一种基于混沌映射的数字图像加密新算法*

熊昌镇[1,2], 邹建成[2], 齐东旭[1,3]
(1. 中山大学信息科学与技术学院, 广东 广州 510275;
2. 北方工业大学 CAD 研究中心, 北京 100041;
3. 澳门科技大学信息学院)

摘 要: 很多基于混沌的映射数字图像加密算法都采用了量化策略, 而量化后, 其映射能否保持混沌的性质仍是一个未知数。在有限精度下, 其映射会产生循环或收敛于不动点, 与理想的密度函数分布背道而驰; 提出了一种新的基于混沌映射的加密算法, 该算法不需要对轨道分布具有先验知识, 所以可以选用任何一个混沌模型, 这极大地扩展了算法的密码空间、大大减少了混沌映射迭代次数并能很好地利用混沌的特性; 同时还引入了广义面包师分割的思想, 进一步提高密钥的空间、增强算法的安全。对所提出的算法进行了安全分析, 实验结果表明: 该算法具有对密钥敏感、密钥空间大、加密后像素分布均匀等特点, 可有效地保障加密图像的安全。

关键词: 混沌映射; 排列; 图像加密
中图分类号: TP391.41 文献标识码: A 文章编号: 0529-6579 (2004) S2-0029-05

随着网络与多媒体技术的飞速发展, 数字图像正逐渐成为人们进行信息交流的重要信息载体。随着人们对信息安全要求的提高, 数字图像加密技术在多媒体通信中获得了广泛的应用。由于图像和视频本身的特性, 图像或视频的加密有其自身的要求, 传统的加密算法 (如 DES 和 RSA) 并不适合于图像或视频加密。从很多方面已经证明混沌映射与传统的加密算法相比, 有很多相似但又不同的特性[1—4]。例如, 传统加密算法对密钥敏感, 然而混沌映射对初始值和参数敏感; 加密算法通过多轮加密来扰乱和扩散数据, 而混沌映射通过迭代把初始区域扩散到整个相空间。而两种技术的主要不同在于: 加密操作是定义在有限集合, 而混沌是严格的数学概念, 定义在实数集。混沌加密并不是新的概念, 早在 1989 年, 混沌函数就被用来设计加密算法[5]。尽管专用的混沌加密算法并不常出现, 但确实存在一些混沌加密算法。例如文献 [6] 提出了一种叫 CKBA (chaotic key-based algorithm) 的加密方法, 该算法首先产生一个基于混沌的时间序列, 然后用它产生一个二进制序列作为密钥, 对图像的像素进行重排并与选择的密钥进行 XOR 或 XNOR 运算。该算法简单, 但在安全性方面有很多的缺点, 正如后来在文献 [7] 指出的一样: 该算法对已知的明文或有选择的明文攻击是脆弱的, 而且其抗穷举攻击的能力令人堪忧。文献 [8] 设计了一种基于混沌 Kolmogorov 流的图像加密算法, 整幅图像作为一个简单块, 通过基于 Kolmogorov 流的混沌密钥控制系统进行加密, 利用伪随机序列来扰乱数据。

大部分基于混沌的图像置乱方案采用了量化策略, 先计算混沌模拟序列, 然后对其进行多值量化生成置换地址码, 而量化后, 该映射能否保持混沌的性质仍是一个未知数。另外, 由于置换地址码的特殊要求, 为能遍历所有的地址, 算法不得不经历许多不能生成置换地址码的迭代, 增加了算法的时间复杂度。我们对产生的实数混沌序列进行从大到小的排列, 并以此来置换图像的位置。该方法不需对轨道分布具有先验知识, 所以可以选用任何一个混沌模型, 极大地扩展了算法的密码空间, 算法大大减少了混沌映射迭代次数, 并能很好地利用混沌的特性。同时我们把广义面包师变换的分割思想引入其中, 以增加其算法的安全性; 我们对该加密算法的加密性能进行了分析, 实验结果表明, 该算法具有良好的安全性, 可有效地保障加密图像的安全。

1 混沌映射

混沌是非线性动力系统产生的一个确定的伪随机序列的过程, 它是非周期性的, 不收敛且对初始

* 收稿日期: 2004—09—11
基金项目: 国家 973 计划资助项目 (2002CB312104); 国家自然科学基金资助项目 (60133020); 北京市科技发展计划资助项目 (KM200310009027)
作者简介: 熊昌镇 (1979 年生) 男, 博士研究生; E-mail: xczkiong@163.com

值极端敏感。通常，混沌系统的原型可表述如下：

$$x(n) = f(x(n-1))$$

其中，$x(n)$ 是由非线性映射 $f(\cdot)$ 产生的混沌序列，$x(0)$ 是其初始条件。一种被广泛应用的动力系统是 Logistic 映射，基本的 Logistic 映射有公式表示为：

$$f(x) = \mu x(1-x)$$

其中 $x \in (0,1)$。研究表明该迭代系统在 $3.569 < \mu < 4$ 时，呈现混沌状态。该序列的概率密度函数可表述如下

$$\rho(x) = \begin{cases} \dfrac{1}{\pi \sqrt{1-x^2}} & 0 < x < 1 \\ 0 & \text{否则} \end{cases}$$

从概率密度函数 $\rho(x)$ 函数可得到该序列的统计特性。如，其均值为

$$\bar{x} = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} x(i) = \int_{-1}^{1} x\rho(x)\,\mathrm{d}x = 0$$

假设有两个初始值 x_0 和 y_0，这两个序列的交叉相关性为

$$C(m) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} (x_i - \bar{x})(y_I - \bar{y}) =$$

$$\int_{-1}^{1}\int_{-1}^{1} (x-\bar{x}) f^m(y)\,\rho(x)\,\rho(y)\,\mathrm{d}x\,\mathrm{d}y = 0$$

从上面可以看出，混沌序列拥有与白噪声相似的特性、简单和对初始值敏感性的特点。但大部分算法都是采用有限的整数表达法来产生地址码。存在数据丢失，很难说其产生的序列还能保持其混沌的性质。文献 [9] 讨论了 Logistic 方程在离散区域下的动力行为。在有限精度下 Logistic 方程的动力行为是：设精度为 N 位有效数字，则在 [0, 1] 上最多有 10^N+1 个不重复点。那么，当迭代次数大于 10^N 时，必然会产生循环。可以预见，在离散区间上 Logistic 方程的动力行为，不是收敛于一个不动点，就是形成一个循环。如在 3 位有效数字下，有一个 13 个值的循环，0.109→0.338→0.950→0.190→0.610→0.946→0.204→0.650→0.910→0.328→0.882→0.416→0.972→0.109。其迭代次数为 1000 时的数据点密度分布如表 1 所示。其中，χ_n 是第 n 次迭代的值，ρ 是相应的出现次数，可以看到结果与理论值 $\rho(x)$ 在有效数字较小时相差较大。由于离散区间只有有限个元素，不可能产生一个非周期轨道。所以要使 N 尽可能的大，使其接近于理想的值。用双精度数据类型来产生混沌映射。为了保持其混沌性质，对产生的实数混沌序列进行从大到小的排列，并以此来置换图像的位置。

表 1 $N=3$ 时的数据点密度分布

Tab. 1 Density distribution at $N=3$

χ_{1000}	0.000	0.109	0.190	0.204	0.328
ρ	661	6	8	6	6
χ_{1000}	0.388	0.416	0.616	0.650	0.750
ρ	6	2	7	6	258
χ_{1000}	0.882	0.910	0.946	0.950	0.972
ρ	4	10	8	8	4

2 加密算法

算法包括以下 4 个步骤。

步骤 1：选择一个混沌映射，利用初始参数 u，x_0 来产生混沌序列，同时再选择一个整数序列 $\delta = (n_1, n_2, \cdots, n_k)$，$0 < n_i < n$ 和 $\sum_i^k n_i = n$，其中 n 是图像行的大小，可把这些参数作为密钥。

步骤 2：利用混沌映射 $f(x) = \mu x(1-x)$ 产生一个双精度类型的混沌序列 $\{x_1, x_2, \cdots, x_n\}$，将实值序列集合 $\{x_1, x_2, \cdots, x_n\}$ 中的 N 个值由小到大排序，形成有序序列 $\{x'_1, x'_2, \cdots\}$ 确定混沌实值序列 $\{x_1, x_2, \cdots, x_n\}$ 中的每个 x_i 在有序序列 $\{x_1', x_2', \cdots, x_n'\}$ 中的位置编号，形成置换地址集合 $\{t_1, t_2, \cdots, t_n\}$，其中 t_i 为集合 $\{1, 2, \cdots, n\}$ 中的一个；按置换地址集合 $\{t_1, t_2, \cdots, t_n\}$ 对图像的第一行像素进行置换，将其第 i 列像素置换至第 t_i 列，$i = 1, 2, \cdots, n$。

步骤 3：置 $x_1 = x_{n+n_i}$，对 2 行到 M 行重复步骤 2；其中 x_{n+n_i} 为第 $i+1$ 行的迭代起点，若 $n_i = n_k$，则重新从 n_1 开始循环使用 δ。

步骤 4：对图像的列作相似的变换，就完成了图像的加密。

解密算法与加密算法基本上相似，不同在于步骤 2 中，按置换地址集合 $\{t_1, t_2, \cdots, t_n\}$ 对图像的第一行像素进行置换，将其第 t_i 列像素置换至第 i 列，$i = 1, 2, \cdots, n$ 即可实现图像的解密。

3 性能分析

一个好的加密方案应该能抵抗各种攻击，如已知明文攻击，唯密文攻击，统计攻击，差异攻击和穷举攻击等。对所提出的加密方案进行安全分析，包括密钥空间分析，相邻像素相关性分析，数据丢失分析等，结果表明该算法具有很强的安全性。

3.1　密钥空间分析

一个好的算法应该对密钥敏感，密钥空间应该足够大来抵抗穷举攻击。我们选择（u，x）为双精度数据类型，所以（u，x）包含 128 位密钥，同时，还采用广义面包师变换的分割方案[8]。文献[10，11]详细描述了到底有多少种分割方案（如表2）。

表 2　给定 n 值时分割方案的种类数

Tab. 2　Number of keys for some selected n value

n	1	2	4	8	16	32
Keys	0	1	5	55	5271	2^{25}
n	64	128	256	512	1024	2048
Keys	2^{50}	2^{103}	2^{209}	2^{418}	2^{837}	2^{1678}

当 $n=64$(→50 位) 已接近 *DES*(56 位,) 而 $n=128$(→103 位) 和 SKIPJACK(80 位) 和 IDEA(128 位) 之间，$N=256$(→209位)，因此，该方案拥有足够长的密钥。

3.2　密钥敏感性测试

为简化计算，采用 128 位密钥进行测试，其测试步骤如下：

(1) 采用密钥 $u=3.7$, $x_0=0.7$ 对 256×256 大小的灰度图像 Lena 进行加密。

(2) 修改密钥 x_0 最后一位，即取 $u=37$, $x_0=0.7000000000001$ 来加密图像。

(3) 对采用稍微不同密钥的两幅加密图像进行比较，结果是用 $u=3.7$, $x_0=0.7$ 密钥加密的图像与用 $u=3.7$, $x_0=0.7000000000001$ 加密的图像有 99.61% 位置的不同，图1显示了其测试结果。图2显示了用 $u=3.7$, $x_0=0.7$ 加密图像，用 $u=3.7$, $x_0=0.7000000000001$ 解密图像的结果。

3.3　相邻像素相关性分析

相邻像素的相关性可反应图像置乱的程度，相关性越大，置乱效果越差，相关性越小，置乱的效果越好。为了测试置乱图像的水平、垂直、对角相邻像素的相关性。首先从图像中随机选择 1000 个相邻像素对，然后用下面的两个公式计算每一对相邻像素的相关性。

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

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

其中，x 和 y 是图像中两个相邻像素的灰度值，在数值计算中，采用以下离散化的公式：

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

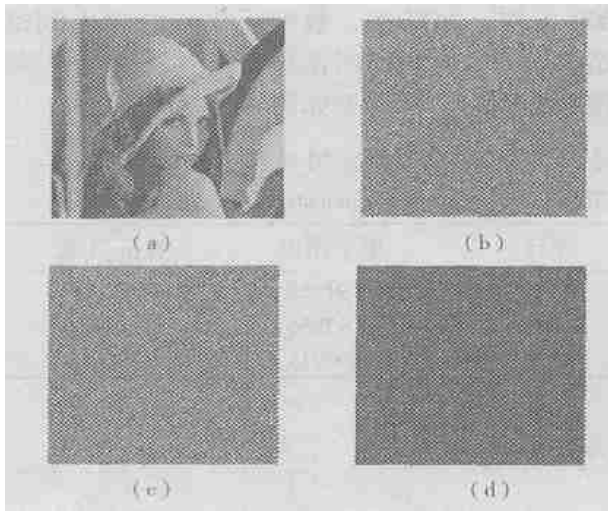

图 1　敏感性测试 1

Fig. 1　key sensitivity result 1

(a) 为原图；(b) 为 key=（$u=3.7$, $x_0=0.7$）的密图；(c) 为 key=（$u=3.7$, $x_0=0.7000000000001$）的密图；(d) 为两幅密的差异图

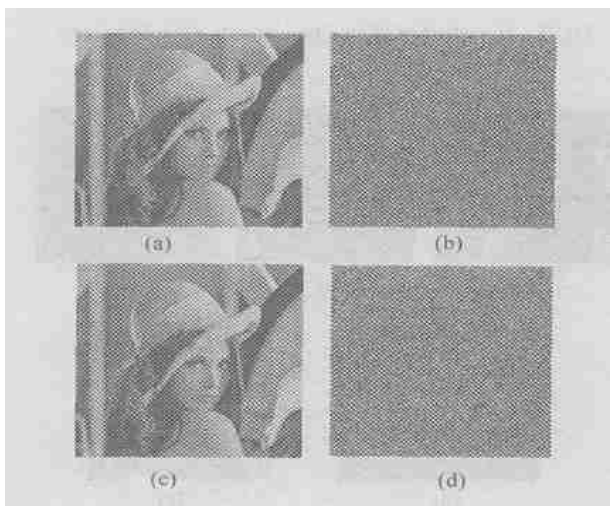

图2　敏感性测试2

Fig. 2 key sensitivity result 2

(a) 为原图；(b) 为 key=（$u=3.7$, $x_0=0.7$）的密图；(c) 为 key=（$u=3.7$, $x_0=0.7$）的解密图；(d) 为 key=（$u=3.7$, $x_0=0.7000000000001$）的解密图

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

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

图 3 显示了在原始图像与置乱图像中，水平相邻像素的相关性系数，分别是 0.91765 、0.01183。说明置乱后的图像分散性很好。垂直与对角线方向可得到相类似的结果，如表 3 所示。

3.4　图像处理攻击

对所提出的基于抽样置乱进行了图像处理（如

jpeg2000 压缩、加噪声、数据丢失) 的攻击测试, 测试结果表明, 对加密图像进行轻微的改变并不影响图像的解密。实验结果如图 4－6。

表 3 图像置乱前后相邻像素的相关系数

Tab. 3 Correlation coefficients of two adjacent pixels

项目	原始图像	置乱图像
水平	0.91765	0.01183
垂直	0.93956	0.00872
对角	0.90215	0.01527

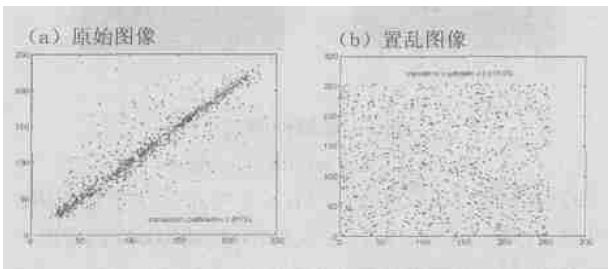

图3 水平相邻像素的相关性分布

Fig. 3 Correlations of two horizontally adjacent pixels

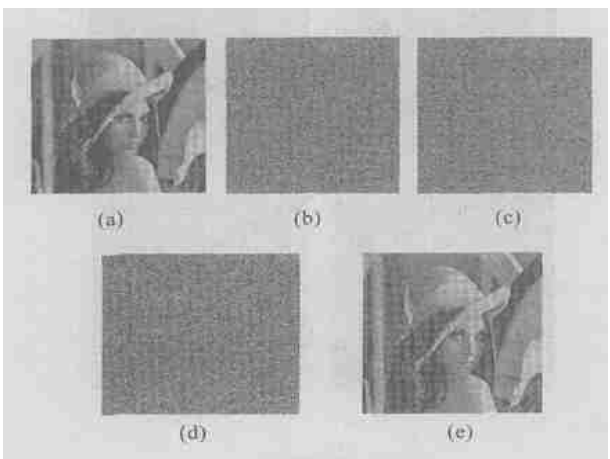

图4 JPEG2000压缩测试(Rate= 5∶1)

Fig 4 Test on image encryption with JPEG compression

(a) 为原图; (b) 为 RSA 加密密图;

(c) 为对 RSA 加密密图 JPEG2000压缩后之解密图像;

(d) 为混沌加密密图, (e) 为对混沌加密图 JPEG2000压缩后之解密图像(PSNR= 31.87)

4 结 论

本文提出了一种新的基于混沌映射的加密算法, 对产生的实数混沌序列进行从大到小的排列, 并以此来置换图像的位置, 该方法不需对轨道分布的先验知识, 可以选用任何一个混沌模型, 极大地扩展了算法的密码空间, 算法大大减少了混沌映射迭代次数, 并能很好地利用混沌的特性; 同时还引入了广义面包师分割的思想, 进一步提高密钥的空间, 增强

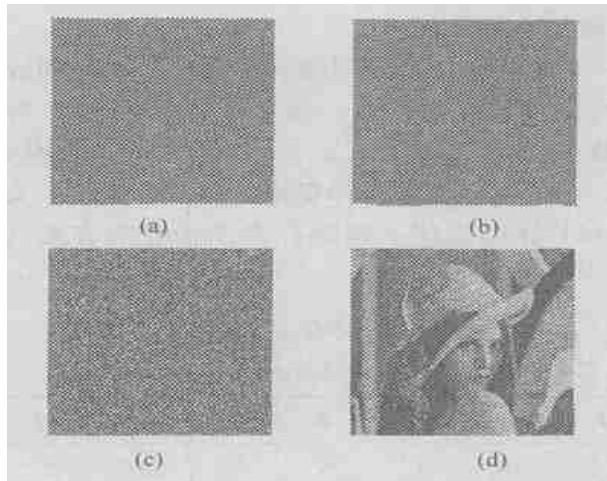

图5 加20%高斯噪声测试

Fig. 5 Test of image under adding 20% Gaussian noise

(a) 为 RSA 加密密图加20%高斯噪声;

(b) 为 RSA 加密密图加20%高斯噪声后解密图;

(c) 为混沌加密密图加20%高斯噪声;

(d) 为混沌加密密图加20%高斯噪声后解密图

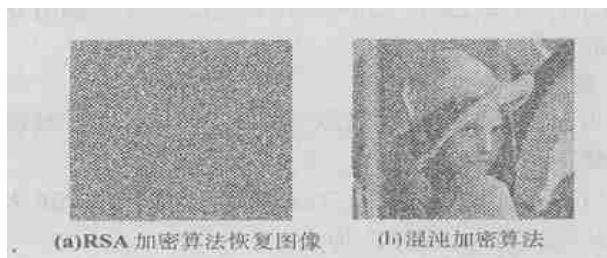

图6 密图左上角25%数据丢失测试

Fig. 6 Test of image under loss of 25% image (left top)

算法的安全; 对所提出的算法进行安全分析, 实验结果表明: 该算法具有对密钥敏感、密钥空间大、加密后像素分布均匀等特点, 可有效地保障加密图像的安全。

参考文献:

[1] KOCAREV L. Chaos-based cryptography: a brief overview [J]. IEEE Circ System Magazine, 2001, 1(3): 6－21.

[2] KOCAREV L, JAKIMOVSKI G. Chaos and cryptography: from chaotic maps to encryption algorithms[J]. IEEE Trans Circ System－I 2001, 48(2): 163－169.

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

[4] MAO Y B, CHEN G, LIAN S G. A novel fast image encryption scheme based on the 3D chaotic baker map[J]. Int J Bifurcat Chaos, 2003: 5－9.

[5] MATTEWS R. On the derivation of a "chaotic" encryption algorithm[J]. Cryptologia, 1989, 8(1): 29－41.

[6] YEN J C, GUO J I. A new chaotic key-based design for

image encryption and decryption [J]. Proc IEEE Int Conference Circuits and Systems, 2000, 4: 49—52.
[7] WU X X, LU J H. Dynamical behavior of logistic equation on a discrete interval[J]. J Shan Hai Teacher University, 1995 (4): 31—33.
[8] SCHARINGER J. Fast encryption of image data using chaotic kolmogorov flows[J]. J Electron Imaging, 1998, 7(2): 318—325.
[9] WANG D S, CAO L. Chaos, fractal and their applications [M]. Hefei: The Press of The University of Science & Technology of China, 1995.
[10] AIGRIER M, Kombinatorik[M]. Springer Verlag, Berlin, Heidelberg, New York, 1975.
[11] JEGER M, HRUNG E. In Die Kombinatorik II. Klett, Stuttgart, 1973.

A New Image Encryption Algorithm Based on Chaotic Map

XIONG Chang zhen[1,2], *ZOU Jian cheng*[2], *QI Dong xu*[1,3]
(1. Department of Electronics, Sun Yat-sen University, Guangzhou 510275, China;
2. CAD Center, North China University of Technology, Beijing 100041, China;
3. College of Information Sciences, Macao University of Sciences and Technology, China)

Abstract: Many digital image encryption algorithms based on chaotic map were presented; most of them use the quantization of coefficients. In finite precision, chaotic map will generate a circulation or an unmovable point, which does not accord with perfect density distributing function. This paper proposes a new encryption algorithm based on chaotic map without transcendental knowledge of orbit distributing. So that people can choose any chaos model, which extends the key space of algorithm. The algorithm reduces iterative number and makes full use of chaotic property of map. This paper also introduces the segmentation mechanism of general baker transformation, which enhances the key space and security of algorithm. The experiment shows that it has the property of key sensitivity, high key space and pixel distributing uniformity.

Key words: chaotic map; arrangement; image encryption

(上接第 28 页)

Audio Watermarking Based on Partial MP3 Encoding

LIU Wei, *WANG Shuo zhong*, *ZHANG Xin peng*
(School of Communication and Information Engineering, Shanghai University, Shanghai 200072, China)

Abstract: An audio watermarking scheme based on partial MP3 encoding is proposed. The original PCM signal is first undergone a partial MP3 encoding to produce quantized MDCT coefficients. An appropriate band in the count1 region, in which magnitude of any quantized MDCT coefficient is either 1 or 0, is chosen for data embedding. Each pair of the quantized MDCT coefficients is used to hide 1 bit. After modification of the coefficients, partial decoder is performed to return to the PCM domain. As the algorithm has taken account the characteristics of MP3 encoding, it is robust against MP3. The method also has good inaudibility and large embedding capacity.

Key words: audio watermarking; MP3 encoding; MDCT