基于离散混沌CAT的图像加密算法研究与实现

王小鸥
(江西应用技术职业学院 信息工程系，江西 赣州 341000)

摘 要：针对图像加密算法中迭代性高、低维离散混沌加密密钥空间小、保密性低等特点，提出利用CAT映射对图像进行离散化，利用该映射的周期性变化对图像进行加密，对不同大小的图像采用不同的周期进行加密。通过实验表明：加密算法能对图像进行有效的加密，得出最佳的参数以达到最好的图像加密效果。

关键词：混沌；CAT映射；离散；图像加密
中图分类号：TP309 **文献标识码：**A

Research and realization of image encryption algorithms based on discrete chaos CAT

WANG Xiao Ou
(Department of information Engineering, Jiangxi College of Applied Technology, Ganzhou 341000, China)

Abstract: Image encryption algorithm is of high iteration, low-key encryption-dimensional discrete chaotic space, and low privacy so we proposed CAT mapping to discrete images. The using of the map cyclical changes in the image is to be encrypted by different-sized images of different encryption cycle. Experiments show that, encryption algorithm can effectively encrypt images and obtain the best parameters to achieve the best image encryption effect.

Key words: chaos; CAT mapping; discrete; image encryption

大多数的混沌加密研究都是单纯的基于低维离散的混沌系统，通过混沌迭代实现图像的置乱。这种方法具有形式简单、加密时间短、便于实现的优点，但存在密钥空间小、保密性能不佳的缺陷。因此，利用低维的混沌系统加密的保密性是不够的。本文提出的算法，首先利用二维的混沌猫映射，对图像进行像素的置乱，然后利用一种新的混合混沌系统对图像进行置换。该系统将两个离散的混沌系统经一定的比例混合后，注入到一个连续混沌系统，这样得到一个性态极其复杂的混沌序列。最后利用得到的混沌序列与图像数据进行一定的运算便可实现加密。利用该方法加密的保密性能不是取决于混沌序列与图像数据的运算算法的复杂度，而是依赖于该方法产生的混沌序列的复杂度。该方法与现代密码体制的要求是一致的，即系统的保密性不依赖于对加密、解密算法和系统的保密，而仅仅依赖于密钥的保密性。这也是该方法的最大特点。实验结果表明，该方法存在着密钥空间大、算法简单、易于实现、保密性好、解密方便的优点。

目前，常见的图像加密方式总体上可以划分为置换图像像素值和置乱图像像素位置两大类。置换图像像素值的加密方式通过改变原图像像素点的灰度值实现图像加密，目前有许多图像加密方式就是通过扰乱原图像像素值来实现图像加密的。置乱图像像素位置的加密方式是指将原图像像素位置排列进行置乱，使攻击者难以辨认原始图像，从而达到图像加密的目的。由于混沌系统对于初始条件的敏感依赖性，对于同一个混沌系统，存在微小差异的初始条件，也会很快产生完全不相关的混沌序列，因此基于混沌的图像加密方式具有较好的安全特性。

1 几种典型的方法

(1)1998年Fridrich发表了文章“Symmetric ciphers based on two-dimensional chaotic maps”，该方案中研究了利用二维的Baker 映射和CAT映射进行像素位置变换，并分析了两种映射的密钥空间和可靠性；

(2)1999年和2002年，YEN J. C.与GUO J. I.提出的三类混沌图像加密方案，相关文章：① A new image encryption

algorithm and its VLSI architecture；② A new chaotic key-based designed for image encryption and decryption；③Design of a new cryptography system，分别发表于1999年IEEE IWSiPS 99，2000年IEEE Proc. ISCAS 和2002年Berlin Heidelberg：Springer-Verlag。前两种算法主要都是对图像的像素值进行置换，后一种方法是对图像的像素值进行置换的同时还进行了置乱，但是总的来说这三种方法采用的不是线性变换就是异或运算，均不容易抵抗已知或者选择明文攻击；

(3)2004年，MAO Y B 在Fridrich 方法的基础上，提出了一个快速的图像加密方案“A symmetric image encryption scheme based on 3D chaotic cat maps”，该方案使用了三维的Baker 映射，这种方案与其他方案相比，具有较高的安全性，能抵抗诸如已知明文攻击、统计分析、差分等多种攻击，且具有较大的密钥空间，最重要的是，在具有高安全性的同时，该算法的加解密速度也相当快[3]。

这种加密方案步骤如下：①产生密钥，选择1个128bit的序列作为密钥，将其分为6组，将这6组分别映射为6个数字。在对图像的像素进行置乱和扩散的过程中这6个数字将作为种子和控制数；②将二维图像堆叠成3维；③用三维离散Baker映射进行图像位置置乱；④将像素值进行扩散；⑤将三维立方体变回到二维图像。其中③ ④重复多次，次数越多则加密的强度就越大，但是时间也会越长。

在国内，也有许多学者在做这方面的研究[4-8]。浙江大学的易开祥、孙鑫、石教英等人提出的基于混沌序列的图像加密算法发表于2000年《计算机辅助设计与图形学报》，该算法已被西安交通大学的李树钧指出未说明使用混沌系统产生全置换矩阵的方法，不能抵抗已知(选择)明文攻击。2004年，发表于《计算机应用》的文献“基于连续混沌系统和Hash函数的图像加密算法”给出了一个基于连续混沌系统的图像加密新方案，该方案利用多维混沌系统与Hash 函数分别产生图像像素置乱矩阵和像素值变换矩阵，方案中利用抽取后的混沌信号产生变换矩阵，从而提高了安全性能。发表于《中国图像图形学报》的文献：“基于二维超混沌序列的图像加密算法”提出了用二维超混沌加密的算法，该算法比之前用一维混沌序列加密大大地扩大了密钥空间。2005年，华南理工大学丘水生的“混沌加密和常规加密相结合的1个系统方案”，实现了混沌加密与常规加密DES(AES)的结合。2006年，发表于《计算机工程》的文献“基于复合混沌系统的图像加密”该算法将三维Chen氏系统和一维Logistic混沌系统级联起来对图像进行加密。

2 CAT映射

首先，利用二维的混沌CAT映射对图像进行置乱，其原因是：(1)该映射是一一映射，因此，明文图像和密文图像之间存在着一一对应的关系，避免了坐标位置的冲突；(2)二维混沌映射具有大的密钥空间，而且，这类映射的结构稳定；(3)采用该映射对图像的置乱速度很快；(4)算法构造简单，通过矩阵运算就可实现。

猫映射最先是由前苏联著名数学家阿诺德发现，因为经常使用1幅猫图演示而得名，如图1所示。1幅图像在CAT映射的作用下，先进行线性拉伸，然后通过取模运算进行折叠；如此循环往复，最终达到混乱。

混沌CAT映射可表示为：

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

由于det$A$＝1，CAT映射是一一映射。该映射的Lyapunov指数为：

$$\lambda_1 = \ln\left(\frac{3+\sqrt{5}}{2}\right) > 0,\ \lambda_2 = \ln\left(\frac{3-\sqrt{5}}{2}\right) < 0$$

3 CAT映射离散化

将CAT映射用于加密，需要先对它进行预处理。

首先，引入参数。参数的引入可以通过改变矩阵A的元素来获得。考虑如下更为一般的CAT映射：

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \boldsymbol{A}_d \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\,1),\ \boldsymbol{A}_d = \begin{pmatrix} ab+1 & a \\ b & 1 \end{pmatrix}, a、b \in N$$

该映射仍为一个保面积映射，且具有正的Lyapunov

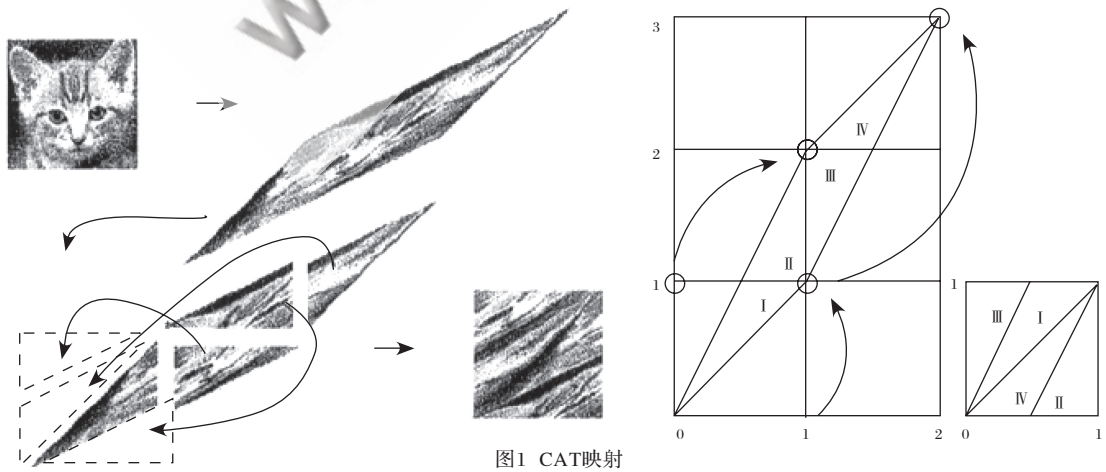


图1 CAT映射

指数。

其次，将CAT映射扩散到$N\times N$并离散化，得到

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \boldsymbol{A}_d \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\, N), x_0, y_0 \in \{0,1,\cdots,N-1\}$$

该映射仍为一一映射。容易证明，上述映射的参数a、b以N为周期，即

$$\begin{pmatrix} (a+k_1N)(b+k_2N)+1 & a+k_1N \\ b+k_2N & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\, N) = \begin{pmatrix} ab+1 & a \\ b & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

其中，k_1, k_2为正整数，a，b都为小于N的正整数

4 CAT映射周期性

由于图像是有限点集，这种反复迭代的结果是，在开始阶段像素点的位置变化会出现相当程度的混乱，但由于动力系统固有的特性，在迭代进行到一定步数时会恢复到原来的位置，也就是具有周期性。可以验证，当取$A=\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$时，如图像大小为128×128，则迭代周期为96；如果图像大小为240×240，则迭代周期为60；如果图像大小为256×256，则迭代周期为192。

5 结果及分析

选取参数$a=40$，$b=30$，迭代次数为5次时，该置乱的结果如图2右图所示，可见，置乱的效果还不错，已经不能辨认原图像的信息。但是，该置乱只是改变了图像像素点的位置，而没有改变像素点的值，所以，也就没有改变图像的直方图，见图3。

图2 加密图像结果

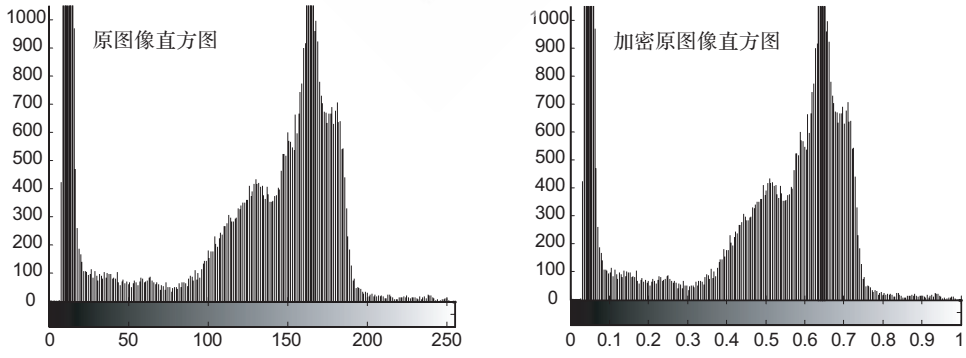


图3 结果直方图

该算法可以很好地对图像进行像素的置乱和置换，但是，对于加密的安全性来说，一个很重要的方面是对明文的敏感性还不能很好地满足，不能很好地抵御选择明文攻击。选择明文攻击指的是攻击者可以利用加密系统对选择的明文进行加密，并通过对明文与密文、密文与密文之间的变化进行对比分析，从而得到加密用的密钥，破解密文。比如，攻击者可以选择两幅仅有一个像素不同的明文，对比密文就可以找到这个像素变换到哪个位置，反复比较就可以找到明文与密文中所有像素的对应关系。虽然这一方法与其他攻击方法相比，实现难度比较大，可能性比较小，然而，如果攻击者能够实施这一攻击，对加密系统的威胁则是最大的，成功的可能性也最高。在目前给出的很多基于混沌的加密系统中，有很多都不能抵御这一攻击，上面给出的方法也同样存在这一问题。

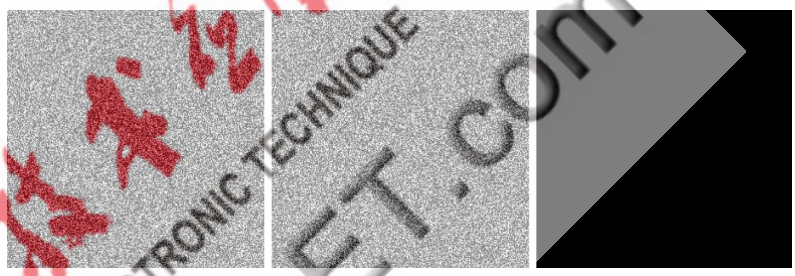
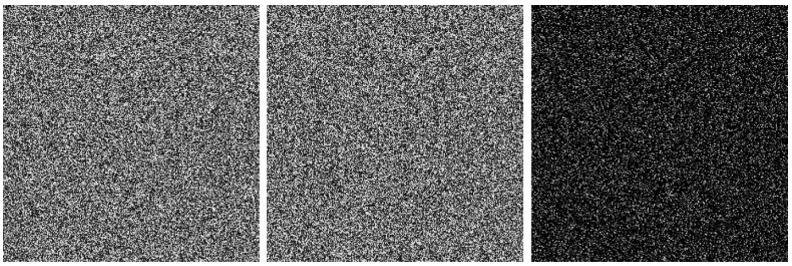

(a)加密图像1 (b)加密图像2 (c)差图像
图4 对明文的敏感度 I

图4中，(a)图和(b)图是加密的原图像只有一点像素值不同时的加密结果，两幅图像的不动点接近于1，从图(c)，它们的差图像中可以看出，两幅图像的像素值基本上一样，所以上述算法还不能抵御明文攻击。

但是，如果能使明文中的每一个像素灰度值的变化影响密文中所有或者大部分的像素值的灰度值，就可以抵御选择明文攻击，因此，对上述算法做如下的改进。

上述映射中，作为密钥的混合比例因子的不同，将影响输出结果，而且，系统对于因子非常敏感。对此如果明文的变化能影响因子，则加密后的图像也会对明文敏感。对此，将因子做如下修改：首先，将所有的明文像素值进行按位异或，然后将所得的值取模，按照对应关系，映射在[0，1]之间，那么，明文中若有一位像素的像素值发生变化，那么得到的加密图像也将会完全不同。

图5中的(a)图是图2原图的加密图像，任意改变图的一点的像素值，得到的加密图像为图中的(b)图。这两幅图的不动点比为



(a)加密图像1 (b)加密图像2 (c)差图像

图5 对明文的敏感度Ⅱ

0.4%，即基本上所有的像素点都不同。从它们的差图像(c)图中也可以看出，(a)图和(b)图是不同的。改进之后的加密方法，对明文十分敏感，即使明文只改变一个像素点，得到的密文也完全不同，所以，改进后的算法能够十分有效地抵御选择性明文攻击。

本文基于对像素进行置乱、置换和扩散的思想，设计了一种快速、安全的图像加密算法。这个算法首先通过CAT映射对像素值进行了置乱，然后通过一种新的混合混沌系统对像素值进行了替换，而且还提出了一种新的方法增强了算法对抵御选择明文攻击的能力。通过各种测试和详细的效果分析，证明这个新的图像加密算法具有良好的实时性、安全性和易实施性，非常适合数据量大、实时性要求高的图像加密。

参考文献

[1] MATTEWS R.On the derivation of a ‘chaotic’ encryption algorithm.Cryptologia. XIII(1)，1989(1)：29-42.

[2] SHANNON C. E. Communication Theory of Secrecy Systems.Bell Syst. Techn. J.1949，28：656-715.

[3] FRIDRICH J . Secure image ciphering based on chaos[R] . Final report for AFRL. Rome New York USA， 1997.

[4] CHEN G， MAO Y.B，CHUI C.K，A symmetric image encryption scheme based on 3D chaotic cat maps， Chaos， Solitons and Fractals.2004，(21)：749-761.

[5] LORENZ E.N，Deterministic non-period flow.J.Atoms.Sci. 1963，20：130-141.

[6] MAY R.M.Simple mathematical models with very complicated dynamics.Nature. 1976， 261：459-167.

[7] FEIGENBAUM M.J. Quantitative universality for a class of nonlinear transformations.J.Stat.Phys. 1978.19(1)：25-52

[8] FORD J. Long-time prediction in dynamics. HORTON W.J.et al eds. John wiley， 1983：79-80.

[9] CHENAND G.，YU X. Chaos control， theory and applications.Berlin，Germany：Spring-Verlag.2003

[10] MATSUMOTO T，CHUA L O，KOMURO M.1985 IEEE Trans.CAS-I 32798.

(收稿日期：2009-01-19)

(上接第51页)

点云。经试验验证，该方法能够较好地提取三维信息和重建，从物体重建的视觉效果来看也是较好的，点云的数量也是非常多的。而且该方法具有实现简单、成本低、速度快、非接触测量数据空间分辨率高等优点。

参考文献

[1] 孙军华，魏振忠，张广军.一种高密度光栅结构光编码方法[J].光电工程，2006，33(7)：78~82.

[2] 张永军，张祖勋，张剑清.利用二维DLT及光束法平差进行数字摄像机标定[J].武汉大学学报(信息科学版)，2002，(6)：566.

[3] 张祖勋,苏国中,郑顺义等.OpenGL 成像机理及其与摄影测量方位元素的相关分析[J].武汉大学学报(信息科学版)，2004，(7)：570.

[4] 尹丽萍,于晓洋,吴海滨. 格雷码与相移结合的结构光三维测量技术研究[J].哈尔滨理工大学学报，2007，5(12)：5-8.

[5] L Hao，STRAUB, R，PRAUTZSCH, H.Structured light based reconstruction under local spatial coherence assumption[C].3rd International Symposium on 3D Data Processing,Visualization,and Transmission,3DPVT 2006.

[6] YANG，CHENG Rong Qian , SHENG Ya Zhu.Robust and accurate surface measurement using structuredlight[J].IEEE Transactions on Instrumentation and Measurement June 2008：1275-1280

[7] WEI Zhen Zhong，ZHOU Fu Qiang，ZHANG，Guan Ging.3D coordinates measurement based on structured light sensor[J].Sensors and Actuators,A:Physical.May 17 2005：527-535

[8] 李红岩. 基于空间二进制编码的阈值分割方法研究[J].计算机仿真，2008,(07)：196-199.

[9] 岳慧敏.基于时间相位展开的三维轮廓测量研究[D].四川大学，2005.

[10] 马颂德,张正友.计算机视觉—计算理论与算法基础[M].北京：科学出版社，1998.

[11] 张祖勋,张剑清. 数字摄影测量学[M].武汉：武汉大学出版社，2001.

[12] 程俊廷,赵灿,莫健华.基于编码结构光和外极线约束的自由曲面三维轮廓术[J].计算机测量与控制,2007，15(1)：102-121

(收稿日期:2009-01-12)