一种基于时空混沌的数字图像加密系统设计与分析*)

彭 军[1] 刘勇国[2] 陈应祖[1] 张 伟[3] 廖晓峰[4]

(重庆科技学院电子信息工程学院 重庆 400050)[1] (电子科技大学计算机科学与工程学院 成都 610054)[2]

(重庆教育学院计算机与现代教育技术系 重庆 400067)[3]

(重庆大学计算机科学与工程学院 重庆 400044)[4]

摘 要 基于时空混沌设计了一种图像加密系统。将128比特长度的加密密钥划分成2个等长的子密钥,分别驱动2个不同的混沌系统以产生时空混沌序列矩阵,再与原始图像异或实现图像的加密处理。对系统的分析结果表明,该系统不但具有容易快速实现、密钥空间大等特点,而且利用混沌系统对初值参数的敏感依赖性,很好地实现了对密钥的敏感特性。本系统可广泛应用于Internet上的数字图像加密传输。

关键词 时空混沌,耦合映像格子,Chen系统,数字图像加密

Design and Analysis of a Digital Image Encryption System Based on Spatiotemporal Chaos

PENG Jun[1] LIU Yong-Guo[2] CHEN Ying-Zhu[1] ZHANG Wei[3] LIAO Xiao-Feng[4]

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

(College of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054)[2]

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

(Department of Computer Science and Engineering, Chongqing University, Chongqing 400044)[4]

Abstract In this paper, a digital image encryption system is presented based on spatiotemporal chaos, in which a 128 bits secret key is divided into two halves subkey to derive two deferent chaotic systems respectively, in order to generate spatiotemporal chaotic sequence matrix, and this matrix will be XOR processed with the source image later. The analysis results indicate that this encryption system can be fast easily implemented, and has a large key space. Moreover, this system is also very sensitive to the secret key, by introducing the nature feature of the chaos into the design of the system such as the sensitivities with respect to initialconditions and control parameters. In last, the encryption system designed in this paper can be widely applied to the digital image encryption transmission in Internet.

Keywords Spatiotemporal chaos, Coupled map lattices, Chen system, Digital image encryption

1 引言

传统的密码学技术如DES、IDEA、Blowfish、RSA等,理论上讲可以用于数字图像加密,但由于数字图像信息量大,使得上述加密算法运算量增加,并且往往需要将二维的图像数据转换成一维的二进制数据流,加密效率难以得到保证。因此有必要研究适合于数字图像数据特点的加密方法。

本文我们将研究一种基于时空混沌的图像加密系统。在该系统中,用一个具有复杂动力学行为的混沌系统去驱动一个低维耦合映像格子模型,以快速产生数字图像加密用的时空混沌序列矩阵,而该序列矩阵对密钥是敏感的。由于混沌序列具有对初值敏感、似噪声和难以预测等良好特性[1,2],使得本系统的复杂度和安全性得以显著提高。

2 图像加密系统设计

2.1 系统框架

本文设计的图像加密系统如图1所示。在该系统中,我们选用了一个Chen混沌系统和一个耦合映像格子模型(CML, Coupled Map Lattices)。

在该系统中,一个长度为128位的密钥被划分成两个等长的子密钥,以分别驱动两个混沌系统(system #1和system #2),其中混沌系统#1的输出还参与到了对混沌系统#2的驱动。系统#2按照某种演变规则产生时空混沌序列矩阵,之后该矩阵与原始图像进行异或得到加密图像。

在选取何种混沌系统时,我们基于如下原则:1)容易用软硬件实现;2)系统动力学行为复杂;3)适合于对图像作加密处理。研究表明[3~5],Chen系统是一个非常容易用电路实现的三阶系统,在相空间有比Lorenz系统和Chua系统更为优越的三维动力学特性,可用于实现安全性更高的加密系统。Chen系统描述如下

$$\frac{dx}{dt}=a(y-x),\frac{dy}{dt}=(c-a)x-xz+cy,\frac{dz}{dt}=xy-bz \quad (1)$$

其中a,b和c为参数,当$a=35$,$b=3$,$c\in[20,28.4]$时Chen系统是混沌的。图2为$a=35$,$b=3$,$c=28$时系统的混沌吸

*)国家自然科学基金(60573047);重庆市科委自然科学基金(CSTC,2005BB2050,2005BB2286);重庆市教委科学技术研究项目基金(KJ051402,KJ051501)。彭 军 副教授,博士,研究方向为网络安全、混沌密码学;刘勇国 副教授,博士后,研究方向为神经网络、入侵检测;陈应祖 工程师,研究方向为计算机应用;张 伟 教授,博士,研究方向为网络安全;廖晓峰 教授,博士生导师,研究方向为神经网络、混沌保密通信。

引子(使用四阶 Runge-Kutta 算法,步长为 0.001)。

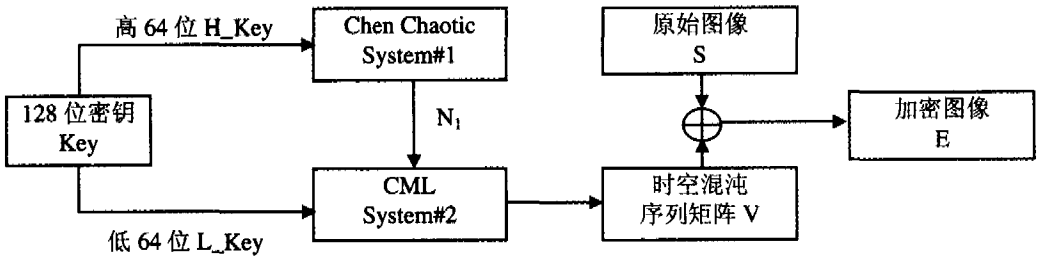
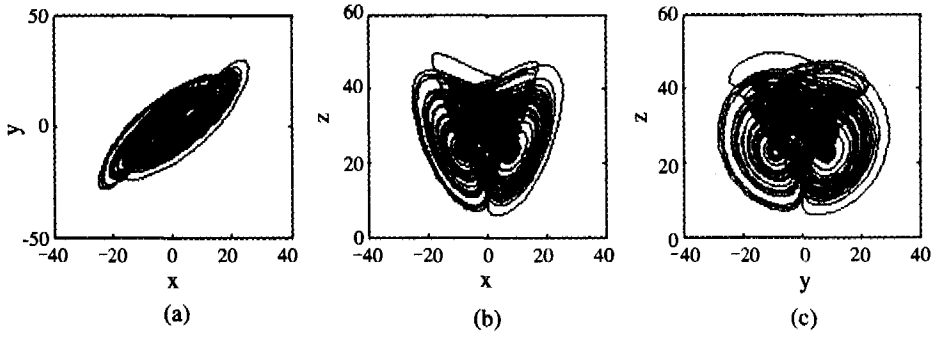


图 1 图像加密系统框图



(a)为 x—y 相图,(b)为 x—z 相图,(c)为 y—z 相图

图 2 Chen 系统的混沌吸引子

此外,耦合映像格子模型是近期时空混沌中研究得较多的一种模型,我们采用文[6]中的一维耦合映像格子模型:

$$x_{n+1}^i=(1-\gamma_1-\gamma_2)f(x_n^i)+\gamma_1 f(x_n^{i-1})+\gamma_2 f(x_n^{i+1}) \quad (2)$$

式中 x_n^i 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,一般取混沌映射。γ_1 和 γ_2 为耦合系数,$\gamma_1>\gamma_2\geqslant 0$,如果 $\gamma_2=0$ 则模型(2)简化为如下形式的单向耦合映像格子模型

$$x_{n+1}^i=(1-\gamma_1)f(x_n^i)+\gamma_1 f(x_n^{i-1}) \quad (3)$$

同时假设模型(2)满足如下周期边界条件

$$x_n^{L+i}=x_n^i,\forall n\in Z \quad (4)$$

其中 L 为系统规模即格子的数量。函数 f 取为 Logistic 映射:

$$f(x_n)=1-ax_n^2,-1\leqslant x_n\leqslant 1 \quad (5)$$

当控制参数 $a=2$ 时,单个格子处于混沌状态。在文[7]中,我们研究了基于模型(2)使用 Chebyshev 混沌映射 $h_{n+1}=\cos(2^w\arccos(h_n))$ 作驱动序列的时空混沌二值序列,并对二值序列的性能进行了详细分析。分析结果表明文[7]产生的时空混沌二值序列具有十分理想的随机性和相关性,且序列的线性复杂度高,易于大批量产生,可广泛应用于保密通信、图像加密等领域。

鉴于以上因素,我们在设计加密系统时,混沌系统选用 Chen 系统和 CML 模型。

2.2 加密算法描述

1)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 $\{s_{ij}\}(i=1,2,\cdots,I\_H;j=1,2,\cdots,I\_W)$。

2)加密密钥 $Key=(K_1,K_2,\cdots,K_{16})$ 为 128 位,其高 64 位为 $H\_Key=(K_1,K_2,\cdots,K_8)$,低 64 位为 $L\_Key=(K_9,K_{10},\cdots,K_{16})$。此处 K_i 代表密钥中的第 i 个字节($i=1,2,\cdots,16$)。

3)按如下规则产生 Chen 系统(1)的初值 (x_0,y_0,z_0) 和迭代次数 N_0

$x_0=(K_1\times K_3\times K_5)\bmod 30$;

$y_0=(K_2\times K_4\times K_6)\bmod 30$;

$z_0=(K_1\times K_4\times K_7)\bmod 30$;

$N_0=200+((K_1+K_2+K_3+\cdots+K_8)\bmod 256)$

设 Chen 系统按上述初值 (x_0,y_0,z_0) 迭代 N_0 次后的状态为 (x_n,y_n,z_n),并由此确定出 CML 模型(2)的演变次数 $N_1=1000+sqrt(x_n^2+y_n^2+z_n^2)$。

4)按如下规则产生 CML 模型(2)中 Chebyshev 驱动方程的初值 h_0 和迭代次数 N_2

$h_0=(K_9+K_{10}+\cdots+K_{16})/256$;

$N_2=(K_9+K_{10}+\cdots+K_{16})\bmod 256$

在 Chebyshev 方程从初值 h_0 出发并演变 N_2+I_H 次后,取后 I_H 个状态值作为 CML 模型的驱动序列。

5)CML 模型在 Chebyshev 序列的驱动下,每个格子(共有 I_H 个格子)演变 N_1+I_W 次,并取后 I_W 个状态值作为加密图像之用。I_H 个格子共有 $I\_H\times I\_W$ 个状态值,构成一个时空混沌序列状态矩阵 V,设为 $\{v_{ij}\}(i=1,2,\cdots,I\_H;j=1,2,\cdots,I\_W)$。

6)对图像进行加密处理,得到加密后的图像 E,此处 $E=\{s_{ij}\oplus floor(|v_{ij}|\times 256)\}(i=1,2,\cdots,I\_H;j=1,2,\cdots,I\_W)$,$\oplus$表示异或操作。

在该加密算法中用到的系统参数设置分别为:CML 模型(2)的耦合系数 $\gamma_1=0.8,\gamma_2=0.01$,Logistic 映射(5)中控制参数 $a=2$,Chebyshev 映射 $h_{n+1}=\cos(2^w\arccos(h_n))$ 中控制参数 $w=2$,格子数 L 取为要加密图像的高度,即 $L=I\_H$。

2.3 解密算法描述

本文设计的加密算法是对称的,也就是加密和解密都使用同一个密钥。此外,加密算法的最后一步操作是异或操作,因而加密结构在不作任何修改的情况下同样适用于解密过程。解密时,在已知加密密钥的前提下,首先获得图像的尺寸信息 I_H 和 I_W,然后执行加密算法中的步骤 2)至 6),对加密图像再次加密即可得到原始图像。

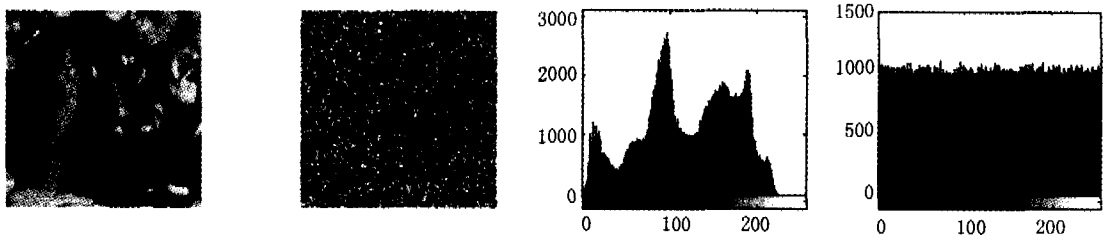
3 系统分析

3.1 效率分析

加密算法中的 Chen 系统和 CML 模型多为迭代映射，可由计算机快速计算。此外，CML 模型中的格子数取为图像的高度，格子在经过有限次演变后即可生成大量的用于图像加密的时空混沌序列矩阵，通过异或运算可快速实现图像加密。解密过程类似于加密过程，可使用与加密过程相同的结构设计，很大程度上降低了硬件的实现成本。

3.2 数值实验分析

使用 Matlab 6.1 工具，对分辨率为 512×512 像素的 peppers 图像进行加密实验。密钥 Key 取为 Jha78xgat5BwKE3s(共 16 个字符)，实验结果如图 3 所示。实验表明，加密后图像无法辨认，并且密图像的像素灰度值统计分布与源图像的完全不同，近似于均匀分布。



(a)为 Peppers 源图像；(b)为加密后的图像；(c)为原图像灰度直方图；(d)为加密图像灰度直方图

图 3 加密结果

3.3 密钥空间分析

我们知道拥有一个大的密钥空间对提高系统的安全性是非常重要的。由算法结构可知，本系统的安全性依赖于密钥的安全。密钥长度设计成 128 位，如果公开混沌系统的参数设置，则系统的密钥空间为 2^{128}，就目前计算条件来看，对系统进行穷举攻击是困难的或是不现实的。若将混沌系统控制参数也计算在内，则密钥空间会更大。

3.4 对密钥的敏感性分析

一个好的加密算法应该实现密文对密钥的敏感性，也就是密钥的微小变化将导致密文的显著变化，该特性将有助于抵抗唯密文攻击。众所周知，混沌系统具有拓扑共扼性，对系统初值和控制参数非常敏感，它们的微小差异都将快速地扩散和传递到整个吸引域空间中。在加密系统中引入混沌，将有效地提高系统的安全性和复杂性。

由算法可知，混沌系统 #1 和 #2 的初值和迭代次数都由密钥生成，而系统 #2 的时空格子演变次数由系统 #1 驱动，这种结构使得密钥的细微变化将会得到完全不同的时空混沌序列，进而导致加密图像的巨大变化。实验数据也验证了我们的分析。在图 4 中，展示的是分别使用密钥 Key1 = Jha78xgat5BwKE3t 和 Key2 = kha78xgat5BwKE3s(它们与源密钥 Key 分别只相差一个字符，即首字符或尾字符不同)对图 3(b)解密得到的图像，均不能得到正确的源图像，而使用原始密钥 Key 却能正确解密出原始图像，表现出密文对密钥的敏感性。

(a)为使用密钥 Key1 的解密图；(b)为使用密钥 Key2 的解密图；(c)为使用密钥 Key 的解密图

图 4 解密结果

结论 本文设计了一个基于时空混沌的图像加密系统并对其进行了分析。该系统具有密钥空间大、对密钥敏感、容易快速实现等特点。在加密算法设计中，引入了多个混沌系统，由于混沌信号对初值和参数的极其敏感性，且混沌信号具有类似噪声的宽频谱特性等，使得攻击者难以对系统进行分析和预测，提高了系统的复杂性和安全性。本系统可广泛用于 Internet 上的数字图像加密传输。

参 考 文 献

1 Lin H B. Chaos. Singapore: World Scientific, 1994

2 Zbigniew K, Szezepanski J. Application of discrete chaotic dynamical systems in cryptography - DCC method. International Journal of Bifurcation and Chaos, 1999, 9(6):1121~1135

3 Chen G, Dong X. From chaos to order methodologies, perspectives, and applications. Singapore: World Scientific, 1998

4 Ueta T, Chen G R. Bifurcation analysis of Chen's equation. International Journal of Bifurcation and Chaos, 2000, 10(8):1917~1931

5 Yassen M T. Chaos control of Chen chaotic dynamical system. Chaos, Solitons & Fractals, 2003, 15(2):271~283

6 Aranson I, Golomb D, Sompolinsky H. Spatial coherence and temporal chaos in macroscopic with asymmetrical couplings. Physical Review E, 1992, 68(24):3495~3498

7 彭军，李学明，张伟，等. 基于耦合映像格子模型的时空混沌二值序列及其性能分析. 计算机科学，2005，32(2):196~198，232