基于广义猫映射和加法模运算的快速图像加密系统*)

石 熙[1] 张 伟[1,2]

(重庆教育学院计算机与现代教育技术系 重庆 400067)[1] (重庆大学计算机科学与工程学院 重庆 400044)[2]

摘 要 二维的混沌映射因其双瞳剪水初值敏感性以及伪随机性而广泛应用于图像加密。本文提出一种快速的图像加密系统,利用扩展的猫映射对图像进行置乱,通过简单的加法模运算对像素的灰度值进行替代与扩散,并且在每一轮迭代中采用不同的密钥。

关键词 广义猫映射,加法模运算,图像加密

Fast Image Encryption System Based on General Cat Map and Additive Modular Arithmetic

SHI Xi[1] ZHANG Wei[1,2]

(Department of Computer and Modern Education Technology, Chongqing Education College, Chongqing 400067, China)[1]

(Department of Computer Science and Engineering, Chongqing University, Chongqing 400044, China)[2]

Abstract With the properties of sensitivity to initial conditions, control parameters and pseudo-randomness, 2D chaotic maps have been widely used in image encryption. This paper proposes a fast image encryption system, its process of confusion permutes a plain-image with general cat map, its process of diffusion is based on additive modular arithmetic, and it adopts the different key in every iteration.

Keywords General cat map, Additive modular arithmetic, Image encryption

1 引言

通过网络传输图像以及其他多媒体文件极大地便利了我们的生活,而如何安全地传输也变得越来越重要。图像加密技术正是解决这个问题的关键。相对于普通文本数据的加密,图像文件具有数据量大、数据冗余度高等特点,这是图像加密需要面对的问题。而混沌映射以及对初值的敏感性、遍历性,以及伪随机性被广泛地用于设计加密系统。由于计算机中的图像文件通常由一个矩阵表示,因此使用二维的混沌映射可以快速地置乱每一个像素的位置以及打破像素之间的相关性。当然,我们还需要通过一个扩散的过程来改变像素的值,以打破明文图像与密文图像之间的关系[1,2]。

本文提出的图像加密算法主要由两个部分组成,即利用二维的混沌映射置乱过程和一个简单的基于加法的扩散过程[3,4]。离散的广义猫映射及其良好的初值敏感性和快速混乱的特性非常适合用来置乱图像像素位置。

2 置乱

经典的 anorld 猫映射是一个可逆的二维混沌映射,定义如下:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod}\ 1) \quad (1)$$

其中 x_n, y_n 的取值在 0 和 1 之间。映射(1)线性变换矩阵的判别式为 1,则映射具有保面积的特性。

广义的猫映射定义为

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod}\ N) \quad (2)$$

其中,$A = \begin{bmatrix} 1 & u \\ v & uv+1 \end{bmatrix}$,$u, v$ 为正整数,x_n, y_n 的取值也扩展到 0 和 N 之间。它是由映射(1)引入两个参数并离散化得来的。映射(2)的线性变换矩阵的判别式仍然为 1,即 $\det A = 1$,保证了该映射是保面积的一一映射。并且,众所周知加密运算是有限域上的变换,要将二维猫映射用于加密,必须将其离散化。

容易验证,映射(2)仍然具有快速混乱原序列和对初值的敏感依赖等重要特性。但离散化扩展必定会损失一些有用的混沌特性,比如映射(2)存在周期。这也是我们在设计算法的时候应当避免的。

映射(2)非常适用于置乱像素的位置[3]。加密时将明文图像每个像素的位置坐标(i, j)作为初值(x_0, y_0),经过 N 次迭代,得到该像素坐标的新位置(x_n, y_n)。解密时则将 A 的逆矩阵作为变换矩阵,迭代相同的次数即可。本文设计的算法使用映射(2)来置乱,但在 N 轮迭代中的每一轮都采用不同的矩阵,也就是说每一轮迭代的变换矩阵的参数 u 和 v 的值都不同。这将增大密钥的空间,并增加迭代恢复的难度,增强算法的安全性。

3 扩散

像素灰度值的扩散是图像加密算法中非常重要的环节。首先,可以改变每一个像素的灰度值,从而改变整个图像的灰度统计值。其次,扩散的过程使得明文图像即便是一个像素的灰度值的改变都能扩散到整幅图像的灰度值的改变,这可以避免选择明文攻击。

本文采用一个简单的基于加法和模运算的扩散方法:

$$q_i = (p_i + p_{i+1} + q_{i-1}) (\mathrm{mod}\ L) \quad (3)$$

其中 p_i 表示明文图像第 i 个像素的灰度值,q_i 则表示密文图像第 i 个像素的灰度值,L 是图像的灰度级别。若图像为 $N \times N$ 的大小,则 $i = \{1, 2, 3, \cdots, N^2-1, N^2\}$,而 p_{N^2+1}, q_0 则作

*)中国博士后科学基金一等资助项目(No. 20060390175);重庆市科委自然科学基金资助项目(No. CSTC 2005BB2286);重庆市教委资助项目(No. kj051501)。石 熙 硕士,主要研究方向为信息安全、图像加密;张 伟 教授,博士后,主要研究方向为信息安全、计算智能与数据挖掘。

为扩散阶段的密钥。加密需要从明文的第一个像素 p_1 起，依次运算到最后一个像素。

解密的运算则是相反的：

$$p_i=(q_i-p_{i+1}-q_{i-1})(\mathrm{mod}\ L) \tag{4}$$

并且，解密需要从密文图像的最后一位像素起，运算到第一个像素。也即是 i 从 N^2 逐一递减到 1。

考虑到公式(3)的灰度值扩散方式是将图像的像素按一定的顺序排列依次运算，所以当两幅明文图像只有第 i 个像素的灰度值不同，则扩散后的两幅密文图像只有第 i 位以后的像素的灰度值才会不同。为了确保明文灰度值的任何变化都可以扩散到整个图像，扩散运算至少进行 2 轮，并且从第二轮开始，q_0 应等于前一轮运算后的最后一个像素 q_{N^2}。即若 I_n 表示第 n 次扩散运算结束后的图像矩阵，第二轮运算的 $q_0=I_1(N,N)$。

4 算法的描述

本文设计的基于广义猫映射的图像加密算法具体由以下几个步骤组成：

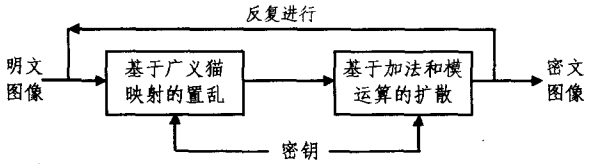


图 1

(1)根据明文图像确定 N 及 L，再输入第 i 轮的置乱密钥 u_i，v_i，扩散密钥 b_i，e_i，其中，u_i，$v_i\in[0,N)$，b_i，$e_i\in[0,L)$；

(2)根据置乱密钥 u_i，v_i，用映射(2)进行一轮迭代，置乱明文像素的位置；

(3)根据扩散密钥 b_i，e_i，利用公式(3)，进行至少 2 轮迭代；

(4)若满足迭代轮数要求，即输出密文图像，否则根据安全需要重复进行步骤(2)(3)。

我们以一幅 256×256 的 8 位灰度图为例，只进行 2 轮迭代，则 $N=256$，$L=256$。随机输入密钥第一轮迭代为 $u_1=56$，$v_1=119$，$u_2=170$，$v_2=215$，第二轮为 $b_1=65$，$e_1=123$，$b_2=237$，$e_2=189$。测试结果如下。

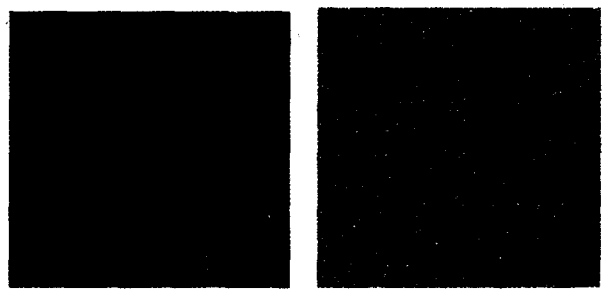


图 2

5 算法分析

5.1 密钥分析

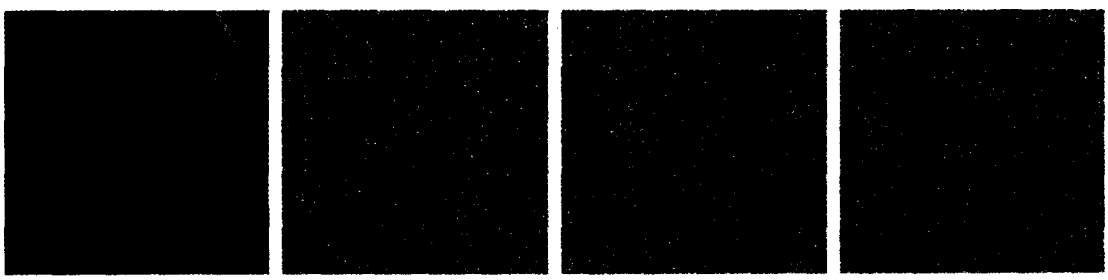
本文算法若要求迭代 k 轮，则用户输入的密钥为 k 组置乱密钥 u_i，v_i 和扩散密钥 b_i，e_i。其中，$i=\{1,2,\cdots,k\}$，u_i，$v_i\in[0,N)$，b_i，$e_i\in[0,L)$。那么，算法的密钥空间则为置乱密钥与扩散密钥的乘积，$S=(uvbe)^k$，而置乱密钥与扩散密钥的空间由 N，L 决定，则算法的密钥空间 $S=(NL)^{2k}$。

以一幅 256×256 的 8 位灰度图为例，$N=256$，$L=256$，密钥空间 $S=2^{32k}$。因此可以根据图像的尺寸和灰度值以及安全需求来决定迭代的轮数。

5.2 对密钥的敏感性

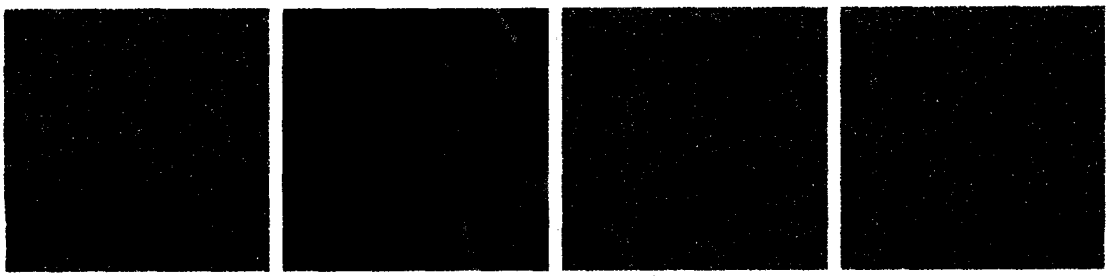
我们以图 2 中的原图为例，仍然做 2 轮迭代，分别测试置乱和扩散环节的密钥敏感度，如图 3 所示。

(1)首先，明文图像如图 3(a)所示，两轮迭代的密钥分别为 $u_1=50$，$v_1=75$，$b_1=150$，$e_1=175$ 以及 $u_2=100$，$v_2=125$，$b_2=200$，$e_2=225$ 密文图像如图 3(b)所示。(2)改变置乱密钥 $u_2=101$，其余参数不变，密文图像如图 3(c)所示。(3)改变扩散密钥 $e_2=226$，其余参数不变，密文图像如图 3(d)所示。



(a) (b) (c) (d)

图 3



(a) (b) (c) (d)

图 4

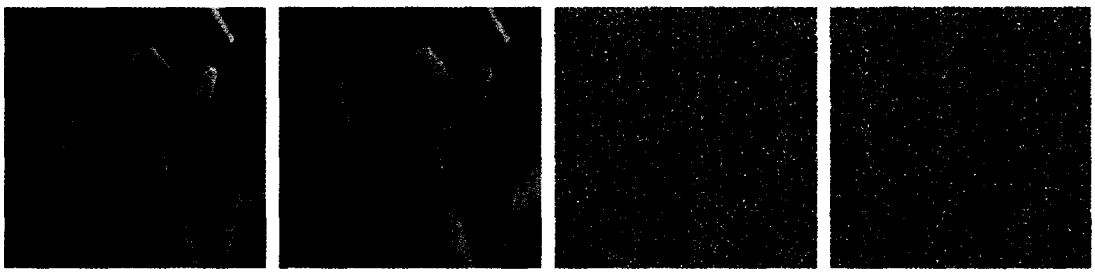
通过比较计算可以得出，尽管置乱密钥只改变了一点，两幅密文图像即图 3(b)与图 3(c)有高达 99.27%的像素灰度值相异；而同样的扩散密钥的改变使密文图像即图 3(b)与图 3(d)没有一个像素灰度值相同。

解密密钥的敏感性测试如图 4 所示。图 4(a)等于图 3(b)，即加密的两轮密钥分别为 $u_1=50, v_1=75, b_1=150, e_1=175$ 以及 $u_2=100, v_2=125, b_2=200, e_2=225$。正确的密钥解密后的图像如图 4(b)所示。若任意更改密钥的一位，都不能得到正确的明文。若改变置乱密钥 $u_2=101$，解密的明文如图 4(c)所示；若改变扩散密钥 $e_2=226$，解密的明文如图 3(d)所示。

5.3 对明文的敏感性分析

加密算法必须对明文足够敏感，明文的任何细微改动都能使密文完全不同。这对抵抗选择明文攻击十分有效。仍然选用 5.2 节中的加密密钥 $u_1=50, v_1=75, b_1=150, e_1=175$ 以及 $u_2=100, v_2=125, b_2=200, e_2=225$，做两轮迭代。两幅明文图像 I_1, I_2 如图 5(a)(b)所示，其中 $I_1(100,150)=164$，$I_2(100,150)=165$。两幅明文图像只有一个像素有一位不同，而肉眼几乎无法分辨。

运算后的密文图像如图 5(c)(d)所示。通过比较计算，可以发现两幅密文图像有 99.2%的像素灰度值不同。



(a) (b) (c) (d)

图 5

5.4 灰度直方图比较

仍然选用 5.2 节的一组密钥加密图像，明文图像和密文图像的灰度直方图的比较如图 6 所示。可以直观地看出，两幅图像即图 3(a)(b)的灰度统计值有着明显的差异，显然密文图像的灰度值分布已经趋于平均，这说明算法的灰度扩散是有效的。

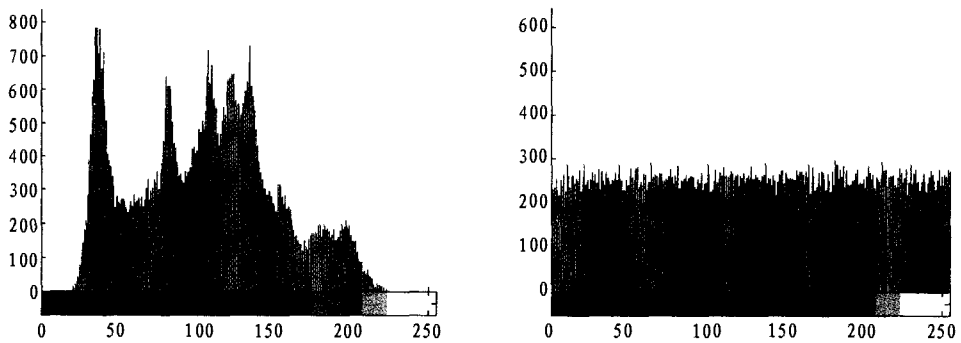


图 6

5.5 相邻两个像素相关性分析

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[5]。分别对明文图像和密文图像即图 3(a)(b)的相邻像素的相关性进行测试，随机选取 1000 对水平方向、竖直方向、对角方向相邻的像素，利用以下公式进行计算。

$$\mathrm{cov}(x,y)=E(x-E(x))(y-E(x))$$

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

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 所示，可以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

	明文图像	密文图像
水平方向	0.9561	0.0307
竖直方向	0.9729	0.0177
对角方向	0.9184	0.0119

结束语 利用混沌映射对初值敏感以及快速混乱的特性对数字图像加密，是近年来一个新的研究方向。本文利用扩展的猫映射对图像进行置乱，通过简单的加法与模运算对像素的灰度值进行替代与扩散，并且在每一轮迭代中采用不同的密钥。经分析，算法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。

参 考 文 献

[1] Schneier B. 应用密码学[M]. 吴世忠，译. 北京：机械工业出版社，2000

[2] William S. 密码编码学与网络安全：原理与实践[M]. 杨明，译. 北京：电子工业出版社，2001

[3] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcat Chaos, 1998, 8(6): 1259

[4] Lian Shiguo, Sun Jinsheng, Wang Zhiquan. Security analysis of a chaos-based image encryption algorithm [J]. Physica, 2005, (A351): 645-661

[5] Chen Guanrong, Mao Yaobin, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons and Fractals, 2004(21): 749-761