第33卷 第10期 计 算 机 工 程 2007年5月
Vol.33 No.10 Computer Engineering May 2007
·安全技术· 文章编号：1000—3428(2007)10—0166—03 文献标识码：A 中图分类号：TP391

一种基于改进的混沌猫映射的图像加密算法

张 燕，黄贤武，刘家胜
（苏州大学电子信息学院，苏州 215021）

摘 要：混沌系统对初始条件和混沌参数非常敏感，生成的混沌序列具有非周期性和伪随机性的特性，近年来在图像加密领域中得到了广泛的应用。该文提出了一种基于改进的混沌猫映射的图像加密算法，该算法利用混沌猫映射和扩散函数相结合来对数字图像进行置乱加密。改进后的混沌猫映射不仅可以基于像素点进行空间域的变换加密，而且可以基于色度域进行变换加密，从而可以有效地抵抗统计攻击。实验结果表明，提出的算法能够得到令人满意的加密效果。

关键词：混沌；图像加密；猫映射；扩散

Image Encryption Algorithm Based on Improved Chaotic Cat Maps

ZHANG Yan, HUANG Xianwu, LIU Jiasheng
(School of Electronics and Information Engineering, Soochow University, Suzhou 215021)

【Abstract】 Chaos is widely used in image encryption because of its high sensitivity to initial conditions and parameters and its generated chaos series without circle and of pseudo stochastic. An image encryption algorithm based on improved chaotic cat maps is proposed. In this method, the image is encrypted by diffusion function and improved chaotic cat maps, which can encrypt image not only based on disordering the positions of image pixels but also based on changing image pixels' value, thereby significantly increasing the resistance to statistical attacks. The method is proved to work well.

【Key words】 Chaos; Image encryption; Cat maps; Diffusion

对于数字图像的安全保密，采用的主要手段是信息隐藏和伪装技术。近年来研究的一种常用的图像加密方法是数字图像置乱变换，其主要有以下3种：(1)基于图像像素点坐标的空间域和频域变换加密；(2)基于图像灰度域变换的加密；(3)基于图像空间域和色度域变换的加密。目前，常用的图像置乱方法主要有：Arnold变换(猫映射)，面包师变换，Standard映射，幻方变换，魔方变换，Hibert曲线，椭圆曲线[1~3]等。

传统的猫映射加密是一种基于图像像素点坐标的空间域变换加密，其存在的一个明显的缺陷就是无法改变原始图像直方图，从而使得恶意攻击者有机会通过直方图来推测原始图像的大致内容。本文对其进行改进，使得猫映射加密不仅可以基于像素点进行空间域的变换加密，而且可以基于色度域进行变换加密，从而可以有效地抵抗统计攻击。同时，因为扩散处理可以将明文中每一位的影响扩散到整个密文中，所以本文利用它来改变图像每个像素点的值，从而使得加密后的图像直方图近似于由随机序列组成的图像直方图。实验结果表明，经过扩散加密后的图像的相关性进一步降低，图像加密效果更令人满意。

1 混沌猫映射

混沌猫映射[4]是由Arnold和Avez提出的一个离散混沌模型：

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \tag{1}$$

其中，(x_n,y_n)是原图像的像素点坐标，(x_{n+1},y_{n+1})是加密图像的像素点坐标，N是图像的大小(一般考虑正方形图形)。于是，混沌猫映射可改写为如下形式的模型：

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N, A = \begin{bmatrix} t & u \\ v & w \end{bmatrix} \tag{2}$$

为了确保以上混沌猫映射是一对一映射，矩阵A的行列式必须满足|A|=1，为此，令

$$A = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$$

混沌猫映射最终可以表述为

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \tag{3}$$

其中，$x_{n+1},y_{n+1},x_n,y_n \in \{0,1,2,\ldots,N-1\}$，a和b均为正整数。

基于此混沌猫映射的图像加密是通过猫映射将原始图像的像素点重新分布，使原始图像变得杂乱无章，从而达到加密的效果。但试验结果表明，混沌猫映射对图像进行加密不能改变图像的直方图 (如图1(b)、图1 (d))，从而给恶意攻击者留下通过直方图来推测图像的大致内容的机会。本文针对猫映射存在的这个问题，对其作了改进。

2 改进的混沌猫映射

由式(3)可见，上述传统的猫映射只是对图像像素点坐标的空间域进行变换，而没有同时对图像的像素值进行变换，使加密后的图像呈现某种规律性，很容易受到已知明文攻击。为了弥补这个缺憾，就需要对传统的猫映射进行改进。本文对传统猫映射作了2步改进。

(1)改进后的猫映射的形式为

作者简介：张 燕(1982－)，女，硕士生，主研方向：图像处理，视频处理；黄贤武，教授、博导；刘家胜，博士生

收稿日期：2006-06-11 **E-mail：**210317042@suda.edu.cn

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ f_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a & 0 \\ b & ab+1 & 0 \\ m & n & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ f_n \end{bmatrix} \bmod N \tag{4}$$

其中，$x_n,y_n \in \{0,1,2,\ldots,N-1\}$，$f_n$和$f_{n+1}$为像素值，a和b均为正整数，m和n为整数。可见，猫映射在改变图像像素点坐标的同时，也改变了对应的像素值，从而使得加密后的图像直方图近似于由随机序列组成的图像直方图。

同时由式(3)可见，无论经过多少次传统猫映射迭代，处在(0,0)位置处的像素始终保持不变。也就是说，如果$(x_0,y_0)=(0,0)$，那么经过n次传统猫映射迭代后，$(x_0^n,y^n{}_0)=(0,0)$。坐标位置(0,0)处的像素点是在正常扫描模式下扫描的第 1 个像素点，如果其在n次置乱过程中都保持不变，就会使攻击者有机会通过比较明文和密文而获得有用信息，从而给整个加密系统构成威胁。为此就需要通过一定的方式将传统猫映射的正常扫描模式改为随机的，从而将(0,0)位置的像素点随机的改变到图像中的任何位置。

(2)对式(3)作改进，形式为

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} + \begin{bmatrix} u \\ v \end{bmatrix} \bmod N \tag{5}$$

其中，a和b正整数，u和v是由Logistic混沌映射[5]随机产生的实值混沌序列。

综合式(4)和式(5)，便可以得到最后改进的猫映射形式为

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ f_{n+1} \end{bmatrix} = \left(\begin{bmatrix} 1 & a & 0 \\ b & ab+1 & 0 \\ m & n & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ f_n \end{bmatrix} + \begin{bmatrix} u \\ v \\ f \end{bmatrix} \right) \bmod N \tag{6}$$

其逆变换形式为

$$\begin{bmatrix} x_n \\ y_n \\ f_n \end{bmatrix} = \begin{bmatrix} ab+1 & -a & 0 \\ -b & 1 & 0 \\ bn-(ab+1)m & am-n & 1 \end{bmatrix} \begin{bmatrix} x_{n+1}-u \\ y_{n+1}-v \\ f_{n+1}-f \end{bmatrix} \bmod N \tag{7}$$

尽管改进的猫映射与传统猫映射相比有一定的改进，可是如果仅用它对图像进行加密，其加密算法和密钥不能有效地分开，加密算法不能公开，不符合现代密码体制的规范。为了弥补这个缺陷，本文在改进的猫映射的基础上，引入了扩散处理过程，其原理如下。

3 扩散处理

在本文加密算法中引入扩散处理，一是为了弥补上述猫映射的缺憾，再者是因为其可以将明文中每一位的影响扩散到整个密文中，这在很大程度上改变了明文的统计特性，从而可以有效地抵抗统计攻击。

根据文献[6]中给出的两种基本类型的扩散函数，本文提出的扩散函数定义为

$$\begin{cases} c(k) = f(x_k,u) \\ q(k) = c(k) \oplus \{[\phi(k) + q^2(k-1) + c(k)] \bmod N\} \end{cases} \tag{8}$$

其中，c(k)是将Logistic混沌映射$f(x_k,u)=x_{k+1}=1-ux_k^2$($x_k$为映射变量，u为系统参数，$-1<x_k<1$，$0<u<2$) 产生的实值混沌序列进行适当比例的抽样放大，经过适当处理后得到自然数混沌序列。φ(k)是待加密的像素点，q(k)是加密后的像素，q(k-1)是前一个已经加密的像素点，N是色度级(如果是 256 色图像，N=256)。上述扩散函数的逆变换为

$$\begin{cases} c(k) = f(x_k,u) \\ \phi(k) = \{[q(k) \oplus c(k)] - q^2(k-1) - c(k) + N\} \bmod N \end{cases} \tag{9}$$

这里，参数设置同式(8)。

4 基于改进混沌猫映射和扩散函数相结合的图像加密解密算法

4.1 加密算法步骤

步骤 1 输入原始图像文件，图像可以用矩阵表示为$A_{N\times N}$，以及加密迭代次数t。

步骤 2 输入初始条件(x_0,u)，由Logistic混沌映射产生一个N×N长的混沌序列$\{x_k|k=0,1,2,\ldots,2Nt-1\}$，对此序列进行适当处理，得到自然数混沌序列，作为扩散处理过程中的c(k)。

步骤 3 对图像运用上述扩散函数进行加密，得到$A'_{N\times N}$。

步骤 4 输入所需参数a、b、m、u、v、f，采用上述的改进猫映射对图像$A'_{N\times N}$进行加密，得到$A''_{N\times N}$。

步骤 5 重复步骤 2~步骤 4 直到迭代达到 t 次为止，得到加密输出图像文件

4.2 解密算法步骤

在得到加密图像文件和正确的密钥的情况下，只需要进行加密过程的逆操作就可以得到正确的解密图像。

5 两种混沌猫映射加密图像比较分析

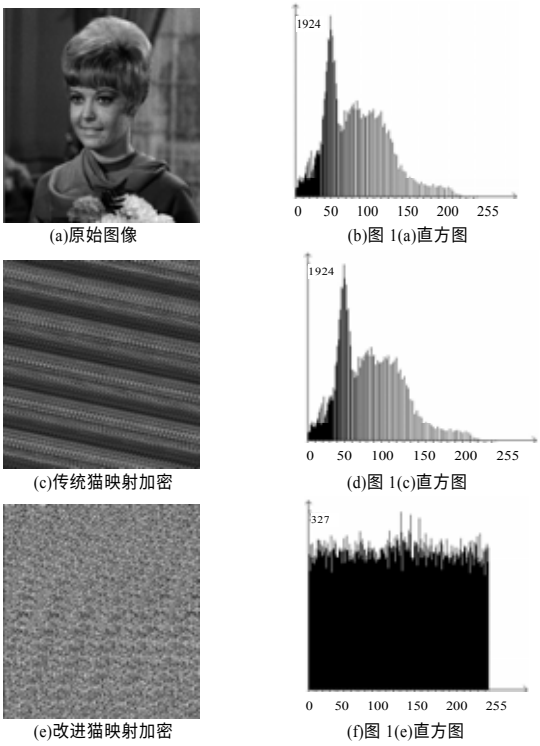
图 1 为在 VC++6.0 编程环境下，分别采用两种混沌猫映射对一幅灰度图像进行加密，试验结果及分析如下。

5.1 密钥空间

与传统的混沌猫映射相比，改进的混沌猫映射多了 m、n、u、v、f5 个参数，因此在密钥空间上后者要比前者大 5 倍。

5.2 直方图

图 1(d)、图 1(f)清楚表明，改进混沌猫映射加密图像的直方图与传统的猫映射加密图像的直方图有着很大的不同，前者更加均匀，更近似于由随机序列组成的图像的直方图，从而使得恶意攻击者无法从直方图来推测图像的大致内容。



(a)原始图像　(b)图 1(a)直方图

(c)传统猫映射加密　(d)图 1(c)直方图

(e)改进猫映射加密　(f)图 1(e)直方图

图 1 猫映射加密对比

5.3 相关性

原图像中相邻像素的相关性很大，为了使图像置乱程度更深，且更加有效地抵抗统计攻击，就须降低相邻像素的相关性。本文从原始图像和加密图像中各选取了 1 000 对像素点来测试其各自在水平方向、垂直方向和对角线方向的相关性，测试结果如表 1 所示。改进猫映射加密图像的相关系数与传统猫映射加密图像的相关系数相比，在垂直方向尽管有略微的增加，但从总体上来说，前者还是有明显降低的。

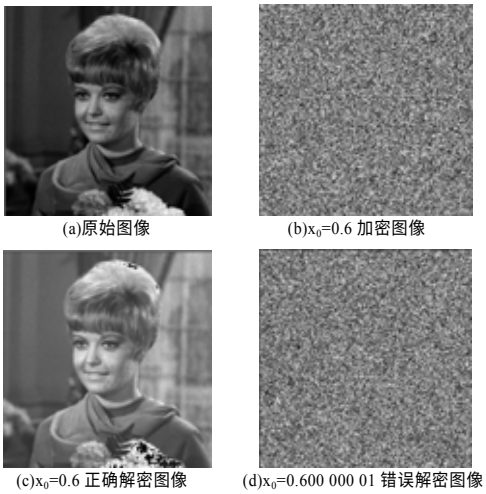
不论从视觉效果，还是从图像置乱程度来看，改进猫映射均优先于传统猫映射。

表 1 两种猫映射加密图像的相关系数比较

	原始图像	传统猫映射加密图像	改进猫映射加密图像
水平方向	0.960 5	0.398 2	0.186 8
垂直方向	0.948 3	0.072 4	0.096 9
对角线方向	0.923 9	0.035 2	0.010 5

6 实验结果及其分析

在VC++6.0 编程环境下利用本文提出的基于改进的混沌猫映射和扩散函数相结合的加密算法对一幅灰度图像进行了加密和解密试验，设置密钥分别为：a=20，b=40，m=5，n=8，u=11，v=5，f=50，x_0=0.6，u=2,t=1。图像加密解密效果如图 2 所示。



(a)原始图像　(b)x_0=0.6 加密图像

(c)x_0=0.6 正确解密图像　(d)x_0=0.600 000 01 错误解密图像

图 2 图像的加密和解密结果

混沌序列对初始值非常敏感，即使初始值有微小的变化也会得到完全不同的解密结果(图 2(d))，如初始值(密匙)x_0=0.600 000 01，u=2.0 时，就无法对图像进行正确解密。

本文从原始图像和加密图像中各选取了 1 000 对像素点来测试其各自在水平方向、垂直方向和对角线方向的相关性，测试结果如表 2 所示。

表 2 本算法加密图像的相关系数比较

	原始图像	本算法加密图像
水平方向	0.960 5	0.008 6
垂直方向	0.948 3	0.044 6
对角线方向	0.923 9	0.007 3

由表 2 可见，利用本算法加密后的图像在水平方向、垂直方向和对角线方向的相关系数都有明显的降低，充分证明了本算法可以有效的抵抗统计攻击。

7 结论

针对传统的猫映射加密图像无法改变原始图像直方图的缺陷，提出了一种利用改进的混沌猫映射和扩散函数相结合来对数字图像进行置乱加密的算法。该算法具有很好的加密/解密效果和安全性，如图 2(c)中解密的密码x_0=0.600 000 01，与正确的密码x_0=0.6 只相差 0.000 000 1，就无法对图像进行正确解密，且改进的猫映射与传统的猫映射相比，密钥空间增大了 5 倍。该算法同时在空间域和色度域对图像进行加密，基本上都采用整数运算和位运算，具有加密速度快、运算简单的特点。

参考文献

1 丁　玮, 齐东旭. 数字图像变换及信息隐藏与伪装技术[J]. 计算机学报, 1998, 21(9): 838-843.

2 Qi Dongxu, Zou Jinacheng, Han Xiaoyou. A New Class of Scrambling Transformation and Its Application in the Image Information Covering[J]. Sciences in China, 2000, 43(3): 304-312.

3 Ding Wei, Yan Weiqi, Qi Dongxu. Digital Image Watermarking Based on Discrete Wavelet Transform[J]. Computer Science and Technology, 2002, 17(2): 129-139.

4 Chen Guanrong, Mao Yaobin, Chui C K. A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps[J]. Chaos, Solitons and Fractals, 2004, 21(3): 749-61.

5 Lian Shiguo, Sun Jinsheng, Wang Zhiquan. Security Analysis of a Chaos-based Image Encryption Algorithm[J]. Physica A, 2005, 351(2-4): 645-661.

6 张小华, 刘　芳, 焦李成. 一种基于混沌序列的图像加密技术[J]. 中国图像图形学报, 2003, 8(4): 374-378.

(上接第 165 页)

善原来伪随机序列数值分布不平衡这一缺点，其它方面的改善还要结合更多的其它办法。

造成混沌流密码系统不够安全的重要原因之一就是数字化混沌系统的动力学特性退化问题。由于计算机生成的混沌系统都是在有限数值精度下运算模拟出来的拟混沌轨道的周期是有限的，这给混沌流密码系统的安全应用带来了很大的隐患，因此必须特别注意和采取适当的措施加以避免。目前，除了采用更高的计算精度和复合多个相同或不同的混沌系统外，还可以采用对混沌系统施加伪随机微小扰动等方法来加大混沌系统迭代序列的周期。

参考文献

1 Robert A, Matthews J. On the Derivation of a Chaotic Encryption Algorithm[J]. Cryptologia, 1989, 13(1): 29-42.

2 Shujun L, Xuanqin M, Yuanlong C. Pseudo-random Bit Generator Based on Couple Chaotic Systems and Its Applications in Stream-cipher Cryptography[C]//Proceedings of the Progress in Cryptology——the 2nd International Conference on Cryptology, India. 2001: 316-329.

3 Shihong W, Weirong L, Huaping L, et al. Periodicity of Chaotic Trajectories in Realizations of Finite Computer Precisions and Its Implication in Chaos Communications[J]. International Journal of Modern Physics B, 2004, 18 (17-19): 2617-2622.

4 Kocarev L, Jakimoski G. Pseudorandom Bits Generated by Chaotic Maps[J]. IEEE Transactions on Circuits and Systems- I: Fundamental Theory and Applications, 2003, 50(1):123-126.

5 Álvarez G, Montoya F, Romera M, et al. Cryptanalyzing an Improved Security Modulated Chaotic Encryption Scheme Using Ciphertext Absolute Value[J]. Chaos, Solitons and Fractals, 2005, 23(5).