一种新颖的基于混沌映像格子的图像保密通信方案*)

游明英[1] 彭 军[1,2] 金尚柱[1] 张 伟[3] 刘海玲[1]

(重庆科技学院电子信息工程学院 重庆 400050)[1] (美国加州州立大学计算机科学系 美国 CA 95819)[2]

(重庆教育学院计算机与现代教育技术系 重庆 400067)[3]

摘 要 基于混沌映像格子(CML)提出了一种新颖的图像保密通信方案。发送方利用 CML 快速产生二值时空混沌序列,并将其与原始图像进行异或加密处理,经通信双方同步后,接收方即可解密出原始图像。由于混沌序列对 CML 中的耦合系数、驱动序列初值等比较敏感,增加了序列抗攻击能力。数值实验结果表明本方案是可行的,并对系统密钥空间、密钥敏感性等密码学特性进行了分析。

关键词 混沌映像格子,图像加密,保密通信

A Novel Image Communication Scheme Based on Chaotic Map Lattices

YOU Ming-ying[1] PENG Jun[1,2] JIN Shang-zhu[1] ZHANG Wei[3] LIU Hai-ling[1]

(College of Electronic Information Engineering, Chongqing University of Science and Technology, Chongqing 400050, china)[1]

(Department of Computer Science, California State University, Sacramento, CA 95819, USA)[2]

(Department of Computer and Modern Education Technology, Chongqing Education College, Chongqing 400067, china)[3]

Abstract Based on chaotic map lattices (CML), a novel image secure communication scheme is proposed. In this scheme, the spatiotemporal binary sequences are rapidly generated and will be used to encrypt source image by exploiting bit-wise xor operation. Once the synchronization of the communication between the sender and receiver is satisfied, the encrypted image then can be correctly recovered into source image. As the chaotic sequences are very sensitive to the coupled parameter of CML and the initial value of the driven system, the capability of the scheme against the cryptographic attack is enhanced greatly. The results of computer numerical stimulation indicate the scheme proposed in this paper is feasible. Finally, we analyze some cryptography properties of the scheme such as the key space and the sensitivity of the encrypted image with respect to the secret key.

Keywords Chaotic map lattices, Image encryption, Secure communication

1 引言

近年来,时空混沌在数学、物理、计算机工程、生物等领域得到越来越多的研究,引起了人们的广泛兴趣。由于时空混沌具有无穷维特性和高度复杂性,在信息加密、图像保密通信中具有很高的应用价值[1-5]。本文借助 CML(混沌映像格子)研究了一种图像保密通信方案,目的在于充分利用时空混沌的优良密码学特性,提供高安全性的信息保密传输。

2 图像保密通信方案

2.1 混沌映像格子(CML)

CML 是一种具有离散时间、离散空间和连续状态的动力系统,在每个格子上由非线性映射(称为局部映射)构成,每个局部映射都与其它格子的局部映射按某种规则进行耦合。由于局部映射的内在非线性动力学行为以及由局部映射之间的空间耦合产生的扩散,导致了 CML 在空间和时间上都呈现出十分优越的时空混沌特性[6]。此外,CML 容易进行解析和数值处理,因此本文拟采用 CML 进行保密方案设计。通常我们使用如下形式的 CML

$$x_{n+1}^i=(1-\varepsilon)f(x_n^i)+\frac{\varepsilon}{2}[f(x_n^{i+1})+f(x_n^{i-1})] \quad (1)$$

式中 $x_n^i(0<x_n^i\leqslant 1)$ 表示第 i 个格子在 n 时刻的状态,f 为格子的局部演化规则,此处我们取 Logistic 混沌映射 $f(x)=rx(1-x)$,$r\in(0,4]$;$\varepsilon\in(0,1)$ 为耦合强度。一般还假设 CML 具有周期边界,即 $x_n^{i+i}=x_n^i(\forall n\in Z)$,其中 L 为系统规模即格子的数量。

CML 系统的驱动序列可以是 CNN, Chen, Chebyshev, Tent 等系统输出的混沌序列,此处选取 Tent 映射

$$f(x)=\begin{cases} lx, & 0\leqslant x\leqslant 0.5 \\ -lx+l, & 0.5\leqslant x\leqslant 1 \end{cases}, 1<l\leqslant 2 \quad (2)$$

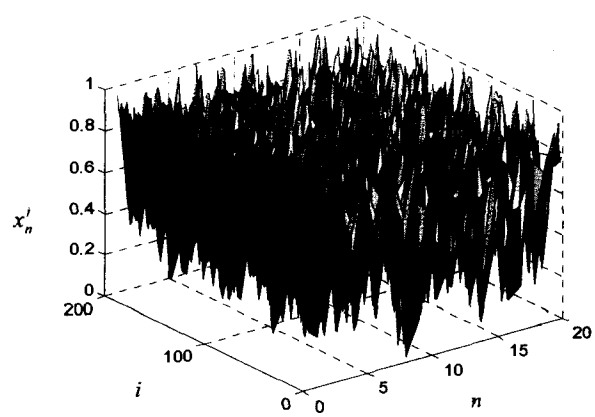


图 1 CML 时空混沌实值序列

图 1 为格子规模 $L=200$,$N=20$,Tent 映射初值 $x_0=0.3$,参数 $l=1.6$,Logistic 映射参数 $r=4.0$,耦合系数 $\varepsilon=0.6$ 时得到的 CML 时空混沌序列。

*)基金项目:重庆市教委科学技术研究项目基金(KJ051402, KJ051501, KJ061409)。**游明英** 讲师,硕士,研究方向为计算机安全、混沌保密通信;**彭 军** 教授,博士,研究方向为网络安全、混沌密码学;**金尚柱** 讲师,硕士,研究方向为网络安全;**张 伟** 教授,博士,研究方向为混沌理论、网络安全;**刘海玲** 讲师,硕士,研究方向为图像处理、计算机应用。

2.2 时空混沌图像保密通信方案

基于时空混沌序列的图像保密通信方案如图2所示。在方案中，发送方使用系统参数(密钥)去驱动CML系统，以产生时空混沌实值序列，二值化处理后对原始图像进行加密处理，再送往通信信道传输给接收方。同时系统参数使用安全通道传输给接收方，以便接收方的CML响应系统产生与发送方同步的时空混沌序列，接收方采用相同的混沌序列二值化方法即可解密出原始图像。

上述通信方案实现的前提是收发双方必须同步。研究表明[8-10]，在一定条件下两个CML系统可以实现同步。也就是说，用一个混沌信号作为初始序列去驱动CML，并且耦合系数ε取适当值时，发送方和接收方的CML系统可以实现时空混沌同步。一旦同步，就可以进行图像保密通信了。

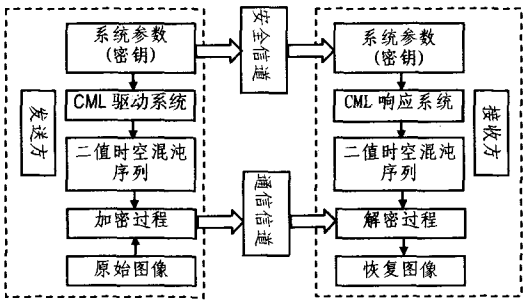


图2 基于CML时空混沌序列的图像保密通信方案

2.3 混沌实值序列二值化处理

CML模型输出的是连续实值序列($-1<x_n<1$)，必须对其进行二值化处理才能用于图像加密。我们采用文献[5]中的方法：将x_n^i表示成一个二值序列，即$x_n^i=(0.b_{n,1}^i b_{n,2}^i b_{n,3}^i \cdots b_{n,p}^i)$，$p$为指定的精度。因此，$\{b_{1,m}^i, b_{2,m}^i, b_{3,m}^i, \cdots, b_{n,m}^i\}$，$1\leqslant m\leqslant p$就可以构成一个伪随机二值序列(PRBS)。由于混沌轨道的遍历性，采用该方法数字化后的PRBS均匀分布[5]。具体地，设CML中第i行的n个格子分别为$x_1^i, x_2^i, \cdots, x_n^i$，则二值化成如下二值矩阵

$$\begin{bmatrix} b_{1,1}^i & b_{2,1}^i & \cdots & b_{n,1}^i \\ b_{1,2}^i & b_{2,2}^i & \cdots & b_{n,2}^i \\ \cdots & \cdots & \cdots & \cdots \\ b_{1,p}^i & b_{2,p}^i & \cdots & b_{n,p}^i \end{bmatrix}_{p\times n}$$

如果精度$p=32$位，则上述矩阵可用于尺寸为$32\times\lfloor n/8\rfloor$的图像数据加密处理。

此外，为防止每个格子局部混沌映射之间发生同步现象(否则所有格点将产生相同的混沌序列)，我们借助文献[7]中的方法即使用Lyapunov指数谱来观察CML的局部混沌同步。式(1)的同步化Lyapunov指数谱为：

$$\lambda_1=\ln(r/2),$$

$$\lambda_2=\lambda_1+\ln[1-\varepsilon+\varepsilon\cdot\cos(2\pi/L)],$$

$$\cdots$$

$$\lambda_L=\begin{cases}\lambda_1+\ln(1-2\varepsilon), & \text{if } L \text{ is even}\\ \lambda_1+\ln[1-\varepsilon+\varepsilon\cdot\cos(2\pi/L)], & \text{if } L \text{ is odd}\end{cases}$$

为了避免耦合的局部映射同步，λ_2必须大于零。即

$$\lambda_2=\lambda_1+\ln[1-\varepsilon+\varepsilon\cdot\cos(2\pi/L)]>0$$

也就是说，CML系统参数r,ε,L必须满足如下关系式才能有效防止局部映射耦合同步产生

$$r[1-\varepsilon+\varepsilon\cdot\cos(2\pi/L)]>2 \qquad (3)$$

2.4 图像加解密过程描述

为了加快图像加密速度，本方案中加密过程就是发送方将二值化后的混沌序列直接与原始图像进行异或操作，解密过程则是接收方利用本地产生的同步化混沌序列，再次与收到的图像进行异或操作即可恢复出原始图像。下面只给出加密过程。

step1：设待加密图像S的高为i_h，宽为i_w(像素单位)，图像S记为$\{s_{i,j}\}$ $(i=1,2,\cdots,i\_h; j=1,2,\cdots,i\_w)$；

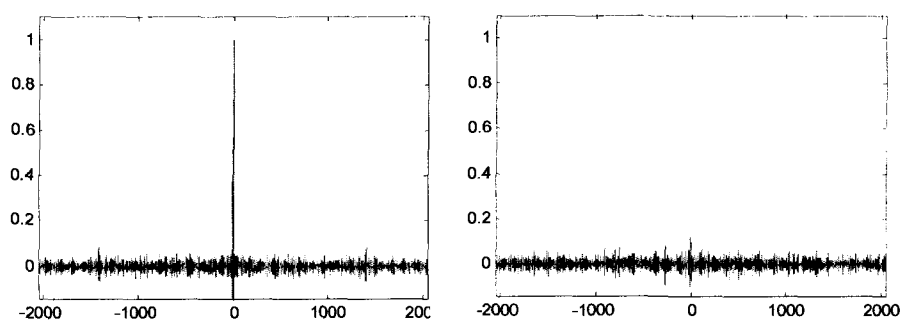
step2：选取系统参数(密钥)，$p=32$，格子数$L=\lceil i_h/p\rceil$，演化步数$N=i_w\times 8$，r和ε在各自取值范围内且满足关系不等式(3)即可，驱动系统Tent映射(2)的控制参数l和迭代初值x_0；

step3：计算Tent映射混沌序列，从x_0出发迭代$L+200$次，取后L个序列作为CML的驱动序列。然后CML每个格子(共有L个格子)演变N次，L个格子共有$L\times N$个状态值，取左上角$i_h\times N(N=i_w\times 8)$个状态值作为加密图像之用，构成一个时空混沌序列状态矩阵，设为$\{c_{i,j}\}(i=1,2,\cdots,i_h; j=1,2,\cdots,N)$；

step4：混沌序列状态矩阵与图像矩阵进行异或操作，即可得到加密后的图像E，$E=\{s_{i,j}\oplus c_{i,j}\}(i=1,2,\cdots,i\_h; j=1,2,\cdots,N)$，$\oplus$表示异或操作；

step5：待收发双方同步后，就可发送图像E了。

3 计算机仿真实验



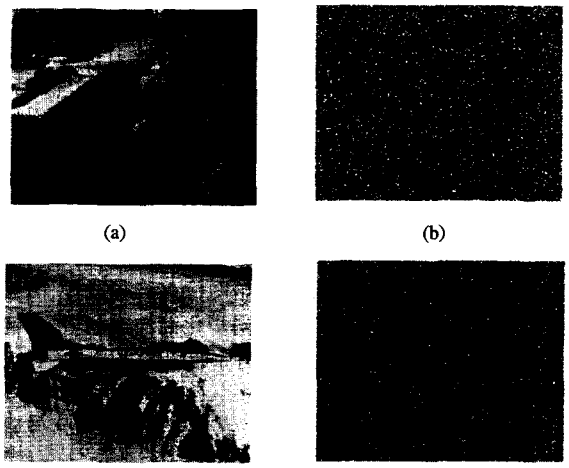
(a)自相关特性曲线　　(b)互相关特性曲线

图3 二值混沌序列相关特性

对本文方案，我们使用MATLAB 7.0对其进行了仿真实验。具体参数如下：$L=16$，$N=512\times 8$，Tent映射初值$x_0=0.3$，参数$l=1.5$，Logistic映射参数$r=4$，耦合系数$\varepsilon=0.6$，精度$p=32$，测试图像选用分辨率为512×512的Woman和Airplane图像。此时关系不等式$r[1-\varepsilon+\varepsilon\cdot\cos(2\pi L)]=3.82>2$成立。

图3为二值化后的时空混沌序列(任选2个)的相关特性曲线,观察图3可知混沌二值序列的相关特性非常好,符合密码学对加密序列的随机性要求。序列的线性复杂度和01平衡性等参数也比较理想[5],此处不再给出。

图4为图像加密通信结果,通过时空混沌序列加密后的图像与原始图像完全不同,类似随机图像,达到了加密效果。接收方使用与发送方相同的系统参数可正确恢复出原始图像,实验结果也证实了方案的可行性和正确性。



(a),(c)分别为Woman和Airplane原始图像,
(b)和(d)分别为使用二值混沌序列加密后的传输图像。

图4 图像保密通信方案仿真结果

4 方案安全性分析

4.1 密钥空间

由本文方案可知,系统安全性依赖于收发双方使用的系统参数的安全性,系统参数相当于传统密码学中的密钥。此处我们只分析实值参数,不妨假设使用双精度(为2^{-32}),方案共有4个实值参数(x_0, r, l, ε),则系统的参数空间为$2^{32\times4}=2^{128}$,相当于有近128位的密钥空间。就目前计算条件来看,可对抗穷举攻击。

4.2 密钥的敏感性分析

密钥的敏感性也就是密钥的微小变化将最终导致密文的显著变化,该特性将有助于抵抗唯密文攻击,也是密码学设计所要求的特性[11]。为了测试对密钥(即系统参数)的敏感性,我们按以下步骤进行实验:

step1:对Woman图像,仍然使用3中的系统参数,但$x_0=0.4$,得到的加密图见图5(b);

step2:对参数x_0进行微小扰动,取值为0.400001,得到的加密图见图5(c);

step3:对初值ε进行微小扰动,取值为0.600001,得到的加密图见图5(d).

从图5(b),(c),(d)看出使用不同的参数得到了不同的加密图像,为更好地解释它们之间的不同,我们按如下公式计算他们之间的相关系数

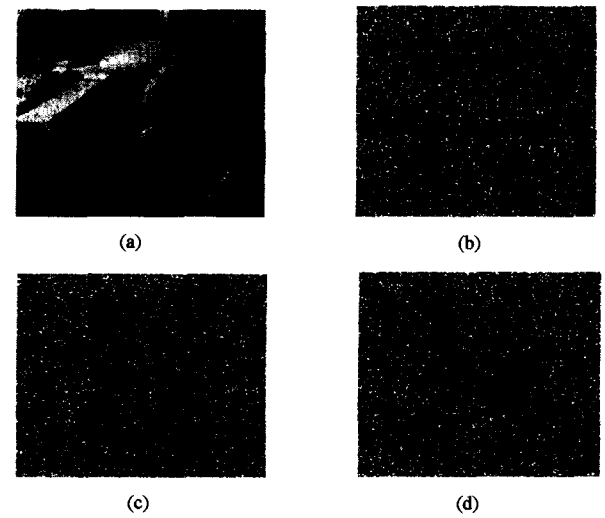
$$C_r=\frac{M\sum_{i=1}^{M}(x_i\times y_i)-\sum_{i=1}^{M}x_i\times\sum_{i=1}^{M}y_i}{\sqrt{(M\sum_{i=1}^{M}x_i^2-(\sum_{i=1}^{M}x_i)^2)\times(M\sum_{i=1}^{M}y_i^2-(\sum_{i=1}^{M}y_i)^2)}} \quad (4)$$

式中M为图像像素总数,x和y分别代表两个图像对应点处的像素值。经过计算,得到表1。

从表1看出相关系数非常小,接近于零,也就是说对系统参数进行微小扰动,将得到完全不相关的加密图像,表明密文对密钥具有高度敏感性。

表1 图像相关系数

计算对象	相关系数C_r
图5(b)和图5(c)	0.00671
图5(b)和图5(c)	−0.00749
图5(b)和图5(c)	−0.00685



(a)为Woman原始图像,(b),(c)和(d)是加密后的图像,
其中(c)和(d)分别为扰动了部分参数后得到的加密图像。

图5 密钥敏感性测试

结束语 本文基于混沌映像格子(CML)提出了一种新颖的图像保密通信方案。由于混沌序列对CML中的耦合系数、驱动序列初值等极端敏感,使得破译混沌序列变得困难。发送方利用CML快速产生二值时空混沌序列,并使用异或加密手段,使得系统的加密速度得到了改善。最后还对系统密钥空间、密钥敏感性等密码学特性进行了分析,数值实验验证了方案的可行性和正确性。本文后续工作将研究方案在对抗其他密码学分析手段如线性分析、差分分析等的能力,并以此进一步完善和改进我们的方案。

参考文献

[1] Jakimoski G, Kocarev L. Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE trans. on CAS-I, 2001,48(2):136-169
[2] Chen G R, Mao Y B, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 2004,21(3):749-761
[3] Wang X G, Meng Z N, Gong X F. Spread-spectrum communication using binary spatiotemporal chaotic codes. Physics Letters A, 2005,334(1):30-36
[4] García P, Jiménez J. Communication through chaotic map systems. Phys. Lett. A,2003,298(1):35-40
[5] Li Ping, Li Zhong, Halanga W A, et al. A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map. Physics Letters A, 2006,349(6):467-473
[6] Kaneko K. Theory and application of coupled map lattices. John Wiley & Sons, 1993
[7] Wang S H, Liu W R, Lu H P, et al. Periodicity of chaotic trajectories in realizations of finite computer precisions and its implication in chaos communications. Int J Mod Phys B, 2004,18(17-19):3617-2622
[8] Hu G, Xiao J H, Yang J Z, et al. Synchronization of Spatiotemporal Chaos and its Application. Physical Review E, 1997,56(3):2738-2746
[9] Xiao J H, Hu G, Qu Z L. Synchronization of spatiotemporal chaos and its application to multichannel spread-spectrum communication. Physical Review E, 1996,77(20):4162-4165
[10] Jiang Y, Parmananda P. Synchronization of spatiotemporal chaos in asymmetrically coupled map lattices. Physical Review E, 1998,57(4):4135-4139
[11] Schneier B. Applied cryptography second edition: protocols, algorithms, and source code in c. New York: John Wiley & Sons, 1996