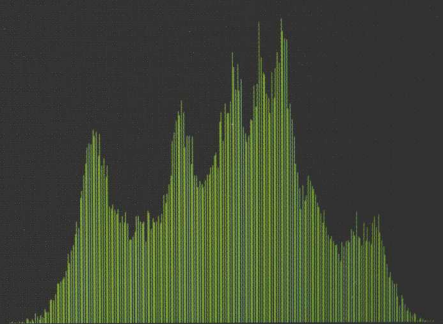
电子信息与电气工程技术丛书 E&E

国家自然科学基金（编号：61562035）资助出版

Chaotic Digital Image Cryptosystem

混沌数字图像加密

◎ 张勇 著
Zhang Yong



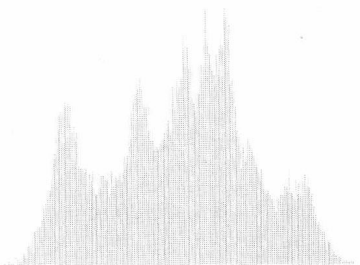
清華大學出版社

工程技术丛书 E&E

Chaotic Digital Image Cryptosystem

混沌数字图像加密

◎ 张 勇 著
Zhang Yong



清華大學出版社
北京

内 容 简 介

本书系统地研究了基于混沌系统的数字图像密码方案与算法及其安全性能分析，重点在于阐述明文关联的快速数字图像密码算法及其安全性能。全书共6章：第1章讨论基于混沌系统的数字图像密码技术研究的发展历程，分析了各个发展时期数字图像密码系统的特点；第2章阐述常用于数字图像密码系统的混沌系统，并讨论了混沌序列的伪随机特性；第3章介绍广泛应用的经典混沌数字图像密码方案和常用的置乱与扩散算法，并阐述了这些算法的安全性能；第4章从七个方面分析基于混沌系统的数字图像密码方案的安全性能，刻画了这些安全性能的数量指标；第5章重点诠释明文关联的混沌数字图像密码算法及其安全性能，并提出“扩散—置乱—扩散”的数字图像加密架构以及加密与解密共享算法的图像密码系统；第6章分析基于DNA计算与混沌系统的典型数字图像加密系统及其面临的挑战，并展望了基于量子计算与混沌系统的数字图像密码技术。

本书可作为高等院校信息安全相关专业的高年级本科生或研究生拓展阅读材料，也可作为信息安全专业高级工程技术人员的参考用书。

图书在版编目(CIP)数据

混沌数字图像加密/张勇著. --北京：清华大学出版社，2016
电子信息与电气工程技术丛书
ISBN 978-7-302-45006-1

Ⅰ. ①混…　Ⅱ. ①张…　Ⅲ. ①混沌－数字图像－图像编码－加密技术　Ⅳ. ①TN919.81

中国版本图书馆CIP数据核字(2016)第216149号

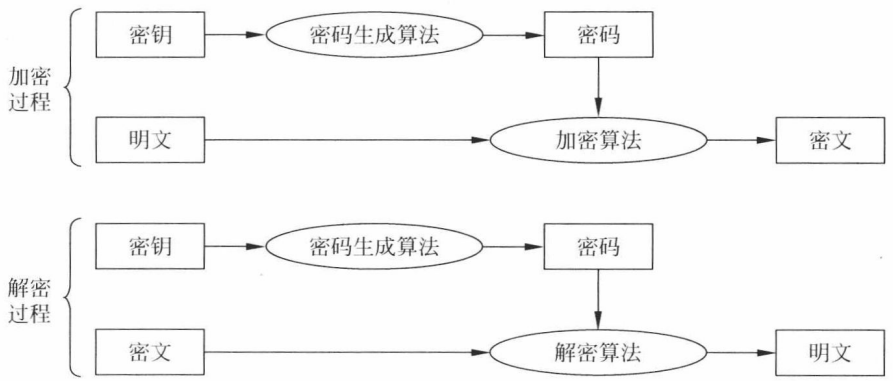
责任编辑：刘　星　战晓雷
封面设计：刘　键
责任校对：焦丽丽
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：14.25　　**字　　数**：346千字
版　　次：2016年10月第1版　　**印　　次**：2016年10月第1次印刷
印　　数：1～1500
定　　价：49.00元

产品编号：070547-01

前言

密码学是信息安全研究领域的核心学科，是研究信息安全获取、安全存储与安全传播的理论。通俗地说，密码学是研究将信息转化为秘密信息的算法的科学。一般地，信息是指有价值的消息，在密码学中，原始的信息被称为明文，转化后的秘密信息被称为密文，转化过程或规则称为加密，加密过程中使用的伪随机数序列称为密码，产生密码的关键信息称为密钥。因此，加密系统至少包括五个要素，即密钥、密码（或密码生成算法或规则）、明文、密文、加密算法（或规则）。解密系统是加密系统的逆系统，也至少包括五个要素，即密钥、密码（或密码生成算法或规则）、明文、密文、解密算法（或规则）。这里，解密算法是加密算法的逆过程。一个典型的密码系统如下所示。



在密码系统中，如果加密过程的密钥与解密过程的密钥相同，此类加密系统称为对称密码系统，或称私钥密码系统（private key cryptosystem），如 DES（Data Encryption Standard，数据加密标准）和 AES（Advanced Encryption Standard，高级加密标准）加密系统；如果加密过程的密钥与解密过程的密钥不同，此类加密系统称为非对称密码系统，或称公钥密码系统（public key cryptosystem），如 RSA（由 Ron Rivest、Adi Shamir 和 Leonard Adleman 三位科学家提出）加密系统。目前，大部分密码学专家坚持这样的观点，即公钥密码系统主要用于通信双方交换私钥（或称对称密钥），或者由权威机构向其授权通信方广播私钥；而保密通信中信息的加密主要是通过私钥密码系统实现的。

尽管 DES 和 AES 仍然是当前应用最广泛的对称密码算法，但是，这两种算法主要用于加密文本信息，一般不适合用于加密数据量大、冗余度大和相关性强的数字图像信息，这促使密码学家寻求新型的快速数字图像加密算法。20 世纪 70 年代发展起来的混沌理论，为产生具有优良统计特性的伪随机数奠定了理论基础，并且混沌系统的初值与参数极端敏感性、非周期性和长期演化轨道不可预测性等特性与图像加密系统的密钥敏感性、密文呈噪声特性和明文敏感性等特性相对应。因此，基于混沌系统的密码产生算法

及其在数字图像加密研究方面的应用受到了广泛关注，并逐渐成长为密码学的一个重要研究分支，且隶属于对称密码系统的范畴。

本书研究基于混沌系统的数字图像密码方案与算法及其安全性能分析，重点在于阐述明文关联的快速数字图像加密算法及其安全性能。本书中的加密/解密算法和安全性能分析均基于 MATLAB 和 Mathematica 软件，但书中给出的程序代码均基于 MATLAB 软件。

全书内容共分为 6 章。

第 1 章讨论基于混沌系统的数字图像密码系统研究的发展历程，将该项研究的发展历程分为三个时期，即初期、蓬勃发展期和成熟期，分析了各个发展时期具有代表性的混沌数字图像密码系统的特点。

第 2 章阐述常用于数字图像密码系统的混沌系统，分析了混沌系统 Lyapunov 指数的计算方法，讨论了连续混沌系统的龙格-库塔(Runge-Kutta)数值离散化随机数生成方法，并借助 NIST(National Institute of Standards and Technology，美国国家标准与技术研究所)统计测试套件(Statistical Test Suite)测试了混沌序列的伪随机特性。

第 3 章介绍受到广泛关注的经典混沌数字图像密码方案与算法，界定了置乱算法与扩散算法的概念，然后深入讨论了图像加密系统中常用的置乱算法，分析了只有置乱算法的图像加密系统的安全性能，接着，重点讨论了基于“异或”运算、“加取模”运算、循环移位运算和域运算等的扩散算法。

第 4 章全面分析基于混沌系统的数字图像密码方案的安全性能，主要包括七个方面，即加密与解密速度、密钥空间、密文统计特性、密钥敏感性分析、明文敏感性分析、密文敏感性分析和信息熵。针对每个方面，均深入研究了其对应的数量指标和理论指标值。

第 5 章重点阐述明文关联的混沌数字图像密码方案与算法，提出了“扩散—置乱—扩散”的数字图像加密方案，基于该方案论证了明文关联的置乱算法与明文无关的扩散算法相结合的快速加密算法的安全性，并深入研究了加密算法与解密算法完全相同的新型图像加密算法。

第 6 章分析基于 DNA 计算与混沌系统的数字图像密码系统，讨论了常用 DNA 编码与计算方法及其面临的挑战。然后，展望了基于量子计算与混沌系统的数字图像密码系统。

本书由国家自然科学基金(编号：61562035)和江西省自然科学基金(编号：20161BAB202058)资助出版。

感谢江西财经大学软件与通信工程学院唐颖军博士、陈滨博士、廖汉程博士、吴文华副教授和邓松博士等专家学者在科研与教学方面对作者的关心与支持，感谢他们对书中核心理论和重要思想的启示和引导，感谢研究生侯文刚、张琼、李雪倩、于曼丽、何维和彭锦同学在图像密码算法的 MATLAB 和 Mathematica 实现方面所做的大量仿真实验工作，感谢我的爱人贾晓天老师在资料检索、书稿校正与文献整理等烦琐工作上为我节省了大量宝贵的时间。感谢清华大学出版社工作人员为本书出版所做的辛勤工作。

除了我们在混沌数字图像密码技术方面的研究成果外，本著作还引用了大量同行专家学者的文献，这些参考文献均为该研究领域中颇有影响力且备受关注的研究成果，但是，限于篇幅，相信仍有大量重要的文献资料被疏漏（特别是中文文献资料）。同时，由于作者水平有限，且该研究领域飞速发展，使得书中难免出现各种错误与不足，恳请同行专家和读者朋友批评指正（E-mail：zhangyong@jxufe.edu.cn）。

张　勇

于江西财经大学枫林园

2016年5月

目录

目录

第1章 绪论

密码学的初期诠释必须从1949年Shannon的杰作[1]谈起，Shannon认为有三种类型的保密系统，即①隐蔽系统(concealment system)，例如借助隐形墨水书写的不可见信息系统；②隐私系统(privacy system)，例如通信双方有专享的秘密通信信道和编码方式的系统；③真正意义上的保密系统(true secrecy system)，在隐蔽系统和隐私系统中，明文、密文和加密/解密算法都是被保密的对象，而在真正意义上的保密系统中，明文被加密后得到的密文是公开的(甚至加密算法和解密算法也是公开的)，只有密钥是受保护的。Shannon认为，密码学是研究真正意义上的保密系统。

Shannon定义了几个重要的概念：

(1)“纯”系统(“pure”system)，假设一个系统对一则明文连续实施加密处理、解密处理和加密处理，且三次处理使用的密钥互不相同，如果这三次处理可相当于对该则明文实施一次加密处理(采用的密钥与前三次处理互不相同)，则该密码系统称为“纯”的。显然，经典的一次一密系统是纯的；只有置乱操作而没有扩散操作的图像加密系统也是纯的。

(2)“相似”系统(“similar” system)，如果两个系统加密同一则明文得到的两个密文的统计特性相同，则这两个系统在密码分析的难度上相同。

(3) 理论安全系统(theoretical secrecy system)，又称为绝对安全系统，如果一个密码系统生成的密文，除了借助于正确的密钥外，无论多长时间，密码分析算法也无法破译，称该系统是理论安全的。

(4) 完美安全系统(perfect secrecy system)，要求密码的数量至少与明文编码的数量相同，对于文本密码系统而言，要求密文表示不同信息的后验概率分布与其表示不同信息的先验概率分布完全相同。

(5) 实用安全系统(practical secrecy system)，又称为计算安全系统，在现实条件下，破译该类系统的计算代价超过了该系统密文信息的价值。一个优良的混沌图像加密系统，属于密码学中的“实用安全”系统。

Shannon认为衡量密码系统安全性能最重要的5个指标如下：

(1) 保密量(amount of secrecy)。

例如,对一个文本加密系统采用唯密文攻击,能够破译该系统的密码(或密钥)所需要获取的最少密文数量称为保密量,Shannon 认为保密量越大,系统越安全。

(2) 密钥长度(size of key)。

密钥是用于产生密码的存根,在对称密码系统中,发信方需要借助专用秘密信道将密钥传递给收信方,甚至需要通信双方脑力记忆而非书面记录,Shannon 认为密钥长度应尽可能短小。

(3) 加密/解密算法复杂性(complexity of enciphering and deciphering operations)。

Shannon 认为,加密/解密算法应该尽可能简单,在 20 世纪 40 年代,大都借助手工推导设计密码算法,这种思想可以节省昂贵的计算设备开销。

(4) 误码扩散(propagation of errors)。

例如,在一个文本密码系统中,密文在传播过程中因受到噪声干扰而出现了误码,不妨假设仅有一个密文字符出现了误码,这可能导致收信方解密后的大量文本失真,甚至全部解密得到的文本均失真。Shannon 希望这个误码扩散程度应最小化。

(5) 消息膨胀(expansion of message)。

在一些文本密码系统中,为了达到更好的保密特性,加密过程中,常常会在明文中添加空字符等,使得加密后的密文长度较原先的明文长度增长了。Shannon 认为,加密后的密文长度不应超过原始明文信息的长度。

Shannon 关于密码系统的安全性能指标主要适用于基于文本的密码系统中,在基于混沌系统的图像密码系统中,我们对这些安全性能指标有了新的认识和理解,并扩展了许多新的安全性能指标。

图像数据相对于文本数据而言,具有数据量巨大、数据相关性强和数据冗余信息量大等特点,这使得传统的基于文本信息的密码系统不再适用于图像加密系统。根据图像的获取和处理两个阶段的不同特点,图像加密系统的研究有两个主要的分支:其一为基于图像在采集/显示过程中的加密与解密处理系统,称为光学图像加密/解密系统;其二为基于以数字信号形态存储与传递的数字图像数据的加密与解密处理系统,称为数字图像密码系统。基于混沌系统的数字图像加密与解密系统主要是隶属于数字图像密码系统,简称为混沌数字图像密码系统。在继续讨论混沌数字图像密码系统研究发展历程之前,对光学图像加密/解密研究方向的突出研究成果做简要介绍。

在光学图像加密/解密研究上做出奠基性工作的科学家是 P. Refregier 和 B. Javidi[2],其主要思想为:设 $f(x)$ 为要采集的光学图像信号,令 $n(x)$ 和 $b(x)$ 为两个独立的具有 $[0,1]$ 均匀分布的白噪声,然后,进行相位遮盖(phase mask),即令 $g(x)=f(x)\exp[i2\pi n(x)]$,接着,令 $H(v)=\exp[i2\pi b(v)]$,用 $H(v)$ 定义冲激响应 $h(x)$,即 $h(x)=\mathcal{F}^{-1}[H(v)]$。最后,加密后的图像信号为相位遮盖信号 $g(x)$ 与冲激响应信号 $h(x)$ 的卷积,即 $\varphi(x)=g(x)\cdot h(x)$。该算法的光学解密过程如图 1-1 所示。

在图 1-1 中,密文光学图像 $\varphi(x)$ 经过光学傅里叶变换后,与相位掩模 $\exp[-i2\pi b(v)]$ 相乘,再经过光学傅里叶反变换后得到 $f(x)\exp[i2\pi n(x)]$,输出到 CCD 阵列,得到明文光学图像 $|f(x)|^2$。对于 P. Refregier 和 B. Javidi 提出的光学加密与解密系统而言,$n(x)$ 和 $b(v)$ 是该系统的密钥。该方案提出五年后,B. Javidi 和 A. Sergent 与

E. Ahouzi 共同提出了双随机相位光学图像加密与解密系统[3]，之后，光学图像加密与解密研究领域成长为图像密码系统的热门研究课题，学者们针对双随机相位光学图像加密算法进行了各种新颖的改良，有些算法使用混沌系统构造随机相位编码[4-20]。需要着重指出的是，早在 2005 年，A. Carnicer 等人指出了某些类型的双随机相位光学加密算法无法对抗选择明文攻击方法[5]。

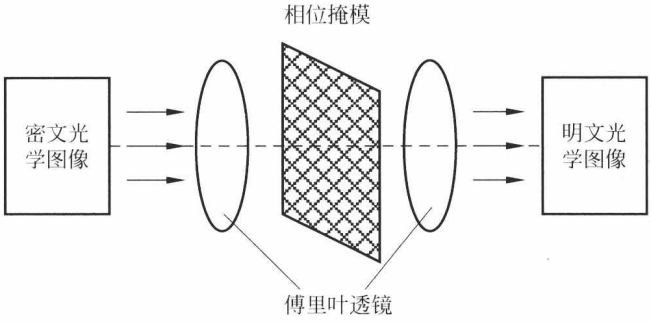


图 1-1 光学解密过程

图像光学加密与解密系统的研究为图像光学保密通信奠定了理论基础，并提供了安全保障。在光学图像加密研究兴起的同时，与传统文本加密算法类似的数字图像加密算法的研究也逐步开展起来，数字图像密码算法的研究也伴随着混沌伪随机序列的研究而发展和成熟。下面详细阐述混沌数字图像密码系统的研究进展情况。

1.1 混沌数字图像加密初期

数字图像的加密与解密操作需要大量的密码，这与“一次一密”技术的要求相同。第二次世界大战时期就提出来的“一次一密”(one-time pads)加密技术，对于任意一则明文信息，都要产生一则与该明文信息体积相同的密码，通过位异或运算得到等体积的密文信息。一次一密技术遗留的一个研究课题是如何产生大量的统计特性优良的随机数(或伪随机数)，“二战”时期由于计算设备的水平颇低，当时产生大量伪随机数的方法是有限的。1989 年，R. Matthews 在 Logistic 映射的研究基础上提出了一个广义的 Logistic 映射，并用该映射产生大量的伪随机数用于数据加密[21]。自此，混沌系统开始与加密系统结合起来，并开创了混沌系统产生伪随机数的新方法。

R. Matthews 提出的广义 Logistic 映射如式(1-1)所示。

$$g(x)=(\beta+1)\left(1+\frac{1}{\beta}\right)^{\beta}x\,(1-x)^{\beta} \tag{1-1}$$

其中，$1\leqslant\beta\leqslant4$，R. Matthews 使用式(1-1)所示混沌系统迭代产生的状态值的其中两位数字(建议取最后两位)，组合为一个新的十进制数(取值在 0～99 之间)，然后将通过取模(模 25)运算得到的数字与明文英文字符的位置序号相加，新的位置序号对应的英文字符即为密文字符。这里参数 β 和状态初值 x_0 为系统密钥，在文献[21]中，取 $\beta=2.53$ 和 $x_0=0.45$，前 5 个数据(使用当时的计算器)为 0.812980077、0.095875139、0.609135158、0.463757308 和 0.785823223，取各个数据的最后两个数字，并取模 25 运算依次得到 2、

14、8、8 和 23，如果加密 5 个明文字符 CHOAS，将得到 5 个密文字符 EVIWQ。

在文献[21]中，R. Matthews 在分析密码系统的性能时，仅考察了密钥空间的大小。对于显示长度为 D 位数字的计算器（去掉个位数字和小数点），密钥空间大小为 $K=10^{2D-4}$，定义密钥熵（key entropy）为 $H(K)$，满足 $2^{H(K)}=10^{2D-4}$，则 $H(K)\approx 6.6(D-2)$，$H(K)$ 就是用二进制数表示的密钥的长度。

R. Matthews 的密码算法主要是针对文本数据的加密与解密，而真正意义上的基于混沌系统的图像密码系统是于 1998 年由 J. Fridrich 提出来的[22]。如果说 R. Matthews 的最大贡献在于开创了借助混沌系统产生数据加密用的伪随机序列的先例，那么 J. Fridrich 的最大贡献在于提出了混沌系统迭代状态值直接用于置乱图像像素点的方法。在文献[22]中，J. Fridrich 的算法思想是这样的：图像中任一像素点可用三元组描述，如 $(x,y,f(x,y))$，其中 (x,y) 表示像素点的位置，$f(x,y)$ 表示位置为 (x,y) 的像素点的灰度值。把 x 和 y 作为二维混沌映射的状态输入，迭代后的状态作为像素点 (x,y) 的新位置，同时，变换 $f(x,y)$ 的值。她把基本的 Baker 映射（如式(1-2)所示）推广到离散 Baker 映射（如式(1-3)所示），同时也给出了 Cat 映射（著名的 Arnold 映射）（如式(1-4)所示）和标准映射（standard map）（如式(1-5)所示）及其离散形式（如式(1-6)所示）。

$$B(x,y)=\begin{cases}\left(2x,\dfrac{y}{2}\right), & 0<x<\dfrac{1}{2}\\ \left(2x-1,\dfrac{y+1}{2}\right), & \dfrac{1}{2}\leqslant x\leqslant 1\end{cases} \tag{1-2}$$

$$B_{(n_1,n_2,\cdots,n_k)}(r,s)=\left(\frac{N}{n_i}(r-N_i)+s \bmod \frac{N}{n_i},\frac{n_i}{N}\left(s-s \bmod \frac{N}{n_i}\right)+N_i\right) \tag{1-3}$$

其中，图像大小为 $N\times N$，n_i 是 N 的因数，且满足 $n_1+n_2+\cdots+n_k=N$，(r,s) 表示像素点的坐标，这里，$0\leqslant s<N$，$N_i\leqslant r<N_i+n_i$。

$$C(x,y)=\begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix} \bmod 1 \tag{1-4}$$

$$S(x,y)=(x+y \bmod 2\pi, y-k\sin(x+y) \bmod 2\pi) \tag{1-5}$$

其中，参数 $k>0$。

$$\begin{aligned}S(i,j)&=(S_1(i,j),S_2(i,j))\\&=\left(i+j \bmod N, j+K\sin\left(\frac{S_1(i,j)\cdot N}{2\pi}\right) \bmod N\right)\end{aligned} \tag{1-6}$$

其中，参数 $K>0$。

J. Fridrich 使用的扩散算法为 $f(x_n,y_n)=f(x_n,y_n)+G(f(x_{n-1},y_{n-1}) \bmod L$，这里 (x_{n-1},y_{n-1}) 为前一个更新了灰度值的像素点（而不是指相邻的像素点），映射 G 的形式可任选，L 为灰度等级数。

J. Fridrich 关于基于混沌系统的数字图像置乱算法的理解如此深入透彻，以至于其后很多年，在数字图像空间域置乱算法研究上都没有出现过大的创新算法。J. Fridrich 的创新性思想是混沌数字图像加密研究进入初期阶段的标志，在标准映射和 Baker 映射选择上，她更倾向于使用 Baker 映射，同样地，Baker 映射在文献[23,24]的密码系统应用中得到进一步的体现。J. Fridrich 在文献[22]中从 4 个方面讨论了图像密码系统的性能，即密钥空间、已知明文攻击、唯密文攻击（cipher-text only type of attack）和混沌映射

伪随机数序列发生器，这 4 方面的性能评价被广泛用于图像密码系统的评价上。

下面进一步讨论在数字图像加密初期阶段一些备受关注的数字图像密码系统研究成果。

G. Jakimoski 和 L. Kocarev 提出了块图像加密扩散算法[25]，对于一个 8 位的灰度图像块，设其包含 L 个像素点，其加密变换公式如式(1-7)所示。

$$x_{i,k+1} = x_{i-1,k} \oplus f_{k-1}(x_{i-1,1}, x_{i-1,2}, \cdots, x_{i-1,k-1}, z_{i-1,k-1}) \tag{1-7}$$

其中，$x_{i,k+1}$ 表示坐标点 $(i,k+1)$ 处的像素点的灰度值，$z_{i-1,k-1}$ 为某一个子密钥，$f_{k-1}(\cdot)$ 为给定的混沌序列发生函数，在文献[25]中给了两种形式，分别借助于 Logistic 映射(如式(1-8)所示)和指数映射(如式(1-9)所示)，这两种混沌序列发生函数如式(1-10)和式(1-11)所示。

$$x_{n+1} = 4x_n(1 - x_n) \tag{1-8}$$

$$x_{n+1} = a^{x_n} \bmod 1 \tag{1-9}$$

其中，$a>1$。

$$f(y_j) = \begin{cases} \text{floor}\left[\dfrac{y_j(256 - y_j)}{64}\right], & y_j < 256 \\ 255, & y_j = 256 \end{cases} \tag{1-10}$$

$$f(y_j) = \begin{cases} a^{y_j} \bmod 257, & y_j < 256 \\ 0, & y_j = 256 \end{cases} \tag{1-11}$$

在式(1-10)和式(1-11)中，$y_j = x_1 \oplus x_2 \oplus \cdots \oplus x_j \oplus z_j$。文献[25]提出的这种借助按位异或运算实现的扩散算法仍然被广泛应用于图像密码系统中。

K. W. Wong 提出了一种借助 Logistic 系统和动态查找表方法的混沌密码系统[26]，在该系统中动态查找表保存了密码，每加密一个字符更新一次查找表，更新方式如式(1-12)所示。

$$j = i + \frac{x - x_{\min}}{x_{\max} - x_{\min}} \cdot N \bmod N \tag{1-12}$$

其中，i 和 j 为查找表中的两项，$x_{\min}$ 和 $x_{\max}$ 为选定的 Logistic 状态的最小值和最大值，x 为 Logistic 映射的有效的状态值(即满足 $x_{\min}<x<x_{\max}$ 的状态值)，N 表示查找表的总项数。K. W. Wong 的密码系统是一种快速的本文数据加密系统，当时是作为对 M. S. Baptista 提出的密码系统[27]的一种改进。由于使用查找表形式更新密码可以有效地减少甚至避免费时的浮点数运算，所以，查找表方法对于图像密码系统而言也是一种有效的密码算法。

G. Tang 等提出了一种混沌系统与 S 盒子(S-box)结合的密码系统[28]，S 盒子原来主要用于表示 AES 算法中的替换矩阵表，后来被密码学者推广用于表示任何通过图表形式的密码替换算法，例如，文献[28]中使用的 S 盒子如图 1-2 所示。

在图 1-2 中，32 位的 Q'_n 通过图中所示的变换法则转化为 32 位的 Q_n。在设计图像密码系统中，结构清晰的非线性 S 盒子受到密码学者的青睐，因为 S 盒子可以快速实现密码的变换。但是，遗憾的是，AES 算法的 S 盒子的设计原理尚无法从数学上证明其合理性[29]，同样地，大多数 S 盒子的设计都是缺乏数学基础的猜想，如图 1-2 中的 S 盒子中，变换前后的两个密码的第 3 个字节(从左到右看)没有发生变化，但是该 S 盒子的确实现

了非线性变换。而且，密码学者们好像并不担心 S 盒子的合理性，而是密切关注 S 盒子产生的密码的平衡性和均匀性。

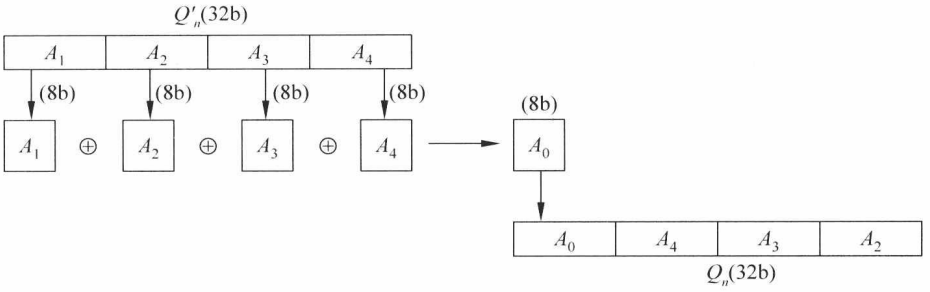


图 1-2　文献[28]中使用的 S 盒子

在混沌数字图像加密研究初期，一个极为有趣的现象是该时期提出的大量的密码系统被后来的密码学者一一破译，而破译的主要方法是各具特色的选择明文攻击方法，就连 J. Fridrich 提出的混沌数字图像密码系统也未能幸免。基于混沌系统的图像密码学在这种加密与解密的激烈争鸣中高速发展着。其中，N. K. Pareek、V. Patidar 和 K. K. Sud 提出的离散混沌密码系统表现尤为突出[30]，几乎与这项研究成果发表的同时，G. Álvarez、F. Montoya、M. Romera 和 G. Pastor 就提出了该图像密码系统的密码分析系统[31]。更为有趣的是，两年后，N. K. Pareek 等也提出了针对他们自己曾提出的该加密方案[30]的密码分析方案[32]。尽管 N. K. Pareek 等提出的密码系统存在着安全问题，但是他们的密码思想却颇有价值。大部分基于混沌的数字图像密码系统中，密钥直接取自混沌系统的参数值或者状态初始值，因此，密钥的长度不能事先确定，而且，在很多混沌图像密码系统中，所采用的混沌系统可以根据需要随意选择，从而必须选用相应的不同长度的密钥。

N. K. Pareek 的密码思想在于给定长度的密钥，例如给定 128 位（在文献[30]中最长为 128 位）长的密钥 K，按 8 位一组（一个字节），可得到 $K=K_1K_2\cdots K_{16}$，然后用于产生混沌系统的状态初始值 X 和迭代次数 N，如式(1-13)至式(1-16)所示。

$$X = (X_S + K_r/256) \bmod 1 \tag{1-13}$$

$$N = N_S + K_r \tag{1-14}$$

$$X_S = \frac{K_1 \oplus K_2 \oplus \cdots \oplus K_{16}}{256} \tag{1-15}$$

$$N_S = (K_1 + K_2 + \cdots K_{16}) \bmod 256 \tag{1-16}$$

式(1-13)和式(1-14)中的 r 为 1～16 的随机数，由 C 语言函数 rand()产生。借鉴这种由固定长度的密钥产生混沌系统的状态初始值和参数的方法，可以设计固定长度密钥的混沌图像密码系统。密码分析系统往往无法得到密码系统的密钥，而是根据加密算法或解密算法的漏洞，破译与密钥等价的密码，称为等价密钥。因此，用于数字图像加密的密码（即等价密钥）也需要考虑其安全性，使得窃听者不能根据其获得的密文推导出全部密码或部分密码。

2003 年，S. Lian 等人定义了“好”的密码系统的含义[33]，他们通过对 S. Papadimitriou 等人[34]提出的加密系统的密码分析，认为一个“好”的密码系统至少具有三方面的优点，即

应用安全性高、加密速度快和算法实现简单。在此基础上，S. Lian 给出了六条建议：

(1) 为避免计算机有限字长效应和混沌系统退化，在离散混沌系统迭代过程中，应使用伪随机数扰动方法；而对于连续混沌系统，应使用离散化后的差分系统动态特性已被证实的系统。

(2) 对单个图像块进行加密处理时，避免多次循环加密。

(3) 对于小数运算，尽可能使用定点运算，而少使用浮点运算。

(4) 应使用尽可能简单的混沌映射，例如，分段线性混沌映射(piecewise linear chaotic system)可有效地应用于密码系统中。事实上，S. Lian 等人对分段线性映射进行了深入的研究[35,36]，从理论上证实了其可产生统计特性优良的伪随机数序列。

(5) 应用多个混沌系统，而不是仅使用一个混沌系统，作为伪随机数发生器。

(6) 设计的混沌加密系统应避免前人已经发现的安全系统弱点，且能对抗现有的各种攻击方法。

众所周知，设计一个基于混沌系统的数字图像密码系统是一件很容易的工作，特别是在混沌数字图像加密研究初期，没有形成完整的密码系统评价体系，更没有类似文本加密系统中的 DES 和 AES 等标准算法可以对比参考，因此，S. Lian 等的研究工作[33]可以算是这个盲目设计加密算法的时期的终结。S. Lian 等尽管提出了一些设计图像密码系统应需注意的事项，但是他们没有提出具体的衡量图像密码系统的量化指标，这要求新的研究工作将从探索混沌数字图像加密系统的评价体系开始，从而刺激更好的图像加密算法的诞生。

1.2 混沌数字图像加密蓬勃发展期

为了衡量图像密码系统对抗差分攻击的能力，2004 年 G. R. Chen、Y. Mao、C. K. Chui 和 S. Lian 定义了两个指标[37,38]，即 NPCR 和 UACI，这两个指标已成为新提出的图像密码系统必须考察的两个性能指标，从而标志着混沌数字图像加密进入了蓬勃发展阶段。NPCR (Number of Pixels Change Rate) 和 UACI (Unified Average Changing Intensity)的定义为：设明文图像 P_1 与 P_2 除了某一个像素点(i,j)处的值相差 1 外完全相同，使用同一图像密码系统和相同的密钥加密明文图像 P_1 和 P_2，得到相应的密文图像 C_1 和 C_2，定义

$$D(i,j)=\begin{cases}0, & C_1(i,j)=C_2(i,j)\\ 1, & C_1(i,j)\neq C_2(i,j)\end{cases} \tag{1-17}$$

则有

$$\mathrm{NPCR}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)\times 100\% \tag{1-18}$$

$$\mathrm{UACI}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C_1(i,j)-C_2(i,j)|}{255-0}\times 100\% \tag{1-19}$$

根据 NPCR 和 UACI 的定义可知，NPCR 和 UACI 反映了图像密码系统的明文敏感程度，即明文的微小变化将导致图像密码系统产生的密文有多少比例的像素点的值发生了

变化(NPCR)或者像素点的值在多大程度上发生了变化(UACI)。G. R. Chen 等人没有给出 NPCR 和 UACI 的理论值,并且在文献[37,38]中,NPCR 的定义均有笔误(定义当 $C_1(i,j)=C_2(i,j)$时 $D(i,j)=1$)。Y. Zhang 在 2014 年时指出 NPCR 和 UACI 的理论值分别为 $255/256\approx99.6094\%$和 $257/768\approx33.4635\%$[39]。

NPCR 和 UACI 是作为衡量明文敏感性的指标被提出来的,但是,密码学者们也常用这两个指标衡量密钥敏感性和密文敏感性。当用作密钥敏感性时,是指当密钥改变 1 位时,基于同一图像密码系统和同一个明文图像,使用变化前后的密钥加密得到两个密文图像,进而由式(1-17)至式(1-19)得到 NPCR 和 UACI 的值。当用作密文敏感性时,首先借助设定的密钥和图像密码系统,加密给定的明文图像 P_1,得到对应的密文图像 C_1,然后改变图像 C_1 中的某一个像素点(i,j)的值(改变量为 1)得到图像 C_2,使用正确的密钥和图像解密系统解密图像 C_2,还原后的图像记为 P_2。最后,根据 P_1 和 P_2 计算 NPCR 和 UACI。

实际研究中,需要抽取大量的像素点样本集合进行测试处理,所以,常常使用平均的 NPCR 和 UACI 的值衡量明文敏感性、密钥敏感性和密文敏感性。G. R. Chen 等在文献[37,38]中使用了 5 种图像密码系统性能分析手段,即密钥空间、密钥敏感性、密文统计特性、明文敏感性(对抗差分攻击)、加密与解密速度等。他们在文献[38]中指出,由于图像密码系统的敏感性要求,使得密文图像不能承受 JPEG 有损压缩和任何类型的噪声干扰,这为图像压缩与加密融合研究提出了新的研究课题。

在混沌数字图像加密蓬勃发展期,密码学者们关于加密方案达成了高度的共识,即各种形式的混沌系统被用于产生加密(或解密)用的密码,密钥用于产生这些混沌系统的初始值或参数,密码通过置乱和扩散运算,将明文图像转化为不可理解的类似于噪声的密文图像,为了提高安全性,置乱和扩散运算需要循环多次,如图 1-3 所示。

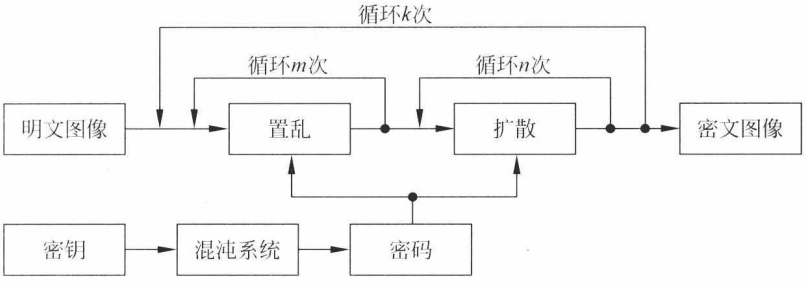


图 1-3　基于混沌系统的数字图像加密方案

下面列举使用了图 1-3 所示数字图像加密方案且借助 NPCR 和 UACI 指标进行加密性能分析的一些典型图像密码方案。

L. Zhang 等人于 2005 年提出一种基于离散指数混沌映射(Discrete Exponential Chaotic Map)和分段线性映射(Piece wise Linear Map)的图像加密算法[40],该算法首先将明文图像展开成一维向量,第一个元素保持不变,使用异或运算,将相邻的两个元素的异或值赋给后者,即仅使用明文进行一次信息扩散;然后,借助于某映射 f 和混沌序列 S 对上一步的中间结果图像进行坐标变换,即置换操作,其变换公式如式(1-20)所示。

$$\begin{cases} s = f(i) \\ t = j \oplus (s + \text{round}(256 \times k) \bmod 256) \end{cases} \tag{1-20}$$

这里，将坐标(i,j)变换为坐标(s,t)，其中，k为混沌序列S中的元素，round为四舍五入函数。

最后，将置乱后的图像I的每个像素点的值进行掩盖操作，如式(1-21)所示。

$$I = I + \text{round}(256 \times K) \bmod 256 \tag{1-21}$$

其中，K为与图像I大小相同的混沌伪随机矩阵。这种图像加密算法综合运用了置乱与扩散算法，但是文献[40]指出，上述加密算法只有当循环次数在4次以上时，NPCR和UACI指标的数值才比较接近理论值。

N. K. Pareek等人在文献[30,32]的基础上，提出了一种新的基于Logistic映射的图像加密算法[41]，与其以前的研究成果类似，使用了80位定长的外部密钥，通过组合异或、加取模256、取反等操作得到了8种类型的产生密码的方法，按每块16个像素点进行逐块加密。文献[41]进行了统计分析(直方图、相关性)、敏感性分析和密钥空间分析，但错误地引用了NPCR的定义。

H. S. Kwok和W. K. S. Tang于2007年提出了一种快速的混沌数字图像加密算法[42]，其算法核心为$c_i = (d_i + k_i + c_{i-1}) \bmod 2^{32}$，这里$d_i$、$k_i$和$c_i$分别表示第$i$个明文图像块、第$i$个密码和第$i$个密文图像块，每个图像块包含4个字节，加密算法的含义为第i个明文块与第i个密码的和再加上第$i-1$个密文块，模2^{32}后得到的结果即为第i个密文块，这种方法被证明是简单有效的加密算法。文献[42]的另一个贡献在于给出了解析形式的NPCR和UACI的期望值算式，如式(1-22)和式(1-23)所示。

$$\text{E[NPCR]} = (1 - 2^{-L}) \times 100\% \tag{1-22}$$

$$\text{E[UACI]} = \frac{\frac{1}{2^{2L}}\left(\sum_{i=1}^{2^L-1} i(i+1)\right)}{2^L - 1} \times 100\% \tag{1-23}$$

这里，L为像素点的灰度等级，即每个像素点的比特数，一般地，$L=8$，此时，E[NPCR]=255/256，E[UACI]=257/768，文献[42]中的E[UACI]有笔误，这里的式(1-23)是修正后的公式。

X. Tong和M. Cui在2008年提出了一种快速图像加密算法[43]，他们组合两个多项式得到一个新的混沌系统，使用该混沌系统产生加密系统的密码，图像加密方案包括两部分，其一为图像像素点的值与密码进行简单的异或运算；其二为了对抗选择明文攻击，对中间结果图像进行按行和列的移位操作，这样可使得NPCR和UACI的值接近于理想值。

2008年，K.-W. Wong等人提出了针对S. G. Lian等人的图像加密算法[44]的改进算法[45]，使用标准混沌映射(Chaotic Standard Map)产生密码，主要的改进在于：在扩散算法中，使用前一个密文图像像素点的低3位作为新的像素点的循环移位值，如式(1-24)所示。

$$c_i = [p_i + c_{i-1} \bmod L] >>> \text{LSB}_3(c_{i-1}) \tag{1-24}$$

这里，L表示像素点的灰度级数，p_i和c_i分别表示第i个明文像素点和第i个密文像素点，