文章编号 1004-924X(2007)07-1096-08

利用图像分割思想的二维混沌映射及图像加密算法

黄 峰,冯 勇
(哈尔滨工业大学 电气工程及自动化学院,黑龙江 哈尔滨 150001)

摘要:根据二维混沌映射思想,设计了一种新的图像加密算法。二维混沌映射包括左映射和右映射两个子映射。通过对图像的拉伸和折叠处理,实现图像的混沌加密。沿图像的对角线方向,将方图分割为上下两个等腰三角形图像;利用等腰三角形图像两列像素之间的像素数目差,以水平方向,依次将某列中的像素插入到相邻下一列像素之中,直至将原始图像拉伸成为一条直线。最后,按照原始图像大小,将这条直线折叠成一个新的图像。映射是可逆的,可应用于图像加密,密钥设计为二维混沌映射的左映射和右映射的组合。进行了仿真研究,结果表明:当密钥为 64 bit 时,密钥空间为 1.84×10^{19},加密速度约为 3 Mb/s。该加密算法具有加密速度快、安全性高、没有信息损失、可移植性强和容易软、硬件实现等特点。

关 键 词:二维混沌映射;图像加密;混沌
中图分类号:TP309.7 **文献标识码**:A

Novel 2D chaotic map based on image segmentation and image encryption approach

HUANG Feng, FENG Yong

(*School of Electrical Engineering and Automation, Harbin Institute of Technology, Harbin* 150001, *China*)

Abstract: A novel image encryption approach based on a new 2D chaotic map and consisting of left map and right map utilizing image segmentation was proposed. The chaotic encryption of image is realized by processing image stretch-and-fold. Firstly, a square image was divided into two isosceles triangles along the diagonal, utilizing the difference of the pixel numbers of two adjacent columns of the triangles, each pixel in a column was inserted to the next adjacent column. Then, the original image could be stretched to a line. Finally, the line was folded over to a new square image whose size was the same as the original image. The process was invertible, so that the positions of image pixels could be used in image encryption. Taking the numbers of the left map and the right map as the keys, the algorithm of the map was formulated, the method of key generation was designed and the security of the proposed image encryption was analyzed. The simulation results show that the proposed encryption approach is valid. When the key is 64 bits, the whole key space size is 1.84×10^{19} and the speed of encryption is 3 Mb/s. The image encryption has several advantages such as rapid speeds, high security and without message loss and it is easy for hardware/software realization.

Key words: 2D chaotic map; image encryption; chaos

收稿日期:2006-11-19;**修订日期**:2007-03-21.
基金项目:国家自然科学基金资助项目(No. 60474016)

1　引　言

随着信息技术的发展，越来越多的图片通过互联网、无线通信等渠道传播。如何保护图片的安全，防止非法攻击，成为一个日益严重的问题。传统加密算法 DES、IDEA、RSA 等得到了成功应用[1]，但这些加密算法是根据文本加密的特点提出来的，在加密图像时，由于图像具有信息量大、相邻像素值相关性强等特点，因此不能完全满足图像加密需要。

近年来，混沌加密得到越来越多的关注。混沌和加密有着密切的联系。Shannon1949 年在加密的奠基性论文[2]中认为：良好的加密系统可以通过拉伸、折叠的过程形成—这正好是混沌映射的产生过程。密码学中最基本的混淆（Confusion）和扩散（Diffusion）等同混沌中的混合（Mixing）和敏感性（Sensitivity）也很相似。1989 年 Matthews[3]采用基于变形 Logistic 映射的混沌加密算法，提出了“混沌密钥”的概念，混沌加密逐渐成为研究的热点[4-6]。

混沌加密主要有两种思想，一种是使用混沌系统生成伪随机密钥流，将密钥流直接掩盖明文。但 Wheeler[7]指出，由于混沌是基于实数集的，加密时需要对混沌流进行近似处理，会出现混沌系统的动力学特性退化。李树钧[8]用一组动力学指标定量描述了逐段线性混沌映射（PWLCM）在有限精度下实现时的动力学特性退化问题。由于混沌没有统一的数学方程，研究工作只能针对特定的混沌系统进行。

混沌映射的另一种思路是采用二维（或多维）混沌映射置乱像素位置。通常利用图像的几何特点，通过对图像的拉伸和折叠处理形成置乱，然后用扩散函数改变像素值。在迭代次数较小时，就能获得良好的加密效果，且速度快、移植方便。常见的混沌映射包括 Baker map、Cat map、Tent map 等。

置乱是一种流行的加密技术，是对像素的排列组合。由于图像信息量大，尝试采用穷举的办法攻击密图是不可想象的，如对大小为 100×100 的图像像素进行全排列，需要做 2.8×10^{35659} 次运算。Scan 语言是一种典型的置乱加密算法。Maniccam[9]通过不同的模式对偶数大小的方图进行扫描，其中模式的类型作为密钥，可用于图像加密。

Fridrich[10]提出了基于二维混沌映射的可逆密钥系统，该系统使用二维混沌映射对明文进行分组置换，经过多轮迭代来实现图像加密。文献[11]将 Baker map 加密对象从方图扩展到矩形图。文献[12]和[13]中分别把 Baker map 和 Cat map 推广到三维。为了增强加密算法抵御明文攻击的能力，采用 Logistic 混沌序列作为扩散函数，与图像像素值进行异或运算。

本文提出了一种新的二维混沌映射，设计了一种图像加密算法。映射由左映射和右映射两个子映射组成，通过对图像的拉伸和折叠处理，实现图像的混沌加密。图像加密算法速度快、安全性高、便于移植。为了抵御明文攻击，加密算法中包含了扩散函数。

2　新二维混沌映射原理和算法

2.1　新二维混沌映射原理

设图像大小为 $N\times N$。首先沿图像的对角线方向，将方图分割为上下两个等腰三角形图像。由于等腰三角形图像每一列的像素数目和相邻列的像素数目是不同的，因此可以从水平方向，将一列中的像素插入到相邻列的像素之间。反复该过程，依次连接，原始图像被拉伸成为一条长 N^2 的直线。然后，再折叠成一个 $N\times N$ 的新图像。如图 1 所示，(a)为左映射，(b)为右映射。

(a)左映射

(a)Left map

(b)右映射

(b)Right map

图 1　映射原理图

Fig. 1　Map principle

举例说明。设图像大小为 4×4，如图 2 所示，当映射为左映射时，则首先将图像沿左上到右下的对角线方向分割为两个等腰三角形图像，依次将像素(3,3)插入到像素(2,2)之前，像素(2,3)插入到像素(2,2)和(1,2)之间，像素(1,3)插入到像素(1,2)和(0,2)之间……重复这个过程，即可将原图像拉伸成为一条直线：(3,3)、(2,2)、(2,3)、(1,2)、(1,3)、(0,2)……最后将直线折叠，得到映射后的新图像。

当映射为右映射时，首先将图像沿右上到左下的方向分割为两个等腰三角形图像。像素插入方向和左映射时相反。上述插入过程均采用将较长的列像素插入到较短的列像素之间的方法，避免了当列的个数为奇数时，出现一列像素无法完成插入操作的问题。

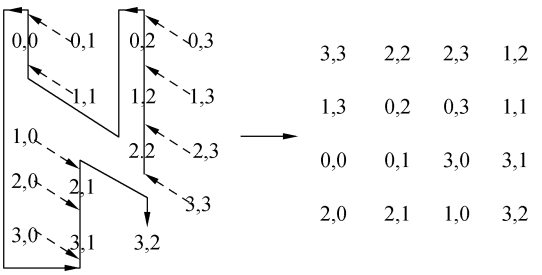


图 2　左映射(图像大小为 4×4)

Fig. 2　Left map in a 4×4 image

2.2　新二维混沌映射计算算法

图像大小为 $N\times N$，设 $A(i,j)$，$i,j=0,1,\cdots,N-1$ 为图像中的任意一点像素值，$l(i)$，$i=0,1,\cdots,N^2-1$，为将 $A(i,j)$ 拉伸后的一维向量。由于映射是由左映射和右映射两个子映射组成，分别给出算法如下：

左映射算法。如图 1(a)所示，左映射算法为：当 $j\geqslant i$ 且 $N-j$ 是奇数时，有

$$l\left[\frac{(N+j+2)(N-j-1)}{2}+2(j-i)\right]=A(i,j)\ , \tag{1}$$

当 $j\geqslant i$ 且 $N-j$ 是偶数时，有

$$l\left[\frac{(N+j+3)(N-j-2)}{2}+2(j-i)+1\right]=A(i,j)\ , \tag{2}$$

当 $j<i$ 且 j 是偶数时，有

$$l\left[\frac{N^2+N+(2N-j-1)\times j}{2}+2(N-i-1)\right]=A(i,j)\ , \tag{3}$$

当 $j<i$ 且 j 是奇数时，有

$$l\left[\frac{N^2+N+(2N-j)\times(j-1)}{2}+2(N-i)-1\right]=A(i,j)\ , \tag{4}$$

右映射算法。可以通过下列过程得到：

将原图做一次镜像，A'表示映射后的图像：

$$A'(i,j)=A(i,N-1-j)\ , \tag{5}$$

其中，$i=0,1,\cdots,N-1$；$j=0,1,\cdots,N-1$。通过左映射算法(1)～(4)，得到右映射算法。

折叠算法。

$$B(i,j)=l(i\times N+j)\ . \tag{6}$$

其中，$i=0,1,\cdots,N-1$；$j=0,1,\cdots,N-1$。

3　图像加密、解密算法

密钥设计。映射分为左映射和右映射，其映射次数可以作为密钥 Key。如 Key=1234，表示依次用左映射 1 次，用右映射 2 次，然后用左映射 3 次，最后用右映射 4 次。由于图像是有限像素点的集合，像素的排列组合是有限的。因此在有限次迭代之后，加密图像会恢复到原来的状态，即混沌映射都具有庞加莱回复性。Fridrich[10] 指出，当迭代次数较小(如<15)时，加密算法是安全的。本文将密钥的每一位设计为小于 10 的整数。由于新混沌映射的周期非常大(不小于 10^5)，这种设计是合理的。

加密算法如图 3 所示。其中 K_1 及 K_2 可以分别是密钥 K 的一部分，也可以相同，或可互相推导，函数 $F(K)$为密钥的函数，输出为扩散函数的参数。

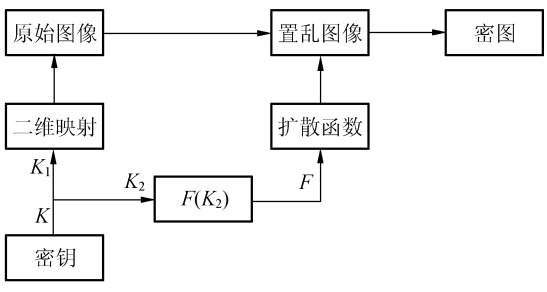


图 3　图像加密算法

Fig. 3　Algorithm of image encryption

本文采用了一种简单的扩散函数：

$$v_k' = v_k + G(v_{k-1}') \bmod L \ , \qquad (7)$$

其中，v_k 是指每一个像素的值，v_k' 为扩散后的像素值，$v_{-1}' = F(K_2)$，$G(v_{k-1}') = 5 \times v_{k-1}'$，$L$ 为像素灰度级。该扩散函数结构简单、扩散速度快。

图像加密算法分为三步：

(1)利用密钥 K_1 及算法(1)～(5)，将图像 $A(i,j)$ 拉伸处理为一条直线 $l(i)$，其中 $i=0,1,\cdots,N^2-1$。

(2)利用算法(6)，将直线折叠处理，得到置乱图像 $B(i,j)$。

(3)利用密钥 K_2 及扩散函数，对置乱图像进行扩散处理得到密图。

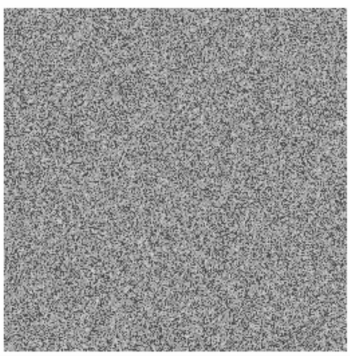
解密算法与加密算法密钥相同、过程相反。由于密钥相同，该加密算法为对称加密算法。

4　加密实例和安全性能分析

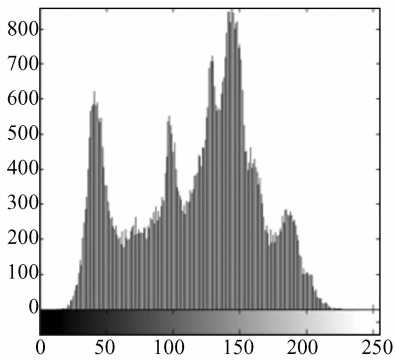
对 $L=256$ 的 lena 图进行加密。为了研究二维混沌映射的加密效果，首先令 $K_2=0$，即不使用扩散函数。此时，加密系统仅仅置乱图像，没有改变图像的像素值。当 Key＝1 时，使用该映射加密之后，图像没有原图的特征，如图 4(b)所示。而 Baker map 在加密次数为 1 时，图像特征明显。如图 4(c)所示，当 Key＝1234567890123456 时，密图用肉眼已无法识别，说明加密效果良好。密图直方图如图 4(d)所示。

(a)原图像
(a)Plain-image

(b)Key＝1 时的密图
(b)Ciphered-image Key＝1



(c)Key＝123456890123456 时的密图
(c)Ciphered-image Key＝123456890123456



(d)密图(c)的直方图
(d)Histogram of ciphered-image Key＝1234567890123456

图 4　加密及解密图像

Fig. 4　Images of encryption and decryption

4.1　安全分析

密钥空间。由于最基本、最流行的破解方法是对密钥进行穷尽搜索，密钥空间大是加密算法安全的前提。加密算法的密钥空间(无扩散函数)

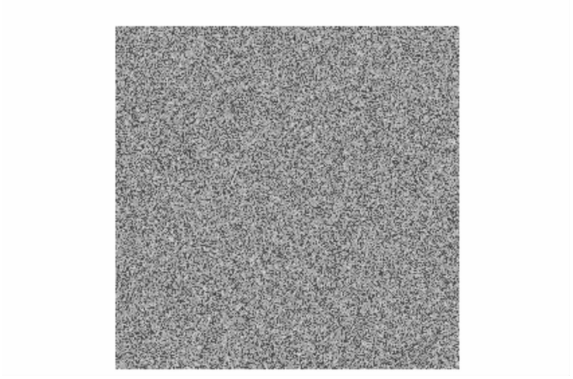
如表 1 所示。研究表明，密钥空间大小只和密钥长度有关，在理想情况下(计算速度允许)，密钥能无限增加。

表 1　密钥长度和密钥空间

Tab. 1　Key space sizes vs key lengths

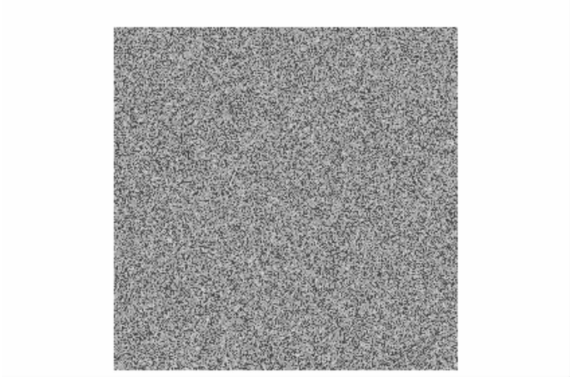
密钥长度(bits)	密钥空间
64	1.84×10^{19}
128	3.4×10^{38}
512	1.34×10^{154}

密钥敏感度。对用 Key=1234567890123456 加密的密图，用 Key_1=1234567890123455 解密，如图 5(a)所示。用 Key_2=1234567890123457 解密，如图 5(b)所示。可以看到，即使加密密钥和解密密钥仅有很小的差异(1 位)，也无法解密密图，证明加密算法对密钥非常敏感。



(a)Key_1=1234567890123455 时的解密图像

(a)Decrypted image Key_1=1234567890123455



(b)Key_2=1234567890123457 时的解密图像

(b)Decrypted image Key_2=1234567890123457

图 5　密钥敏感度测试

Fig. 5　Sensitivity of key

统计分析。由于图像相邻像素之间具有很强的相关性，因此，如果加密后相邻像素之间相关性越趋近于零，越能说明加密算法的安全性。相邻的相关系数如下：

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{8}$$

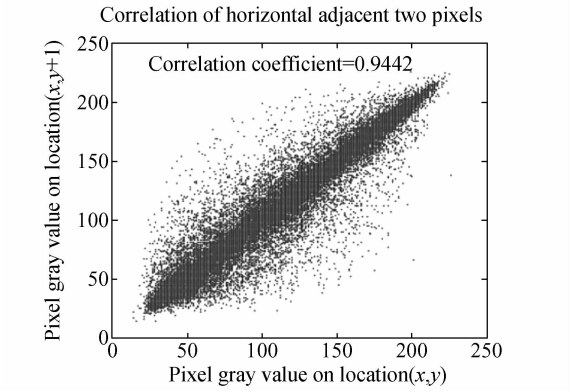
其中 x、y 为两个相邻点的灰度值，

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

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

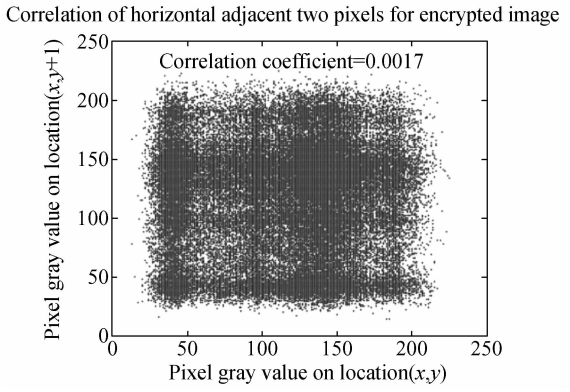
$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}|(x_i-E(x))(y_i-E(y))|$$

图 6 为密图像素(x,y)和$(x,y+1)$之间的关系。原图的相关系数为 0.9442，加密之后的相关系数为 0.0017。其他相邻点的相关系数如表 2 所示，可见加密后密图像素之间的相关系数非常小。



(a)原图

(a) Plain-image



(b)密图

(b) Ciphered-image

图 6　原图和密图相邻点间的关系

Fig. 6　Correlations of two adjacent pixels in the plain-image and the ciphered-image

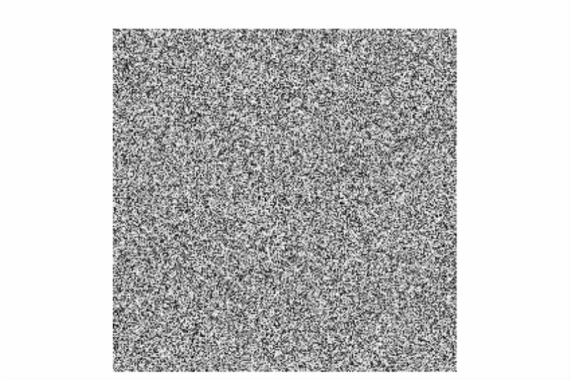
表 2　加密前后随机点(x,y)与相邻点的相关系数

Tab. 2　Correlation coefficients of two adjacent pixels

	原图	密图
水平方向	0.9442	0.0017
垂直方向	0.9711	0.0031
对角线方向	0.9187	0.0050

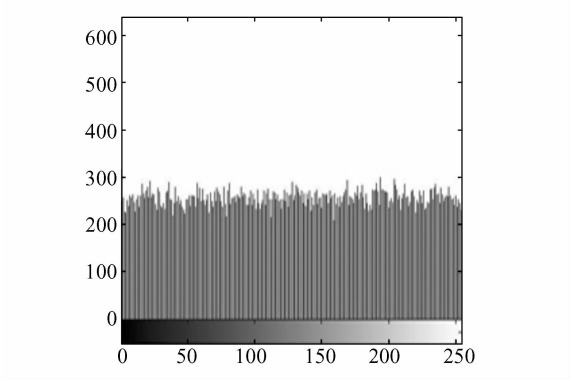
4.2　扩散机制

仅对图像进行像素置乱不够安全，不能抵御已知(选择)明文攻击。因此，为了增强加密算法的安全性，需要在二维混沌映射的基础上增加扩散函数。本文采用的扩散函数如式(7)所示，其中令 $v_{-1}=F(K_2)=150$，增加扩散机制之后，原图的像素值发生改变。加密后的图像和直方图如图 7 所示：



(a)密图

(a)Ciphered-image



(b)直方图

(b)Histogram

图 7　密图及其直方图

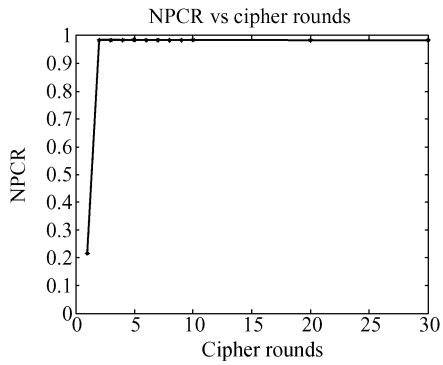
Fig. 7　Ciphered-image and histogram

在增加了扩散函数之后，为了检验加密算法扩散性，对两个只有一个像素点有差异的图像进行 NPCR(Number of Pixels Change Rate)和 UACI(Unified Average Changing Intensity)分析。两图像的像素值分别为 v_1' 和 v_2'，如果 $v_1'(i,j)\neq v_2'(i,j)$，则 $D(i,j)=1$

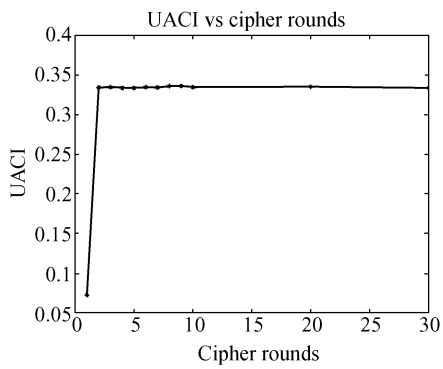
$$\mathrm{NPCR}=\frac{\sum_{i,j}D(i,j)}{256\times 256}\times 100\%\ , \tag{9}$$

$$\mathrm{UACI}=\frac{1}{256\times 256}\left[\sum_{i,j}\frac{|v_1'(i,j)-v_2'(i,j)|}{255}\right]\times 100\%\ . \tag{10}$$

结果表明，在参数不变的情况下，即使只是两个有一位像素不同的图像，随着加密次数的增加，密图也会变得完全不同，扩散速度非常快。如图 8(a)所示，当加密次数 $n=2$ 时，两个加密图像便已基本不同(NPCR≈1)。



(a)



(b)

图 8　NPCR 和 UACI 随加密次数增加而变化的情况

Fig. 8　NPCR and UACI vs ciphering rounds

5　新映射与其他混沌映射比较

Baker map 是最典型、应用最广的混沌映射之一，在图像加密领域得到广泛的应用[10-12]。新

映射和 Baker map 比较：

(1)密钥空间更大。文献[10]介绍了 Baker map 的两种形式，但即使是 Baker map 的一般形式(即密钥不是图像大小的因数的情况)，Baker map 的密钥空间最大仅为 2^{N-1}(N 为图像的宽)，而新映射的密钥空间只和密钥本身长度有关。只要计算速度允许，密钥长度没有限制。

(2)对密钥变化更加敏感。新映射只要密钥稍有变化，密图就会截然不同。因此，用相似但不相同的密钥无法对密图解密。而使用相似的密钥也可以对 Baker map 加密密图进行解密。

(3)加密算法更加简单。Baker map 一般形式下的算法具有非常复杂的形式。加密算法比较复杂。而新映射算法简单，加密算法非常简洁。

(4)能满足实时加密需要。在一台 Pentium III (M) 1.13 GHz 的笔记本电脑上仿真结果表明，未优化的 VC 程序，Key＝1234567890123456 时，加密速度约为 3 Mb/s。

6 结　论

本文根据折叠、拉伸的思想，得到一种新的二维混沌映射，提出一种新的图像加密算法。仿真结果表明：图像加密算法密钥为 64 bit 时，密钥空间为 1.84×10^{19}，加密速度约为 3 Mb/s，基本满足实时图像加密需要。使用新映射的优点是：

(1)算法非常简单，容易编程实现。

(2)二维混沌映射是可逆的。

(3)基于二维混沌映射的加密/解密算法没有信息损失。

(4)具有与其它混沌映射一样的性质，能应用于信息安全的其他领域。

(5)加密的密钥基本没有限制，在速度允许的前提下，可以为任意整数(每位最好＜10)。

(6)密图和原图大小一致，没有大小差异。

(7)能满足实时需要，适合大尺寸图像加密。

(8)加密算法简单，容易硬件实现。

由于压缩后的图像也可以表示为二维矩阵形式，因此，混沌映射加密算法如何结合流行的图像压缩[14]技术，对压缩后的图像进行加密，将是一个值得探讨的问题。

参考文献：

[1] BRUCE S. *Applied cryptography-protocols, algorithms, and source code in C* [M]. second edition, New York: John Wiley & Sons, Inc, 1996.

[2] SHANNON C E. Communication theory of secrecy systems [J]. *The Bell System Technical Journal*, 1949, 28(4): 656-715.

[3] MATTHEWS R. On the derivation of a "chaotic" encryption algorithm[J]. *Cryptologia*, 1989, *XIII*(1): 29-42.

[4] CHANG C C, HWANG M S, CHEN T S. A new encryption algorithm for image cryptosystems [J]. *The Journal of System and Software*, 2001, 58(7): 83-91.

[5] 樊春霞，姜长生. 一种基于混沌映射的图像加密算法[J]. 光学 精密工程，2004，12(2)：179-184.
FAN CH X, JIANG CH SH. Image encryption based on discrete chaotic maps [J]. *Opt. Precision Eng.*, 2004, 12(2): 179-184. (in Chinese)

[6] 梁士利，张玲，王广，等. 一维加法 CA 的同步系统研究光学精密工程[J]. 光学 精密工程，2006，14(3)：495-497.
LIANG SH L, ZHANG L, WANG G, *et al*.. Study on synchronization of 1D-k3 additive cellular automata [J]. *Opt. Precision Eng.*, 2006, 14(3): 495-497. (in Chinese)

[7] WHEELER D D. Problems with chaotic cryptosystems [J]. *Cryptologia*, 1991, *XII*(3): 243-250.

[8] LI S, MOU X, CAI Y, *et al*.. Problems with a probabilistic encryption scheme based on chaotic systems [J]. *Int. J. Bifurc. Chaos*, 2003, 13(10): 3063-3077.

[9] MANICCAM S S, BOURBKIS N G. Image and video encryption using scan patterns [J]. *Pattern Recognition*, 2003, 37(4): 725-737.

[10] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps [J]. *Int. J. Bifurc. Chaos*, 1998, 8(6): 1259-1284.

[11] SALLEH M, IBRAHIM S, ISNIN I F. Enhanced chaotic image encryption algorithm based on chaotic maps [C]. *IEEE Conf Circuits and Syst*, 2003,2:508-511.

[12] MAO Y B, CHEN G R, LIAN S G. A novel fast image encryption scheme based on 3D chaotic Baker maps [J]. *Int. J. Bifurc. Chaos*, 2004, 14(10):3613-3624.

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

[14] 田宝凤,徐抒岩,孙荣春,等. 一种适合星上应用的遥感图像有损压缩算法[J]. 光学 精密工程,2006, 14(4): 725-730.
TIAN B F, XU SH Y, SUN R CH, *et al*.. A lossy compression algorithm of remote sensing image suited to space-borne application [J]. *Opt. Precision Eng.*, 2006, 14(4): 725-730. (in Chinese)

作者简介:黄　峰(1978—),男,湖南邵阳人,现在哈尔滨工业大学攻读博士学位,主要从事图像处理、混沌加密方面的研究。E-mail:huangfeng@hit.edu.cn