第 34 卷 第 1 期 计 算 机 工 程 2008 年 1 月
Vol.34 No.1 Computer Engineering January 2008
·安全技术· 文章编号：1000—3428(2008)01—0145—02 文献标识码：A 中图分类号：TP309

一种基于四维混沌映射的图像加密算法

张 健[1]，于晓洋[1]，任洪娥[2]
(1. 哈尔滨理工大学测控技术与通信工程学院，哈尔滨 150080；2. 东北林业大学信息与计算机工程学院，哈尔滨 150000)

摘 要：混沌映射所具有的初值敏感性和随机性，使得基于混沌理论的图像加密算法成为一个研究热点。绝大多数学者都采用低维的混沌映射，而四维混沌映射相比于低维映射参数更多也更复杂。该文用四维混沌映射进行图像加密，在增加密钥量的同时，加密的速度并没有降低，而且具有抗穷举攻击和统计攻击的能力。对一幅 1 024×768 的 24 位BMP图像来说，加密时间约为 0.35 s，解密时间约为 0.361 s，可以满足传输要求。

关键词：混沌；敏感性；图像加密；混淆；扩散

Image Encryption Algorithm Based on Four-dimension Chaotic Map

ZHANG Jian[1], YU Xiao-yang[1], REN Hong-e[2]
(1. College of Measurement-control Technology & Communications Engineering, Harbin University of Science and Technology, Harbin 150080;
2. College of Information and Computer Engineering, Northeast Forestry University, Harbin 150000)

【Abstract】 The initial sensitivity and randomness of the chaotic map make the image encryption algorithm based on chaotic theory become a hot researching field recently. Many people adopt the low-dimension chaotic map to encrypt, however, the high-dimension map is more complex and has more parameters. This paper uses the four-dimension map to encrypt image, at the time of increasing the key quantities, the encryption speed is not reduced. Moreover the abilities of resisting exhaustive attack and statistic attack are enhanced. For an image of 1 024×768 24 bits BMP, encryption cost approximately 0.35 s and decryption cost approximately 0.361 s, then it can meet the transmission requirement.

【Key words】 chaos; sensitivity; image encryption; confusion; diffusion

随着 Internet 的快速发展和多媒体技术的广泛应用，对图像的加密就显得非常重要。传统的加密方法如 DES 算法可以用于图像加密，但密钥长度太短，容易遭受攻击。而 RSA 算法虽然可以提供长的密钥，但其加密速度太慢，不适合对图像这种大数据量数据进行加密。

自 1989 年英国数学家Matthews首先提出应用混沌理论进行加密的方法[1]之后，应用混沌理论进行加密体系的设计有了巨大的发展[2-6]。Habutsu等人提出的混沌密码是根据混沌系统对系统的参数变化及系统的初始条件非常敏感这一事实来设计的，Chua L O和Hayes S提出了基于混沌自同步的加密方案，Protopopescu V A等人提出了将混沌系统作为伪随机序列发生器的加密方法，Fridrich J等人提出的基于二维混沌的分组密码加密体制，但是这些加密方案都是基于低维的混沌映射，低维映射的参数和系统变量相对较少，密钥量相对就小，必然会给加密系统带来一定的危险性。

本文提出了基于四维混沌映射的图像加密方法，由于四维映射的参数和系统变量都增大了，密钥量也随之增加，可以有效地抵抗穷举攻击。用 Matlab 软件进行仿真实验，结果表明，该方法的加密解密速度很快，可以抵抗统计攻击和图像处理等攻击。

1 基于混沌映射的加密算法

1.1 混沌映射

混沌理论作为新兴学科，已经迅速融入到了多个学科，变成一门重要而前沿的科学。混沌映射具有初值敏感性、参数敏感性和不可预测性等特性，如“蝴蝶效应”。随着混沌映射系统参数的多少，混沌映射的维数也不同。典型的一维、二维、三维映射分别如式(1)~式(3)所示。

$$x_{n+1}=\lambda x_n(1-x_n) \tag{1}$$

其中，x_n为系统轨迹；λ为系统参数。

$$\begin{cases} x_{n+1}=x_n+h(x_n-x_n^{\,2}+y_n) \\ y_{n+1}=y_n+h(y_n-y_n^{\,2}+x_n) \end{cases} \tag{2}$$

其中，x_n, y_n为系统轨迹；h为系统参数。

$$\begin{cases} \dfrac{\mathrm{d}x}{\mathrm{d}t}=\delta(y-x) \\ \dfrac{\mathrm{d}y}{\mathrm{d}t}=\rho x-y-xz \\ \dfrac{\mathrm{d}z}{\mathrm{d}t}=xy-\beta z \end{cases} \tag{3}$$

其中，x, y, z 分别是代表一定意义的变量，为系统轨迹；δ, ρ, β 为系统参数。

用混沌映射进行加密的安全性就在于，混沌映射对系统初始值和参数值敏感，把初始值和参数值作为密钥来处理，它们的微小变化都会产生两种截然不同的加密结果，这显然增加了系统的抗攻击能力。

但是由于低维映射与四维映射相比，其密钥量相对较小，因此用四维混沌映射进行加密显然会提高系统的抗攻击能力。四维混沌映射[7]如式(4)所示。

作者简介：张 健(1980－)，男，博士研究生，主研方向：图像处理，信息安全；于晓洋，教授、博士生导师；任洪娥，教授
收稿日期：2007-02-15 **E-mail：**zhangjianok00@163.com

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2 x_3 x_4 \\ \dot{x}_2 = b(x_1 + x_2) - x_1 x_3 x_4 \\ \dot{x}_3 = -cx_3 + x_1 x_2 x_4 \\ \dot{x}_4 = -dx_4 + x_1 x_2 x_3 \end{cases} \tag{4}$$

其中，x_1, x_2, x_3, x_4是系统轨迹；a,b,c,d是系统参数。当a= 30,b= 10,c=1,d=10 时，系统出现混沌吸引子，呈现混沌状态。如果给定系统的初始值，则在有限双精度内，混沌映射将产生不重复的序列。

1.2 基于四维混沌映射的加密方案

根据四维混沌映射的特点可以将图像加密分成位置变化和像素值的变化，其步骤如下：

(1)给定一个待加密图像(以 256×256 的灰度图像为例)，将图像从上到下分成 4 块，每一块都有 256×256/4=16 384 个点。

(2)给定四维混沌映射的初始值x_1, x_2, x_3, x_4，将映射迭代，取前 16 384 次迭代的双精度值，共 16 384×4 个值，让这 4 个初始值各自产生的 16 384 个数分别按照从大到小的排序进行排列，将此排序规则对应地把图像的位置进行变化，即改变图像每个分块的位置，从而达到位置置乱的目的。

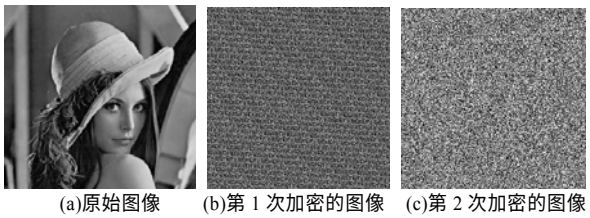
(3)图像每一点的像素值是 0~255 灰度等级中的一个，对应的是 8 位的二进制数。取x_1产生的 16 384 个值，将每个值小数部分的第 8 位k_8分别和数值 5 比较，如果$k_8 \geq 5$，则将第 1 块图像各点像素值的对应二进制置反(1 变成 0，0 变成 1)，否则不变，这样第 1 块中的所有像素值都发生了变化，同理将其他块分别与x_2, x_3, x_4的值比较，从而整个图像的像素值都发生了变化，即灰度直方图发生了变化。

通过上面 3 个步骤，图像的位置和像素值都发生了变化，原始的图像已经不存在，达到了加密的目的。加密的安全性就是基于混沌映射的初始值敏感性以及很大的密钥量。解密是加密的逆过程，根据同样的初始值采用逆变换就可以实现。

2 仿真实验

2.1 仿真实验分析

采用Matlab软件进行仿真实验，选取一幅 256×256 的灰度图像，如图 1(a)所示。令初始值x_1=12, x_2=15, x_3=9, x_4=21。按照前面的步骤进行加密，位置置乱后的图像如图 1(b)所示，最终加密的效果如图 1(c)所示。



(a)原始图像　(b)第 1 次加密的图像　(c)第 2 次加密的图像

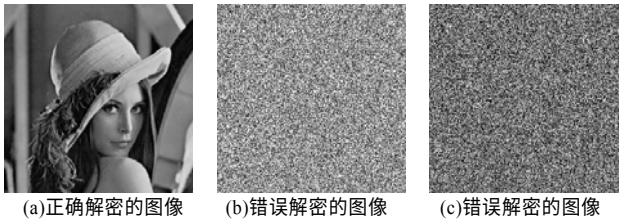
图 1　原始图像和加密后的图像

从图 1 中可以看到，加密之后的图像已经没有原始图像的任何信息，从而达到了图像加密的目的。为了验证加密算法的有效性，可以对该方法进行安全性分析。

2.2 安全性分析

(1)敏感性分析

混沌加密的安全性就在于它的初始值敏感性，也就是说攻击者用与初始值很相近的一个数值进行破解，也不能恢复出原始的图像。图 2(a)是正确解密的图像，图 2(b)是x_1=12, x_2=15,x_3=9,x_4=21.000 001 破解的图像，图 2(c)是x_1=12.000 02, x_2=15,x_3=9, x_4=21 破解的图像，可以看到和初始值有微小的差值也不能恢复原始的图像。因为在一般的计算机系统中，十进制小数双精度为 15 位，采用穷举攻击的难度将达到 10^{15}，所以用穷举法进行攻击显然是不行的。



(a)正确解密的图像　(b)错误解密的图像　(c)错误解密的图像

图 2　正确解密图像和错误解密图像

(2)时间复杂度分析

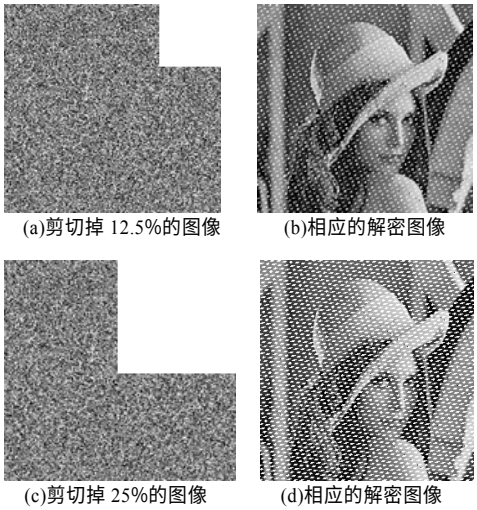
本算法中，生成混沌序列需要迭代 $M \times N$ 次，若问题的规模为 m，则生成混沌序列的时间复杂度为 $O(m)$。为线性阶的时间复杂度,而且时间复杂度较低。为检测算法的时间开销,对不同大小的 8 位和 24 位 BMP 位图进行了大量的加解密实验。实验所采用的硬件系统是 Pentium4 1.8 GHz CPU, 256 MB DDR 内存；软件系统为 WindowsXP 操作系统，Matlab 编程平台。在实验中，对数据大小为 1.93 MB 的 1 024×768 的 24 位 BMP 图像加密所用的时间约为 0.35 s，解密所用的时间约为 0.361 s，可见算法的效率是较高的。

(3)空间复杂度分析

算法中主要的空间开销是保存混沌序列所使用的 4 个一维数组。它们总的大小等于图像像素数。如果待加密图像大小为 $M \times N$，采用 int 型的数组，则它们总的大小为 $M \times N$ 个 int 型的空间。可见空间开销只与图像大小有关，与图像位数无关。例如，对一幅 1 024 ×768 大小的图像，其空间开销约为 1 024 ×768 ×4 / (1 024 ×1 024)≈ 3 MB。若问题规模为 m，则算法的空间复杂度为 $O(m)$，为线性阶的空间复杂度。

(4)图像处理攻击分析

如果加密图像被攻击者进行恶意破坏，如加噪、滤波、剪切等图像处理操作，测试结果表明：对加密图像的轻微改变并不影响图像的解密操作。图 3(a)是对加密图像剪切掉 12.5%的图像，图 3(b)是相应的解密图像；图 3(c)是对加密图像剪切掉 25%的图像，图 3(d)是相应的解密图像。可以看到剪切 12.5%对图像的恢复没有太大的影响，即便是剪切掉 25%，也可以清晰地看到原始图像的轮廓。



(a)剪切掉 12.5%的图像　(b)相应的解密图像

(c)剪切掉 25%的图像　(d)相应的解密图像

图 3　剪切加密图像的解密结果

(下转第 149 页)