文章编号:1671-4598(2019)08-0254-04 DOI:10.16526/j.cnki.11—4762/tp.2019.08.053 中图分类号:TP391.41;TP309.7 文献标识码:A

# 基于混沌理论的图像加密技术研究

陈龙彪，谌雨章，邹 鹏
（湖北大学 计算机与信息工程学院，武汉 430062）

**摘要**：为对基于混沌理论的图像加密技术有一个更加系统的了解，对其进行了一个简单的研究；混沌密码学因其较低的数学复杂性和更好的安全性而受到越来越多的关注；它成功避免了数据扩展，从而降低了传输成本和传输延迟，基于混沌理论的数字图像加密技术利用了被称为混沌映射的离散非线性系统动力学原理，根据系统的类型，可以使用多种类型的混沌映射；通过对已有的基于混沌理论的加密技术进行归纳总结，并进行相关的实验研究，寻找其中的异同点，以谋求对这一领域的进一步了解。

**关键词**：混沌理论；图像加密；对称密码学

# Research on Image Encryption Technology Based on Chaos Theory

Chen Longbiao, Chen Yuzhang, Zou Peng
(School of Computer Science and Information Engineering, Hubei University, Wuhan 430074, China)

**Abstract**: In order to have a more systematic understanding of image encryption technology based on chaos theory, a simple study is carried out. Chaotic cryptography has received more and more attention due to its lower mathematical complexity and better security. It successfully avoids data expansion, which reduces transmission cost and transmission delay. The digital image encryption technology based on chaos theory utilizes the principle of discrete nonlinear system dynamics called chaotic mapping. According to the type of system, multiple types of Chaotic map can be used. Through summarizing the existing encryption technology based on chaos theory, And carrying out the related experimental research. We look for similarities and differences, as to seek further understanding of this field.

**Keywords**: chaos theory; image encryption; symmetric cryptography

## 0 引言

伴随着数字信号处理技术、网络技术以及通信技术的迅速发展，越来越多的数字图像、音频和视频等以数字媒体的形式通过网络来进行传播[1]。然而，数字信息其本身的特点决定，其通过开放或不安全的系统来传输信息时，极易被他人所截取获褚篡改。因此，如何保证数字信息的安全性及其完整性已然成为了现代信息科学研究的一个十分重要的课题[2-3]。

现代密码学领域可分为多个研究领域，但总的来说，它们可以被大致分为两大类型：对称密钥密码学和非对称密钥密码学。通常情况下，对称密钥密码学因其特性而被优选用于诸如图像和视频的大数据加密[4-6]，而混沌密码学正是属于对称密钥密码学的范畴。密钥用于产生混沌系统的参数或初始值，混沌加密技术通过置乱和扩散运算，将明文图像转化为不可理解的密文图像，通常来说，这两个运算会被重复执行多次直到达到足够的加密级别。具体的加密过程如下图所示：

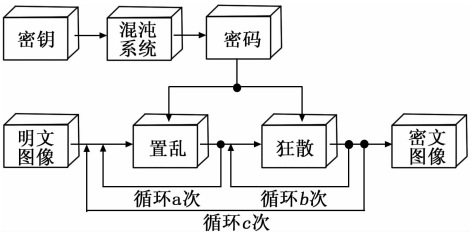



图1 数字图像加密过程

图像加密质量通过测试其防御不同攻击的能力，例如已知的明文攻击，密码文本攻击，统计攻击和暴力攻击等。每次攻击的防御能力取决于所选映射的某些属性及其配置参数。

## 1 相关理论基础

### 1.1 密码学

密码学是研究密码编制和密码破译的技术科学以及信息安全研究领域的核心学科，用于研究信息的安全获取、安全储存以及安全传播[7]。研究密码变化的客观规律，用以进行密码编制以保守通信秘密的分支，称为编码学；用以进行密码破译以获取通信情报的分支，称为破译学，二者合称为密码学。在密码学中，原始信息被称为明文，而经过转换加密后的信息称为密文，加密过程中使用的伪随机序列被称为密码，用于生成密码的关键信息被称为密钥。综上所述，一个完整的加密系统至少包含五要素，即：明文、密文、密钥、密码以及加密算法。同理，解密系统也需要五要素，只是要将加密算法替换成解密算法，这里可

**收稿日期**:2019-04-05； **修回日期**:2019-04-28。
**基金项目**:湖北省大学生创新创业训练计划项目(201710512051,201810512051)。
**作者简介**:陈龙彪(1997-),男,湖北咸宁人,大学生,主要从事深度学习、图像处理方向的研究。
**通讯作者**:谌雨章(1984-),男,湖北武汉人,博士,副教授,硕士生导师,主要从事光电探测、图像处理方向的研究。

以认为解密算法是加密算法的一个逆过程。一个常见的密码系统可以用图 2 来表示。

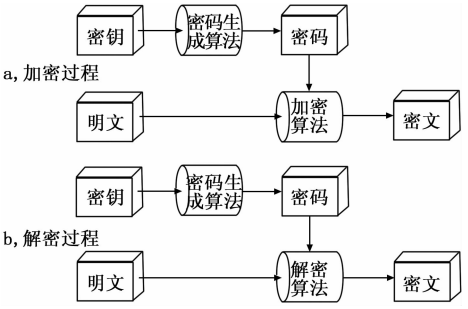



图 2　常见密码系统

### 1.2　典型混沌系统

1.2.1　Logistic 映射

混沌映射指的是从空间某一区域到其本身的一个连续函数。一维 Logistic 映射是一类十分简单却已经被研究得十分成熟的系统，可定义为：

$$x(n+1)=\mu x(n)[1-x(n)] \tag{1}$$

其中，当满足 $3.569945627<\mu\leqslant 4$ 时，系统在 $[0,1]$ 上是混沌的。

1.2.2　Arnold 映射

Arnold 映射是二维图像置乱系统中使用最为频繁的混沌系统之一，因其由 Arnold 和 Avez 提出的，并在猫脸图像上进行的实验，所以该映射也被成为 Cat 映射。其映射方程如下：

$$\begin{bmatrix}x_{n+1}\\y_{n+1}\end{bmatrix}=\begin{bmatrix}1 & m\\ n & mn+1\end{bmatrix} \tag{2}$$

其中：$m$ 和 $n$ 均为实数，且 $x_n$，$y_n\in[0,1)$。

基于 Arnold 映射的置乱操作仅需要经过几组简单的线性变换和取模运算，就能非常有效地对图像完成置乱，也正是这个原因，才使得 Arnold 映射在图像置乱加密领域有着极其重要的地位。

1.2.3　Lorenz 混沌系统

Lorenz 混沌系统是美国气象学家洛伦兹在研究天气预报时提出的一个系统，因此也称为大气对流模型。他将提出的模型进行简化，得到了如下的方程组：

$$\begin{cases}\dot{x}=-\sigma(x-y)\\ \dot{y}=-xz+\lambda z-y\\ \dot{z}=xy-bz\end{cases} \tag{3}$$

有两组固定参数可选，分别为 $\sigma=10$，$\lambda=28$，$b=3$ 和 $\sigma=16$，$\lambda=40$，$b=4$。Lorenz 混沌系统通过数值积分来获取具备实数值的混沌序列。

### 1.3　混沌密码系统基本规则

早在 2006 年，G. Alvarez 等人通过大量基于混沌系统的图像加密文献的阅读，发现很多文献其实并不具备密码系统的基本要素，实际上并不能付诸实际亦或是并不具备安全性，或者说是对系统安全性能的分析不够，有的甚至直接出现了无密钥系统。在这样一个严峻的环境下，为有一个统一的标准，G. Alvarez 通过文献的总结提炼，提出了混沌密码系统的基本规则[8]，且这些规则已经得到了密码学专家的普遍认可：

Rule 1：应该对使用的混沌系统的实现方法和过程进行尽可能详细的描述。

Rule 2：如果是离散化的连续混沌系统或是数字形式的混沌系统，应对其退化情况和伪随机序列的统计特性进行讨论。

Rule 3：在安全性能不受影响的前提下，密码系统应该尽可能简单易实现，并且实现的速度也希望尽可能的快。

Rule 4：密钥应明确定义。

Rule 5：密钥空间应该明确定义，且密钥空间中密钥的有效性应给予讨论。

Rule 6：密钥空间中密钥的敏感性应给予讨论，以使得两个具有微小差别的密钥加密同一明文得到的密文内容截然不同。

Rule 7：未知部分密钥的信息不能通过已知部分密钥得到，明文信息也无法通过部分密钥解密密文得到。

Rule 8：通过密钥来产生密码的算法是唯一确定的，应该对其做十分精确的描述和限定。

Rule 9：密码系统应该具备明文敏感和密钥敏感的特点，意思是具有微小差别的两个密钥加密同一明文得到的密文信息应截然不同，同样，同一密钥加密具有微小差别的两段明文，所得到的密文信息也要截然不同。

Rule 10：加密得到的密文应该与随机噪声相比拟，它的统计特性应该与密钥的选择无关。

Rule 11：所设计的密码系统能够对抗当前已知的被动攻击方法。例如，能对抗唯密文攻击、已知明文攻击、选择密文攻击等等攻击方法。

Rule 12：密码系统能够对抗线性攻击方法和差分攻击。

Rule 13：密码系统能够对抗现有的各式特殊攻击方法的攻击，例如基于混沌预测、混沌相位分析和混沌同步的攻击方法等。

Rule 14：密码系统能够对抗现有的各式特殊应用攻击方法的攻击，比如通过特殊图像来进行攻击的方法等。

Rule 15：密码系统应该能对抗穷举攻击，要求密钥的长度大于 100b。

Rule 16：应该混沌伪随机序列进行统计特性分析。

Rule 17：保密通信系统应该通过实际的网络通信信道的测试。

以上规则简而概之就是：1）混沌序列发生器能够快速生成统计特性优良的伪随机序列；2）密钥长度应该大于 128b，由有效密钥所构成的密钥空间应该足够大；3）密码系统对明文、密文、密钥都是十分敏感的；4）密文的统计特性应该与噪声想比拟；5）密码系统可以极有效地抵抗 6 类被动攻击的方法；6）加密和解密的速度应足够快。

## 2　相关技术研究及分析

### 2.1　扩散技术研究

扩散意味着扩展单个明文数字对许多密文数字的影响，因此明文的统计结构变得不清楚。在不改变像素点原来位

置的前提下，将任意一个明文的像素点信息尽可能多的隐藏在多的密文的像素点中。

Yaobinmao 等人[9]提出，将一维 Logistic 映射用于生成扩散模板：

$$x(n+1)=4x(n)[1-x(n)] \tag{4}$$

映射生成的值最初是浮动的并且始终维持在 0.2～0.5 之间，然后对每 8 比特数据进行缩放和量化，这可以直接用于 XOR 和 MOD 操作，映射的初始值取自密钥。Alireza Jolfaei 等[10]提出的一种基于 W7 密码流的加密方法，W7 密码流是一种同步对称加密流，旨在以非常高的数据速率实现高效的硬件实现，该算法支持 128 位的密钥长度，由一个控件和一个功能单元组成。

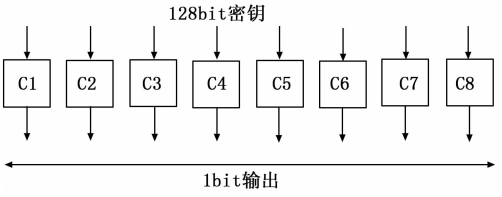



图 3 W7 流混沌序列发生器

Musheer Ahmad 等人[11]使用一维 Logistic 映射生成扩散模板，该模板类似于文献［9］中提出的方法，在生成模板 XOR 操作后进行扩散。Xin Ma 等人[12]提出了使用 Chebyshev 映射作为密码流生成器，其描述如下：

$$x(n+1)=T_k(x_n)=\cos(k\cdot\arccos(x_n)) \tag{5}$$

其中：$x_n\in[1,-1]$，$k$ 和 $x_n$ 分别是参数和状态值。

若满足 $k\in 2^k$，即切比雪夫的阶数时，系统是混乱的。初始值 $x(0)$ 和参数 $k$ 用作扩散模块的密钥。在文献［9］中也使用了 Logistic 映射来生成扩散模板，但是他们还添加了耦合强度因子，它在 XOR 操作之前修改了生成像素的权重，它可以表示为：

$$Shuffled\_image\oplus Keystream=Chipher\_image$$

其中：$f$ 是耦合强度因子。$f\in(0,1)$。

### 2.2 置乱技巧研究

所谓置乱，从另一方面来说，也就是使用使密文统计信息对明文统计信息的依赖关系复杂化的转换。最常用的置乱算法大致可分为三大类：第一类，将行置乱和列置乱或者说是交叉行、列置乱应用于二维图像矩阵；第二类，先把二维图像降维展开成一维的列向量或者一维的行向量，然后再对降维后的向量进行置乱操作；第三类，通过 2×2 置乱矩阵来对二维图像中的所有点的位置进行变换。

Yaobinmao 等人[9]首先提出将二维图像转换为三维，通过使用二维到三维转换技术来达到更深层次的置乱，具体操作如式（6）所示：

$$W\times H=W_1\times H_1\times D_1 \tag{6}$$

其中 $W$ 和 $H$ 是原始图像的宽度和高度（以像素为单位），$W_1$，$H_1$ 和 $D_1$ 是三维空间的新维度标尺。

数字图像经过三维变换后，再由三维映射关系进行混沌，等式（7）表示三维映射图方程组。

$$\begin{cases}\left(2x,2y,\dfrac{z}{4}\right) & 0\leqslant x\leqslant\dfrac{1}{2},0\leqslant y\leqslant\dfrac{1}{2}\\ \left(2x,2y-1,\dfrac{z}{4}+\dfrac{1}{2}\right) & 0\leqslant x\leqslant\dfrac{1}{2},\dfrac{1}{2}\leqslant y\leqslant 1\\ \left(2x-1,2y,\dfrac{z}{4}+\dfrac{1}{4}\right) & \dfrac{1}{2}\leqslant x\leqslant 1,0\leqslant y\leqslant\dfrac{1}{2}\\ \left(2x-1,2y-1,\dfrac{z}{4}+\dfrac{3}{4}\right) & \dfrac{1}{2}\leqslant x\leqslant 1,\dfrac{1}{2}\leqslant y\leqslant 1\end{cases} \tag{7}$$

在文献［10］中，使用了基于 Henon 映射的混沌方法。Henon 映射是由具有混沌吸引因子状态方程表示的二维可逆迭代映射的原型，是依农（Henon M）在 1976 年提出的洛伦兹方程的庞加莱映射的简化模型。二维 Henon 映射定义如下：

$$\begin{aligned}x_{n+1}&=1+y_n-ax_n^2\\ y_{n+1}&=\beta x_n\end{aligned} \tag{8}$$

初始点为 $(x_0,y_0)$，$(x,y)$ 是系统的二维状态。当 $a=1.4$ 且 $\beta=0.3$ 时，系统处于混沌状态。为了减小相邻像素相关性，置乱图被应用于垂直和水平两个不同方向上。

Ahmad M 等[11]提出了基于 Cat 映射和块的混沌算法，在基于块的算法中，首先将图像划分为较小的块，然后在块被混沌之后，每个块被独立地混沌，因为 Cat 映射具有循环重复的属性，所以他们在每轮迭代之后，都会使用二维 Logistic 映射来改变 Cat 映射的参数。

二维耦合 Logistic 映射表达式如式（9）：

$$\begin{aligned}x_{n+1}&=\mu_1\mu_2(1-x_n)+\gamma_1y_n^2\\ y_{n+1}&=\mu_1y_n(1-y_n)+\gamma_2(x_n^2+x_ny_n)\end{aligned} \tag{9}$$

引入三个二次耦合项，增强二维 Logistic 映射的复杂性。当满足条件（9）时，该系统是混沌的，并且在区间（0，1）中产生混沌序列 $x$，$y$。

$$\begin{cases}2.75\leqslant\mu_1\leqslant 3.4\\ 2.7\leqslant\mu_2\leqslant 3.45\\ 0.15\leqslant\gamma_1\leqslant 0.21\\ 0.13\leqslant\gamma_2\leqslant 0.15\end{cases} \tag{10}$$

### 2.3 密钥空间分析

密钥空间指的是所有的合法密钥所构成的集合。如果窃听采用穷尽的方法来破解密码系统的加密或者是解密系统，概率意义上来说，只需要尝试密钥空间中一半的密钥。对于已经知道的明文和密文对，用借助加密过程来破解密钥时，由已知的明文和随机选择的密钥，由加密设备设备得到相应的密文，如果所得到的密文与已知的密文完全一致，那么随机选择的密钥就是真是的密钥；而当借助于解密的过程来破解密钥时，由已知的密文和随机选择的明文密钥，由解密设备得到的相应的明文，如果得到的明文与已知的明文完全相同，则随机选择的密钥为真是的密钥。

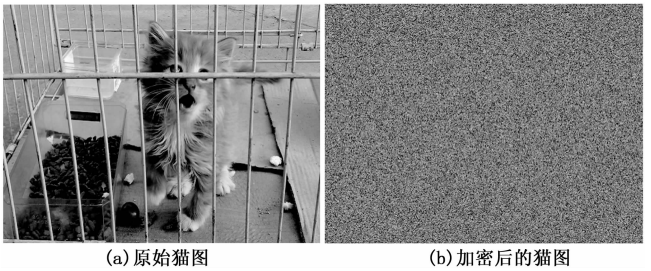
一个好的图像加密算法应该对密码密钥十分敏感，并且密钥空间应该大到足以使暴力攻击变得不可行，尤其是对于加密/解密速度非常快的密码系统，密钥长度应该至少为 128b。根据目前的计算机水平，多数密码学者建议采用 128b、192b、256b 或者 512b 长的密钥。

Yaobin Mao[9]方法的密钥长度为 128 位且对密钥非常

敏感，结果表明密钥中的单个位变化导致解码图像之间的差异达到 99.59%。文献［10］具有 128 位密钥，密钥空间大小为 $2^{218}$。此外，如果我们将混沌算法的两个子点视为密钥的一部分，则密钥空间大小将更大。这意味着如果精度为 $10^{-14}$，则密钥空间可以达到 $3.66\times10^{66}$。显然，密钥空间足够大，可以抵御各种暴力攻击。文献［11］中描述的算法在使用了 8 个混沌映射的初始条件，并且 $x_0$，$y_0$，$z_0$，$\mu_1$，$\mu_2$，$\gamma_1$，$\gamma_2$ 和 $\lambda$ 的初始条件可以用作加密和解密的秘密密钥。在这种情况下，若精度为 $10^{-14}$，则密钥空间大小为 $(10^{14})^8$，其已经足够大以抵抗任意暴力攻击。因此可以看出，只要密钥空间足够大，就可以有效地防止入侵者的所有暴力攻击。

## 3　实验结果与分析

为进一步了解基于混沌理论的图像加密算法的一个有用性与正确性，设计相关实验进行验证，对一张清晰的猫图片进行加密，得到了加密的图片，加密前后的猫图如图 4 所示。



(a) 原始猫图　　(b) 加密后的猫图

图 4　加密前后的猫图进行对比

通过的加密前后的猫图片的 RGB 三个通道灰度值的出现的概率进行统计，来分析经过基于混沌理论加密后图像是否满足混沌密码系统的基本规则，并分析其加密的安全性，得到的加密前后的猫图的 RGB 三通道的直方图分别如图 5、6 所示。从直方图可以看出，加密前的图像三个通道的直方图中，每种灰度的频率各不一样，能直接反映出图像的信息。而反观加密后的图像的三个通道的直方图，可清晰的发现各个通道的不同灰度值的出现频率是一致的，说明加密成功，满足前文提到的加密规则，同时，也说明加密成功，攻击者无法通过加密后的图片获得原始图像的相关信息。

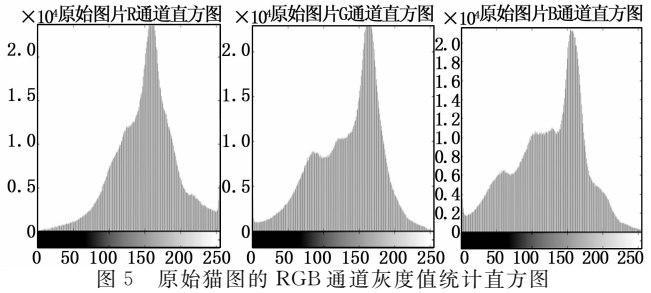



图 5　原始猫图的 RGB 通道灰度值统计直方图

## 4　结束语

通过研究大量的基于混沌加密的图像加密算法后，可以得出结论，基于混沌加密的图像加密算法的架构和遵守的规则几乎都是一模一样的，差异仍在于所选用的映射类型，控制方式以及控制映射的参数数量不同，这反映了系统的鲁棒性，基于混沌加密的图像加密算法的这种特性同时也简化了混沌算法用于图像加密的一个数学过程。

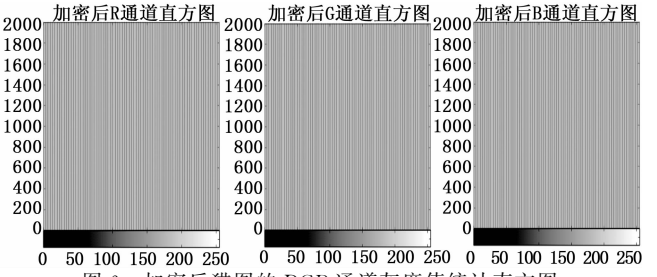



图 6　加密后猫图的 RGB 通道灰度值统计直方图

尽管基于混沌的图像加密算法对图像的加密有较好的效果，但是由于数字图像具有数据量巨大且数据冗余度及其高以及相关性强的特点，现有的基于冯诺依曼计算理论的数字计算机仍然显得力不从心，所以寻找新的计算工具和计算理论来对数字图像进行加密显得格外迫切。近年来的基于 DNA 编码和计算以及量子计算的发展，有望解决这一难题，数字图像的加密在今后肯定也会有一个更好的前景。

**参考文献：**


[1] 廖建华. 基于混沌理论的数字图像加密技术研究［D］. 长沙：中南大学，2010.

[2] 张　伟. 混沌理论在数字图像加密技术中的应用研究［D］. 2013.

[3] Menezes A J，Vanstone S A，Oorschot P C V. Handbook of Applied Cryptography［M］. Floriada：CRC Press，1996.

[4] 葛　滨，鲁华祥，陈　旭，等. 基于超混沌的快速图像加密算法［J］. 系统工程与电子技术，2016，38（03）：699－705.

[5] 闫　兵，柏　森，刘博文，等. 基于交叉混沌映射的小波域图像加密算法［J］. 计算机应用研究，2018，35（06）：1797－1799，1811.

[6] 拜亚萌，张燕玲，邓小鸿. 自适应分块的医学图像混沌加解密算法［J］. 计算机应用研究，2018：1－5.

[7] 郑　东，赵庆兰，张应辉. 密码学综述［J］. 西安邮电大学学报，2013，18（06）：1－10.

[8] Gonzaloalvarez，Shujunli. Some basic cryptographic requirements for chaos－based cryptosystems［J］. International Journal of Bifurcation & Chaos，2006，16（08）：2129－2151.

[9] Yao B M，Guan R C，Shi G L. A novel fast image encryption scheme based on 3D chaotic baker maps［J］. International Journal of Bifurcation and Chaos，2011，14（10）：3613－3624.

[10] Jolfaei A，Mirghadri A. An image encryption approach using chaos and stream cipher［J］. Journal of Theoretical & Applied Information Technology，2010，19（2）：117－125.

[11] Ahmad M，Alam M. A new algorithm of encryption and decryption of images using chaotic mapping［J］. International Journal on Computer Science & Engineering，2010，2（1）：46－50.

[12] Ma X，Fu C，Lei W M，et a. A novel chaos－based image encryption scheme with an Improved Permutation Process［J］. International Journal of Advancements in Computing Technology，2011：223－233.