基于超混沌映射和加法模运算的图像保密通信方案

潘 勃 冯金富 陶 茜 李 骜
(空军工程大学工程学院 西安 710038)

摘 要 提出了一种基于Clifford超混沌映射的图像加密方案,发送方利用Clifford映射快速地产生混沌序列,对图像在时域作加密预处理;然后通过简单的加法模运算对像素的灰度值进行替换与扩散,并且在每次迭代中采用不同的密钥。经通信双方同步之后,接收方即可解密出原始图像。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 Clifford映射,混沌序列,图像加密,加法模运算
中图法分类号 TP309 **文献标识码** A

Image Encryption Communication Scheme Based on Clifford Map and Additive Modular Arithmetic

PAN Bo FENG Jin-fu TAO Qian LI Qian
(Engineering College, Air Force Engineering University, Xi'an 710038, China)

Abstract Based on Clifford super chaotic map, a novel image secure communication scheme was proposed. In this scheme, the process of confusion permutes a plain-image with Clifford map for the pretreatment, and process of diffusion is based on additive modular arithmetic. In every iteration, the arithmetic adopts the different keys. Once the synchronization of the communication between the sender and recevier is satisfied, the encrypted image can be correctly recovered into the source image. The results of computer numerical stimulation indicate the sheme proposed is feasible. Finally, we analyzed some cryptography properties of the scheme such as the key space and the sensitivity of the encrypted with respect to the secret key.

Keywords Clifford map, Chaotic sequences, Image encryption, Additive modular

1 引言

混沌现象是非线性系统的一种内在类似随机过程的表现,混沌系统产生的混沌信号具有类噪声、结构复杂以及对初始条件极端敏感的特性,因而被广泛地应用于设计加密系统[1]。目前国内外大多数文献都采用将置乱像素位置的加密方式与置换像素值的加密方式结合起来,对原始图像经过预处理和再加密两步进行。由于在加密过程中图像的位置信息与像素值信息均被混沌序列加密,使得攻击者破译密文的难度增加,因而这种加密方式的安全性有很大提高。

本文提出的加密方案主要由两部分构成,即利用超混沌Clifford映射置乱过程和基于加法模运算的像素扩散过程。在进行复合加密时,使用不同的混沌系统或者在同一系统中使用不同的系统参数,充分利用混沌序列的密钥敏感性,以此保证加密结果的抗攻击性。这样也大大增加了可以作为密钥的参数个数,从而增加了密钥空间[2]。

2 图像预处理

超混沌序列是一种特殊的混沌系统,通常具有两个或两个以上正的Lyapunov指数的混沌系统称为超混沌系统。正的Lyapunov指数越多,系统轨道不稳定的方向越多,系统的随机性越强,其抗破译能力越高[2-4]。因此,它们更适合于图像加密。

Clifford是一种超混沌系统,该系统表达式如下:

$$\begin{cases} x_{k+1}=\sin(ay_k)-z\cos(bx_k) \\ y_{k+1}=z\sin(cx_k)-\cos(dy_k) \\ z_{k+1}=e\cos(bx_k) \end{cases} \tag{1}$$

设定初值:$x=-10, y=-0.1, z=-1.0, r=0, s=0, t=0, a=2.24, b=0.43, c=-0.65, d=-2.43, e=1.0$时,迭代1000次,Clifford映射处于混沌状态。绘制出Clifford迭代轨迹如图1所示。

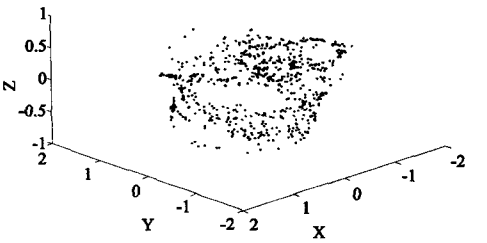

图1 Clifford迭代轨迹

到稿日期:2008-09-09 返修日期:2008-12-23 本文受国家高技术研究发展计划(863)项目(2007AAJ127),空军预研项目(KJ08053)资助。
潘 勃(1983-),男,博士生,主要研究方向为混沌保密通信、武器系统抗干扰技术等,E-mail:gcxypanbo@yahoo.cn;冯金富(1964-),男,教授,博士生导师,主要研究方向为武器系统与控制、多传感器信息融合、武器控制系统等;陶 茜(1983-),女,博士生,主要研究方向为系统工程与智能决策;李 骜(1981-),男,博士生,主要研究方向为机载制导武器系统技术与运用。

数字图像由图像像素的灰度值来描述，将图像在时域中加密，就是通过对像素位置置乱或灰度值的置换来实现。应用式(1)的超混沌序列先对图像进行预处理。本文利用 Clifford 映射产生三维混沌序列，设原始图像 I 的大小为 $N\times N$，则 $i=\{1,2,3,\cdots,N^2\}$ 相应的预处理算法描述如下[8]：

Step 1　设定 Clifford 映射的初始值 X_0,Y_0,Z_0，系统每次迭代产生 3 个混沌值：X_i,Y_i,Z_i；

Step 2　取 X_i,Y_i,Z_i 的小数部分，由于混沌轨道的遍历性，采用该方法数字化后的伪随机二值序列均匀分布。以 X_i 为例，$X_i=(0,d_1,d_2,d_3,\cdots d_p)$，$p$ 为指定的精度，那么，$(d_1,d_2,d_3,\cdots d_p)$ 就可以构成一个伪随机序列。将 3 个混沌值的第 i 位提取，并组成一个新的十进制整数 S；

Step 3　对 S 作取模运算，并将结果表示成一个二进制序列；

Step 4　将原始图像 I 的像素值转化为二进制，并与 Step 3 所得的二进制序列做异或运算；

Step 5　再将所得结果转化为十进制，就完成了对图像像素位置置乱的预处理。

本文设计的算法使用 Clifford 映射来置乱，其根本原理还是通过做异或运算来置换像素值，因而安全性不够高，很难抵御已知明文攻击[8,9]。因而，需要对预处理后的图像做进一步加密。

3　像素值扩散

在以上预处理的基础上，本文将置乱像素位置的加密方式与像素值扩散的加密方式结合起来，对原始图像进行预处理和再加密[5,6]。像素灰度值扩散是将每一位明文和每一位密钥的影响尽可能地作用到较多的输出密文位中去。这种加密目的是有效隐藏明文的统计特性，使得明文图像即便是一个像素灰度值都能使整幅图像的灰度值改变，这样可以有效地抵抗统计和抗差分攻击。本文在文献[10]的基础上引入灰度值扩散系数，相应的扩散算法描述如下：

设加密后图像 Z 的大小为 $N\times N$，则图像像素值为 $Z(i)$，其中 $i\in(1,2,3,\cdots,N\times N)$，不妨设 $D(i)$ 表示明文图像的第 i 个像素点的灰度值，$C(i)$ 表示密文图像第 i 个像素值的灰度值，L 为图像的灰度级别。则本文采用的加法模运算的扩散算法为：

$$C(i)=C(i-1)\oplus(D(i)+K_1D(i)+K_2C(i)) \bmod L \quad (2)$$

其中，K_1,K_2 为灰度值扩散系数，这里取 $K_1,K_2\in(1,,2,\cdots,L)$。而 $D(N^2+1),C(0),K_1,K_2$ 则作为像素值扩散阶段的密钥。算法需要从预处理图像的第一个像素点 $D(1)$ 算起，一次运算直到最后一个像素点 $D(N^2)$ 为止，得到再加密的图像 Z'。

算法的解密过程则是相反的：

$$D(i)=(C(i)-K_1D(i+1)-K_2C(i-1))\oplus C(i-1) \bmod L \quad (3)$$

与加密过程相反，解密过程需要按照式(3)的方法，从密文 Z' 的最后一个像素点 $Z'(N^2)$ 开始运算到第一个像素点 $Z'(1)$。也就是要从最后一个像素点 $C(N^2)$ 运算到第一个像素点 $C(1)$，为方便表示，下文分别用 c_1,c_2 代替 $C(N^2),C(1)$。

4　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去驱动保密通信系统，以产生时空混沌实值序列，二值化后对原始图像进行加密处理，再送往通信信道接收。同时，将密钥(系统参数)使用安全信道传输给接收方，以便接收方的响应系统的产生与发送方时空混沌序列的，接受方采用相同的混沌序列二值化方法即可解密出原始图像。

保密通信方案实现的前提是通信的接收双方必须同步，文献[9,11]的研究表明：在一定同步条件下，收发双方可以实现同步通信。如果采用耦合同步的方法，发送方可以用一个混沌信号作为初始序列去驱动加密系统，并且当耦合系数取适当值时，发送方和接收方的加解、密系统可以实现时空同步。

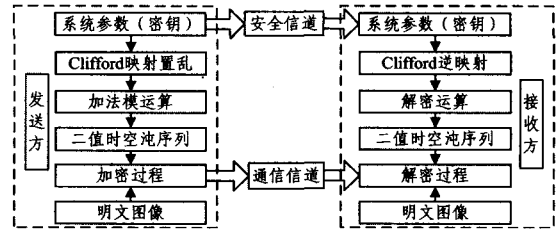

图 2　图像保密通信方案

5　仿真结果及分析

实验环境为：PIV 2.4GHz，内存为 768M，硬盘为 80G 的个人计算机，整个程序在 Windows XP 操作平台下完成，软件使用 MATLAB 7.0，明文图像选取 Cameraman，灰度值为 256，大小 256×256，对本方案，对其进行仿真实验，具体参数如下：

Clifford 映射初始条件为 $x_0=0.5238,y_0=0.2342,z_0=0.6774$；像素扩散算法初始条件是迭代次数为 3 轮，且 $N=256,L=256$。随机输入密钥第一轮迭代 $c_1=65,c_2=120$；第二轮迭代值取 $c_1=60,c_2=125$；第三轮迭代值 $c_1=65,c_2=128$。测试结果如图 3 所示。

(a)原始图像　(b)加密后的密文图像

图 3　加密前后的图像

6　算法分析

6.1　密钥空间分析

系统的安全依赖于收发双方使用的系统参数的安全性(密钥)。如本文算法迭代 k 轮，混沌系统初值分别为 x_0,y_0,z_0，用户输出置乱密钥 K_1,K_2 和扩散密钥 c_1,c_2，其中 $K_1,K_2\in[0,L),c_1,c_2,\in[0,L)$。则密钥空间为置乱密钥和扩散密钥的乘积，$M=(x_0y_0z_0K_1K_2c_1c_2)^k$，且扩散密钥的空间由 L 决定，该算法的密钥空间为 $M=L^{7k}$。不妨设使用双精度为 2^{-32}，则该系统的参数空间为 $2^{32\times7}=2^{224}$，相当于有近 224 位的密钥空间，就目前的计算条件来看，本算法可以有效地对抗穷举攻击。

6.2　密钥敏感性分析

密钥的敏感性分析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明文攻击[7]。为了测试对密钥的敏感性，本文按以下步骤进行实验：

Step 1　对 Cameraman 图像（如原始图像图 4(a)所示，仍然使用第 5 节中的系统参数，但 x_0 取 0.5237，得到的加密图像如图 4(b)所示；

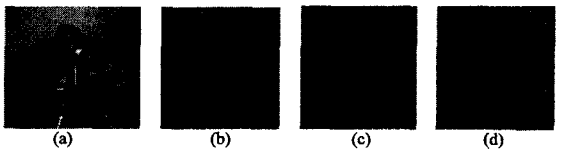

图 4　密钥敏感性分析

Step 2　对参数 z_0 进行微小扰动，取值为 0.6775，得到的加密图像如图 4(c)所示；

Step 3　对初值 c_1 进行小扰动，保持 c_2 取值不变，而 c_1 取值为 64，其它迭代值不变，最终得到的加密图像如图 4(d)所示；

对密钥敏感性的实验表明，本文所给出的算法加密效果理想，加密后的图像没有留下明文图像的痕迹，而密钥的细微差别便会导致无法正确解密图像。

6.3　灰度直方图比较

通过选用第 5 节中的一组密钥加密图像，明文图像和密文图像的灰度直方图如图 5 所示。

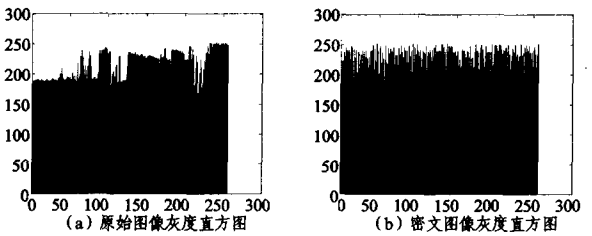

图 5　灰度直方图比较

可以直观地看出，两幅图像的灰度统计值有着明显的差异，密文图像的灰度值分布均匀，灰度变化平均值较为理想，相邻像素相关性小，从能量分布的角度讲，加密扰乱了原始图像的能量分布，因此说明算法的灰度扩散是有效的，该算法的加密效果较好，安全性较高。

6.4　相邻两个像素的相关性分析

通过比较明文图像与密文图像的相邻像素的相关性，可以考察算法对图像置乱的程度[10]。本文分别对明文图像和密文图像中水平相邻、垂直相邻和对角线相邻的 3 个像素的相关性进行测试，随机选取 1000 对水平竖直对角方向相邻像素，利用以下公式进行计算：

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)]^2$$

$$C(x,y)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)][y_i-E(y)]$$

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x_i)][y_i-E(y_i)]$$

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

其中，x,y 代表随机选取的这 1000 对相邻像素的灰度值。测试的结果如表 1 所列，可看出加密后的图像与明文图像相比，其相邻像素的相关性大大降低了。

表 1　明、密文的像素相关性对比

	明文图像灰度值相关性	密文图像灰度值相关性
水平方向	0.9638	0.0432
竖直方向	0.9659	0.0114
对角方向	0.9291	0.0131

结束语　本文基于 Clifford 映射和简单的加法模运算完成了对明文图像的置乱和像素的灰度值的替换与扩散，并且每一轮迭代采用不同的扩散密钥。经仿真分析，该方案可以根据安全需求具有足够的密钥空间，对密钥以及明文都非常具有敏感性，能够抵抗灰度值或者相关性的统计分析，并且计算简单，速度快，适用于图像加密以及实时加密传输。本文的后续工作将研究对抗其它密码学分析手段，如线形分析、差分分析等的能力，并以此改进本文的方案。

参 考 文 献

[1]　李月，杨宝俊. 混沌振子系统(L-Y)与检测[M]. 北京：科学出版社，2007

[2]　徐茂智，游林. 信息安全与密码学[M]. 北京：清华大学出版社，2007

[3]　黄润生，黄浩. 混沌理论及其应用[M]. 武汉：武汉大学出版社，2005

[4]　陈尔东. 基于混沌理论的信息加密方法研究[D]. 大连：大连理工大学，2005

[5]　Jakimoski G, Kocarev L. Chaos and cryptography: block encryption ciphers based on chaotic maps[J]. IEEE trans. on CAS-I, 2001, 48(2): 136-169

[6]　陈永红，黄席德. 基于混沌序列的图像加密解密算法[J]. 计算机工程，2004，30(21)：104-106

[7]　郭建胜，沈林章，张锋. 基于混沌序列的图像加密算法的安全性分析[J]. 计算机工程，2008，34(8)：12-15

[8]　李鹏，张雪峰，田东平. 基于 Hyperhenon 映射的数字图像 DCT 域加密技术[J]. 计算机工程与设计，2008，29(9)：2212-2214

[9]　张健，于晓洋，任洪娥. 基于 cat 映射和 Lu 混沌映射的图像加密方案[J]. 电子器件，2007，30(1)：155-157

[10]　石熙，张伟. 基于广义猫影射和加法模运算的快速图像加密系统[J]. 计算机科学，2008，35(6)：190-192

[11]　游明英，彭军，金尚柱，等. 一种新颖的基于混沌映像格子的图像保密通信方案[J]. 计算机科学，2008，35(5)：260-262

(上接第 249 页)

[7]　Gartner T, Driessens K, Ramon J. Graph kernels and Gaussian processes for relational reinforcement learning[C]// Proceeding of the International Conference on Inductive Logic Programming (ILP'03). 2003

[8]　Mackay D. Introduction to Gaussian processes[OL]. http://wol.ra.phy.cam.ac.uk/mackay

[9]　Chu Wei, Ghahramani Z. Gaussian Processes for Ordinal Regression[J]. Journal of Machine Learning Research, 2005, 6: 1019-1041

[10]　Liu Quan, Gao Yang, Chen Daoxu, et al. A Heuristic Contour Prolog List Method Used in Logical Reinforcement Learning [J]. Journal of Information & Computational Science, 2008, 5(5): 2001-2007

[11]　Liu Quan, Gao Yang, Cui Zhiming, et al. An Tableau Automated Theorem Proving Method Using Logical Reinforcement Learning[C]// Advances in Computation and Intelligence, LNAI, 4683. 2007

[12]　高阳，陈世福，陆鑫. 强化学习研究综述[J]. 自动化学报，2004，33(1)：86-99