.814758	0.407891

从表 1 中的数据可以看出，经过互扰的序列的各项测试结果均比较理想，优于 Logistic 序列.

4.2. 序列稳定性的比较与分析

根据定义，测得互扰序列和 Logistic 序列的 k 错近似熵，结果如表 2 所示.

从表 2 可以看出，互扰序列的 k 错近似熵大于 Logistic 序列的，且随着扰动间隔的增加，k 错近似熵越大.为了更直观地观察互扰序列的扰动间隔对序列近似熵的稳定性的影响，根据(5)式得到了 R_{ApEn} 与 k 的关系图，如图 3 所示.图 3 显示，互扰序列的近似熵的稳定性要好于Logistic序列的稳定性，且扰动间隔越大，序列近似熵的稳定性越好.

表 2　互扰序列与 Logistic 序列 k 错近似熵比较

k 错近似熵 ($m=2$)	互扰序列 ($\Delta=1000$)	互扰序列 ($\Delta=100$)	互扰序列 ($\Delta=10$)	Logistic 序列
$k=0$	0.67108322	0.66911187	0.65217438	0.65086296
$k=1$	0.65121870	0.64877612	0.61435007	0.60960507
$k=2$	0.62448081	0.62136185	0.56877327	0.56226259
$k=3$	0.59252514	0.58721405	0.52334753	0.51680530

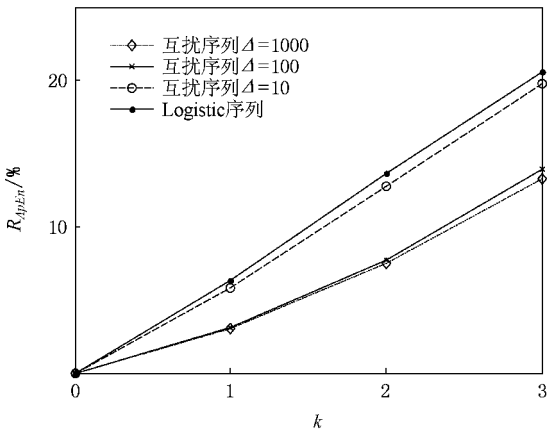

图 3　R_{ApEn} 与 k 关系图

5. 应用实例

以下用混沌系统互扰产生的密钥流对图像进行加密和解密，原理框图如图 4 所示.密钥流发生器在密钥 key 的作用下产生伪随机序列 x，密钥流发生器的结构如图 1 所示.原始图像 p 与伪随机序列 x 在加密函数的作用下生成密文 c，经过信道传输，接收端得到密文 c'，密钥流发生器在 key′ 的作用下产生伪随机序列 x'，c' 与 x' 在解密函数的作用下得到恢复图像 p'.加密和解密函数均为异或.当加密和解密端的密钥流发生器的密钥 key = key′ 时，能得到正确的恢复图像.

根据框图对图像用 Matlab7.1 进行加解密仿真.对于密钥流发生器，所选取的密钥 key 即系统参数为 $x(1)=0.001$，$y(1)=0.002$，$n_1=n_2=8$，$\Delta_1=\Delta_2=10$，$\phi=4$，为消除混沌过渡态的影响，选取迭代 $k=10000$ 次后的序列值作为密钥流序列.加密/解密结果如图 5(b)和(c)所示；为测试算法对密钥的敏感性，将解密密钥作微小变动，即只将 $x(0)$ 的值改为 0.1001，其解密结果如图 5(d)所示.

通过原始图像与加密图像的直方图(图 6)可以看出，加密图像较之原始图像具有更好的均匀特性.说明混沌序列互扰产生的密钥流能有效地掩盖明文信息.

接下来对加密图像的相邻像素进行相关性分

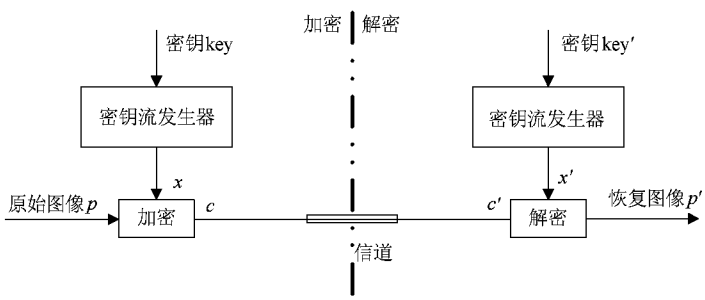

图 4　图像的加密与解密过程

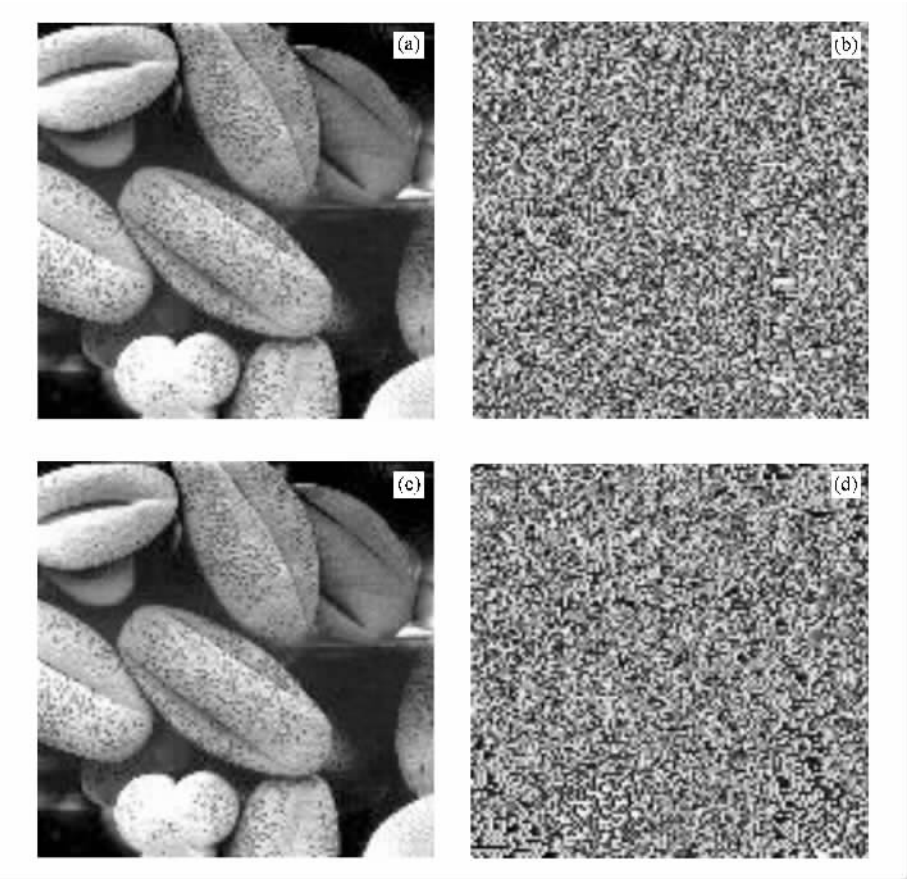

图 5 图像加密/解密仿真结果 (a)原始图像;(b)加密图像;(c)正确解密图像;(d)错误解密图像

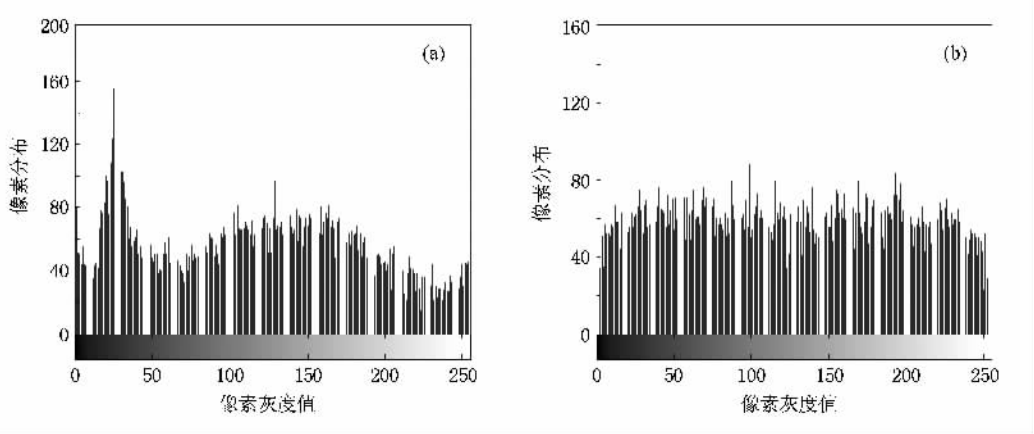

图 6 原始图像及加密图像直方图比较 (a)原始图像直方图;(b) 加密图像直方图

析.在原始图像和加密图像中随机抽取 1000 个点,根据文献[15]提出的方法对原始图像和加密图像的水平、垂直和对角方向相邻像素点的相关性进行计算,得到如图 7 的结果.

本节以一个简单的加密算法为例说明了基于混沌系统互扰的结构在流密码中的应用.仿真结果表明,混沌系统互扰产生的序列能够有效地用于图像的加密和解密.结合第 4 节对密钥流序列的性能分析,及对原始图像及加密图像直方图和相邻像素点的相关性比较,说明密钥流序列用于流密码加密的安全性比较高.可见,基于混沌系统互扰的结构是一个具有良好特性的密钥流产生器.在混沌流密码的设计中,可以尝试以此结构为模块,选择一个或多个此模块来设计更为复杂的流密码加密系统.

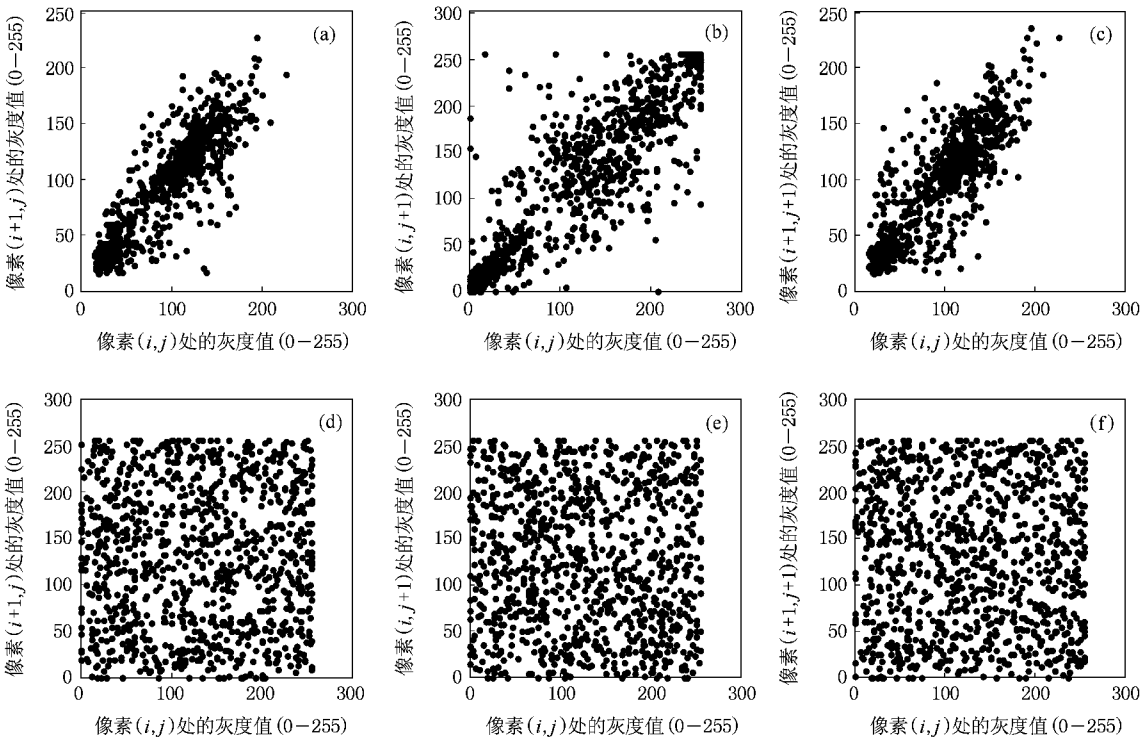

图 7　原始图像和加密图像相邻像素点的相关性比较　(a)和(d)为水平相邻相关性；(b)和(e)为垂直相邻相关性；(c)和(f)对角相邻相关性

6. 结　　论

本文提出了基于混沌系统互扰的流密码设计方案，并提出衡量序列稳定性的新指标：k 错近似熵. 通过仿真，定量地直观地说明了此流密码设计方案的可行性与有效性. 另外，与现有文献中提出的用 m 序列扰动混沌系统方案相比，由于互扰系统初始条件增加，本文提出的方案的密钥空间大大增加. 最后，通过一个应用实例说明，混沌系统互扰产生的序列能够有效地用于图像的加密和解密，且安全性较高. 基于混沌系统互扰的结构能够作为一个模块应用于流密码的设计中.

[1] Kocarev L, Jakimoski G, Stojanovski T, Parlitz U 1998 *Proc. IEEE Int. Sym. CAS.* **4** 514

[2] Xu S J, Wang J Z 2008 *Acta Phys. Sin.* **57** 37 (in Chinese) [徐淑奖、王继志 2008 物理学报 **57** 37]

[3] Kuang J Y, Deng K, Huang R H 2001 *Acta Phys. Sin.* **50** 1856 (in Chinese) [匡锦瑜、邓　昆、黄荣怀 2001 物理学报 **50** 1856]

[4] Bernstein G M, Lieberman M A 1990 *IEEE Trans. CAS.* **37** 1157

[5] Pareek N K, Patidar V, Sud K K 2003 *Phys. Lett.* A **309** 75

[6] Kocarev L, Jakimoski G 2003 *IEEE Trans. CAS*-I **50** 123

[7] Borcherds P H, Mccauley G P 1993 *Chaos, Solitons & Fractals* **3** 451

[8] Lin T, Chua L O 1991 *IEEE Trans. CAS.* **38** 557

[9] Heidari-Bateni G, McGillem C D 1994 *IEEE Trans. Commun.* **42** 1524

[10] Zhou H, Ling X T 1997 *Acta Electron. Sin.* **25** 95 (in Chinese) [周　红、凌燮亭 1997 电子学报 **25** 95]

[11] Sang T, Wang R L, Yan Y X 1998 *Electron. Lett.* **34** 873

[12] Rukhin A, Soto J, Nechvatal J, Smid M, Barker E, Leigh S, Levenson M, Vangel M, Banks D, Heckert A, Dray J, Vo S 2001 *NIST Special Publication* **800-22** 13

[13] Cai J P, Li Z, Song W T 2003 *Acta Phys. Sin.* **52** 1871 (in Chinese) [蔡觉平、李　赞、宋文涛 2003 物理学报 **52** 1871]

[14] Ding C S, Xiao G Z 1994 *Stream Ciphers and Its Applications* (Beijing: National Defence Industry Press) p79 (in Chinese) [丁存生、肖国镇 1994 流密码学及其应用 (北京：国防工业出版社) 第 79 页]

[15] Chen G R, Mao Y B, Chui C K 2004 *Chaos, Solitons & Fractals* **21** 749

Stream cipher design based on inter-perturbations of chaotic systems*

Xiang Fei† Qiu Shui-Sheng

(*School of Electronic and Information Engineering, South China University of Technology, Guangzhou* 510640, *China*)

(Received 17 January 2008; revised manuscript received 14 May 2008)

Abstract

A new stream cipher design scheme is proposed, which uses the sequences generated by two chaotic systems to inter-perturb their sequence values and the control parameter, so as to obtain a new sequence as key stream. Inter-perturbed sequence and Logistic sequence are tested by several tests of NIST's (National Institute of Standards and Technology) STS randomness test suite. Simulation results prove that the cryptographical properties of inter-perturbation sequence are better than those of Logistic sequence. k-error approximate entropy is proposed to test the stability of inter-perturbed sequence and Logistic sequence. Simulations indicate that the stability of inter-perturbed sequence is better than that of Logistic sequence. An image is encrypted and decrypted by the inter-perturbed sequence. Simulation results show that the inter-perturbation sequence can cover up plaintext effectively and safely.

Keywords: chaotic system, inter-perturbed sequence, key stream

PACC: 0545

* Project supported by the National Natural Science Foundation of China (Grant No. 60372004) and the Natural Science Foundation of Guangdong Province, China (Grant No. 06025729).

† E-mail: fayexiang@hotmail.com