图像密码算法设计与实现方面的优秀著作，呈现了DES和AES图像密码系统的C、C#与MATLAB实现技术，阐明了明文关联图像密码算法最新研究成果的设计方法与实现技巧，是图像信息安全科研工作者的必备参考书。

张　勇 著

数字图像密码算法详解

——基于C、C#与MATLAB

清華大學出版社

国家自然科学基金（编号：61762043）赞助出版

张　勇 著

数字图像密码算法详解
——基于C、C#与MATLAB

清華大學出版社
北京

内 容 简 介

本书系统地研究了新型数字图像密码系统及其安全性能，重点阐述了基于DES、AES的图像密码算法和基于混沌系统的明文关联图像密码算法的C、C#与MATLAB语言实现技术及其安全性能。全书分为7章，第1章回顾了图像密码技术领域的研究历程，并为后续章节的学习打下了基础；第2章详细分析了DES算法及其数字图像加密应用技术；第3章探讨了AES算法实现及其数字图像加密应用技术；第4章以基于AES的图像密码系统为例，从加密/解密速度、密钥空间、信息熵、统计特性和敏感性分析等方面探讨了图像密码系统的性能分析方法；第5章阐述了明文关联的图像密码系统的实现算法与性能分析；第6章讨论了加密算法与解密算法相同的图像密码系统的设计方法与性能分析；第7章诠释了融合公钥与私钥的数字图像密码算法及其性能评价体系。

本书可作为高等院校信息安全相关专业的研究生教材或拓展阅读材料，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

数字图像密码算法详解：基于C、C#与MATLAB/张勇著. —北京：清华大学出版社，2019
ISBN 978-7-302-52595-0

Ⅰ. ①数…　Ⅱ. ①张…　Ⅲ. ①数字图像处理－密码算法－研究　Ⅳ. ①TN911.73

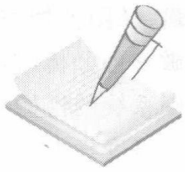
中国版本图书馆CIP数据核字(2019)第044619号

责任编辑：赵　凯　王一玲
封面设计：常雪影
责任校对：李建庄
责任印制：宋　林

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 刷 者：北京鑫丰华彩印有限公司
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：17.25　　**字　　数**：421千字
版　　次：2019年5月第1版　　**印　　次**：2019年5月第1次印刷
定　　价：59.00元

产品编号：078773-01

前言



1977年，美国国家标准局，即现在的美国国家标准与技术研究院（NIST）发布了数据加密标准（DES），这是地球上第一个用于文本信息加密的标准（为美国政府服务）。由于DES的密钥长度仅为56位，20世纪末的个人计算机已经可以在有限的时间内借助穷举密钥方法破译DES。于是2002年，NIST发布了高级加密标准（AES）取代DES。AES的密钥长度可以取128位、192位或256位，至今仍然为文本信息的加密标准。

然而，在数字图像加密方面，全球仍然没有一个标准密码算法，同时也没有衡量图像密码算法优劣的一系列标准指标。有些学者认为基于文本数据的AES算法不适合于数字图像加密，由于数字图像具有数据量巨大、信息冗余度大、相邻像素点相关性强等特点，AES用于数字图像加密可能存在加密速度慢、加密效果差的缺点。事实上，这种观点忽视了AES的强大数据加密能力。本书首先从DES和AES算法的阐述开始，详细分析了这两种数据加密算法应用于图像加密时的性能特点；然后以基于AES的图像密码算法的性能为比较基准，研究了3种基于混沌系统的图像密码算法。

全书内容共分为7章。

第1章首先回顾了图像密码技术的研究历程，按时间顺序，从Shannon关于保密通信的杰作开始，一直阐述到本书截稿时图像密码算法的最新研究成果；然后展示了本书使用的灰度图像以及3个软件平台，即MATLAB、Eclipse C和Visual Studio。其中，Eclipse C用于C语言开发，第2章的DES使用了C语言；而Visual Studio用于C#语言开发，全部章节的图像密码算法均使用了C#语言。

第2章首先详细介绍了DES算法结构及其实现方法，然后介绍了TDES（三重数据加密标准）算法及其在图像加密方面的应用技术，并给出了MATLAB、C语言和C#语言工程。一般地，由于MATLAB库函数丰富，所以MATLAB常用于图像密码算法快速实现，但是，MATLAB程序是解释执行的（MATLAB库函数除外），故MATLAB程序不能用于客观地评价图像密码算法的执行效率；C语言是比较图像密码算法执行速度的最佳语言，但是C语言程序调试复杂且图形界面设计难度大；C#语言的执行效率较C语言稍差，但是基于面向对象技术，程序健壮，本书借助C#语言评价图像密码算法效率。

第3章首先深入分析了AES算法的实现技术，并设计了其MATLAB和C#实现代码，接着，基于AES设计了两种图像密码系统，即AES-S和AES-D。AES-S系统是基于CBC模式使用AES加密大数据的标准结构。AES-D系统包含两个AES-S系统，实现了图像分块的双向加密处理。此外，附录B介绍了优化的AES图像加密MATLAB代码。

第4章在第3章的基础上，即以基于AES的图像密码系统（AES-S和AES-D系统）为

例，从图像加密/解密速度、密钥空间、信息熵、统计特性（包括相关性分析与直方图分析）和敏感性分析（包括密钥敏感性分析、明文敏感性分析和密文敏感性分析）等方面讨论图像密码系统的性能评价方法，并在本书使用的计算机配置下给出“优秀最低速度标准”和“合格最低速度标准”的定义方法及其数值，以衡量图像密码系统的加密/解密速度。

第5章研究了一种典型的明文关联的图像密码系统（PRIC），其由两个明文无关的扩散模块和一个明文关联的置乱模块组成，采用了“扩散—置乱—扩散”的系统结构。通过设计PRIC系统的MATLAB程序和C#程序，详细分析了PRIC的安全性能，并得出PRIC是一款优秀的图像密码系统的结论。

第6章研究了一种加密算法与解密算法共享的新型图像密码系统EADASIC。在EADASIC系统中，加密算法（含密码发生器）与解密算法（含密码发生器）完全相同，因此，EADASIC系统输入为明文图像和密钥时，输出为密文图像；而输入为密文图像和密钥时，输出为还原后的明文图像。在详细介绍EADASIC系统结构和算法的基础上，设计了其MATLAB程序和C#程序，并详细分析了其安全性能。仿真结果表明，EADASIC系统（含密码发生器）的执行速度高于“优秀最低速度标准”，而EADASIC系统（不含密码发生器）的执行速度超过了30Mb/s。EADASIC系统是一种高速图像密码系统。

第7章介绍了一种重要的新型图像密码系统，即融合了公钥和私钥的新型图像密码系统PKPKCIC，现有的图像密码系统大都隶属于对称密码系统，即通信双方共享相同的私钥（即私密钥），加密处理和解密处理均由私钥出发生成密码矩阵，然后进行加密和解密处理。一般地，通信双方约定的私钥将在一定时间内持续使用，这使得已知/选择明文或已知/选择密文攻击成为可能。融合公钥与私钥的新型图像密码系统中，每次加密使用不同的公钥，公钥与密文一起通过公共信道发送到接收方，公钥借助私钥生成密码矩阵，密文图像对公钥极其敏感，从而可以挫败各种被动攻击，或者说，使得各种密码分析方法的效率与穷举密钥方法相当。在详细介绍PKPKCIC系统算法的基础上，设计了其实现的MATLAB程序和C#程序，详细分析了其安全性能（包括公钥敏感性分析），证实了PKPKCIC系统是一种优秀的图像密码系统。

本书是《混沌数字图像加密》（清华大学出版社，2016）的姊妹篇。在《混沌数字图像加密》中详细阐述了分级密钥图像密码算法、明文关联图像密码算法、明文关联置乱加密算法、加密与解密共享密码算法等，且算法均基于MATLAB语言实现。本书第5章基于《混沌数字图像加密》第5.3节的图像密码算法，并基于C#语言进行了算法实现。本书第6章和第7章是全新的图像密码算法。值得一提的是，本书使用的具体的混沌系统只是代表，可以选用任何能产生优秀伪随机序列的混沌系统替代本书中算法使用的混沌系统（密码发生器算法需要做相应的调整）。此外，书中的MATLAB程序、C语言工程和C#程序都是完整的代码呈现，本书使用巧妙的方法组织各个程序，使其成为一个层层独立可运行又逐层关联叠加完整的工程。

需要强调的是：全书仿真使用的计算机配置为Intel Core i7-4720HQ四核处理器（主频为2.60GHz）、32GB DDR3L 1600MHz内存、128GB SSD固态硬盘、Windows 10（64位）操作系统，使用的软件包括Eclipse C/C++（MinGW编译器）、Visual Studio 2017（社区版）、MATLAB R2016a（版本号：9.0.0.341360，64位）、Mathematica 11、Word 2017、Visio 2017和福昕PDF阅读器等。书中的算法均由MATLAB和C#语言实现，针对DES密码算法设

计了C语言的实现代码，由于篇幅所限，书中的C#项目仅包含算法的加密与解密处理部分（算法性能分析可参考MATLAB代码）。感谢这些优秀的数学软件、程序设计软件和文档编辑软件。数学家C. Moler的*Experiments with MATLAB*和程序设计大师P. Deitel、H. Deitel父子的*Visual C# 2012 How to Program*对作者也有很大的帮助。

本著作由国家自然科学基金（编号：61762043，61562035，61702238）、江西省自然科学基金（编号：20161BAB202058）和江西省教育厅科学技术研究项目（编号：GJJ160426）资助出版，特此真挚鸣谢。

特别感谢江西财经大学罗良清教授、江西财经大学钟元生教授、南昌大学周南润教授、华东交通大学汤鹏志教授、江西财经大学党建武教授、广东海洋大学叶国栋教授、湘潭大学李澄清教授，以及我的两位授业恩师洪时中教授与陈天麒教授，对我科研工作的指导和对本书出版的大力支持。我的两位授业恩师虽已退休多年，仍然时刻关注着科技发展和学术动态，是我从事科研工作的巨大精神支柱。感谢我的爱人贾晓天老师在烦琐的资料整理上为我节约了大量时间；感谢同事廖汉程博士、胡冬萍博士、唐颖军博士和吴文华副教授等在科研工作上的共识、讨论与支持；感谢清华大学出版社赵凯编辑的细致工作。

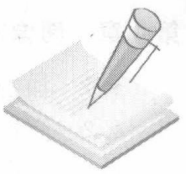
本书在回顾图像密码技术研究领域时引用了大量同行专家、学者的文献，这些参考文献均为该研究领域中颇有影响力且备受关注的研究成果，但是限于篇幅，相信仍有大量重要的文献资料被疏漏（特别是中文文献资料），敬请同行专家、学者谅解。

由于作者水平和能力有限，且该研究领域飞速发展，书中难免有不妥之处，恳请同行专家、学者和读者朋友批评指正。

张勇　于江西财经大学枫林园

2019年1月

目录



第1章

绪 论

通信研究的根本问题在于如何以近似的或准确的方式在时空的某一点再现来自另一点的信息[1]，这里的“信息”是指从通信双方已知的某个消息集合中选取的有价值或有意义的消息及其组合。例如，以汉语进行网络通信(例如借助于“微信”聊天工具)，就是从汉字集合中选取了要表达的思想内容的所需汉字组合，而在进行通信前，不能预知对方将使用哪些汉字组合。Shannon 指出，密码学和保密通信系统是通信理论的一个有趣的应用，同时，他指出真正意义上的保密通信系统在于信息加密，即通信信道是公有的和公用的，通信内容是透明的，甚至加密/解密算法也是公开的，只有密钥是私有的和受保护的[2]。本书研究的图像密码系统就是 Shannon 意义上的保密系统，可抽象地理解为从明文空间到密文空间的可逆变换，且明文空间与密文空间是相同的，均取为图像的有效像素值的集合。

1.1 图像加密的研究进展

本节按时间先后顺序，依次介绍那些为图像加密研究做出了重大贡献的专家和学者在密码学领域的杰出贡献，他们的研究成果推动了图像加密技术的发展和成熟(注：由于篇幅有限和作者能力有限，难免有些重大成果被疏漏)。

1949 年，伟大的信息论创始人 Shannon 在他的杰作中指出主要存在两种类型的加密处理，即乘积加密和加权加密[2]。假设两个加密变换分别记为 R 和 S，则乘积加密算子为 $T=RS$(系统输入赋给 S，S 的加密输出作为 R 的加密输入，R 的输出作为乘积加密的输出)，加权加密算子为 $T=pR+qS$，其中，$p+q=1$(系统输入以概率 p 赋给 R，以概率 q 赋给 S，R 或 S 的输出作为加权加密的输出)。Shannon 列举了几种常用的文本密码技术，如有趣的 Vigenère 密码和 Playfair 密码。Vigenère 密码中，密钥取长度为 d 的字符序列$\{k_i, i=0,1,2,\cdots,d-1\}$，加密长度为 n 的消息$\{m_i, i=0,1,2,\cdots,n-1\}$，密文为 $e_i=(m_i+k_{i \bmod d}) \bmod 26$，$i=0,1,2,\cdots,n-1$。当 $d=1$ 时，Vigenère 密码退化为 Caesar 密码；当 $d=n$ 时，Vigenère 密码即为 Vernam 密码(即一次一密系统)。Shannon 在密码学上的重大贡献在于他提出了扩散(Diffusion)和置乱(Confusion)的加密方法[2]。扩散方法将明文信息的统计特性分散到尽可能多的密文信息中(从而明文中的冗余信息分散到密文信息中)，例如，$y_n=\sum_{i=1}^{s} m_{n+i} \pmod{26}$，

其中，m 表示明文字母；y 表示密文字母。置乱使密钥与密文的关系尽可能复杂，即从密文信息的统计量中无法反演密钥。扩散和置乱方法使得密码系统可以有效地对抗已知/选择明文攻击和唯密文攻击。

1989 年，Matthews 提出借助混沌系统产生大量伪随机数的方法[3]，建议将混沌系统的参数和初始值用作密码系统的密钥，从而大大减小了密钥的长度，这是对一次一密系统(One-time Pad)的密钥管理的重大改进。Matthews 认为 Logistic 映射(即 $x_n=\lambda x_{n-1}(1-x_{n-1})$)的混沌区域内存在着大量周期窗口，并不适合用作密码发生器，他借助不动点分析方法设计了一种新型的混沌映射，这里称为 Matthews 映射，即 $g(x)=(\beta+1)(1+1/\beta)^{\beta}x(1-x)^{\beta}$，其中，$1\leqslant\beta\leqslant4$，$0\leqslant x\leqslant1$。然后，Matthews 使用控制参数 β 和初始值 x_0 作为密钥，迭代 Matthews 映射得到密码流。

1998 年，Baptista 提出借助混沌系统的遍历性加密字符的算法[4]，这里使用了一维 Logistic 映射，即 $x_{n+1}=bx_n(1-x_n)$，将状态空间的取值域等分为 256 个区间，每个区间对应一个字符，对应关系作为密钥。此外，控制参数 b 和初始值 x_0 也作为密钥。明文由字符组成，密文由表示迭代次数的整数组成。例如，从 x_0 开始迭代 Logistic 映射，当迭代的状态值落入第一个明文所在的小区间时，其迭代次数为第一个密文；以此时的迭代值作为新的初值，继续迭代到状态值落入第二个明文所在的小区间时，新的迭代次数为第二个密文；依此类推(参考文献[4]中，当发送方的控制参数 $\eta=0$ 时，取大于 250 且小于 65532 的最小迭代次数；当 $0.99\geqslant\eta>0$，每次迭代到目标区间的同时发送方借助高斯分布的随机数发生器产生一个随机数 κ，如果 $\kappa\geqslant\eta$，则取大于 250 且小于 65532 的迭代次数，否则继续迭代。接收方无须知道 η)。这种方法可以用于加密数字图像，只是加密后的密文图像比原始明文图像体积稍大。同年，Fridrich 指出，图像数据量巨大使得公钥密码术不适用于图像加密，因此，她提出了基于扩展的二维混沌映射的私钥(对称)图像加密算法[5]。实际上，Fridrich 的突出贡献在于首次提出了借助离散化的 Baker 映射进行图像像素点位置扰乱的算法，有些学者甚至将“置乱—扩散”结构称为 Fridrich 结构(我们更倾向称之为 Shannon 结构)。

2004 年，Chen 等提出了图像密码系统对抗差分攻击能力的两个指标[6-7]，即像素数改变率(Number of Pixels Change Rate，NPCR)和归一化像素值平均改变强度(Unified Average Changing Intensity，UACI)。这两个指标是作为明文敏感性测试指标提出来的，现在也广泛用于测试密钥敏感性和密文敏感性。

2005 年，Lian 等破译了 Fridrich 的图像密码算法[8]，Wang 等破译了 Chen 等提出的基于三维猫映射的图像密码算法[9]。自此，选择明文攻击方法成为破译各种密码方案设计有缺陷的图像密码系统的最常用方法，涌现了大量破译图像密码系统的研究工作。

2006 年，Pareek 等提出使用 80 位长的“外部”密钥，而不是直接使用混沌系统初值和参数作为密钥，进行图像加密的算法[10]；Pisarchik 等尝试借助单向耦合映像格子进行图像加密的算法[11]；Li 等展示了选择明文攻击、选择密文攻击和已知明文攻击方法的典型应用方法[12]；Gao 等在 Logistic 映射基础上提出了一种新的混沌映射，并证实了新映射可以产生随机特性更好的密码序列[13]。

2007 年，Xiang 等提出了只加密像素点高 4 位的选择图像加密算法[14]；Kwok 等提出借助 Tent 映射和高维猫映射生成伪随机序列的方法，并使用 NIST 伪随机序列测试标准详细测试了这些伪随机序列的统计特性[15]；Zeghid 等展示了 AES 可以用于图像加密[16]；

Zhang 等提出了使用猫映射和单向耦合映像格子进行图像加密的算法，该算法结构与 Feistel 结构类似[17]。

2008 年，Massoudi 等综述了图像加密系统的选择加密算法，从 Shannon 密码理论中找到了理论依据[18]；Arroyo 等分析了 Pisarchik 等[11]的图像密码系统的安全性问题[19]，提出了一种所谓的时间攻击方法；Gao 等提出了一种借助混沌序列置乱图像像素点的方法[20]；Behnia 等提出了借助混沌耦合映射和单混沌映射产生密码序列的算法[21]；Tong 等进一步提出了借助复合混沌映射产生密码序列的算法[22]；Wong 等提出了使用循环移位操作的扩散算法，循环移位在几乎不增加运算量的前提下，提高了扩散性能[23]。

2009 年，Wong 等提出了借助查找表实现扩散的算法[24]；Wang 等提出了借助 Logistic 映射的状态更新标准映射(Standard Map)、Arnold 猫映射和推广的 Baker 映射控制参数的方法[25]；Mazloom 等提出了一种借助耦合非线性混沌映射产生密码序列的方法[26]；Gangadhar 等提出了一种基于超混沌的图像密码算法，并详细分析了其对抗唯密文攻击和已知/选择明文攻击的性能[27]；Tong 等提出了一种明文关联的反馈型密码发生器，并对密文作了 NIST SP800-22 伪随机性测试[28]；Wang 等提出了组合 4 个一维混沌映射产生密码序列的方法[29]。

1998—2009 年，图像密码系统研究的主要工作有 3 个方面：①研究新的混沌系统，评估其产生伪随机序列的统计特性及其在图像加密方面的应用；②研究已有的混沌系统的组合及其变种系统，评估其产生的伪随机序列的统计特性及其在图像加密方面的应用；③研究图像加密的新的置乱算法和/或扩散算法，提高图像密码系统对抗已知/选择明文攻击等被动攻击的能力。事实上，这一时期的大量研究工作偏重于前两方面的研究，而或多或少地忽视图像密码系统算法与结构设计方面的研究，导致这些研究成果被后来的学者们使用已知/选择明文攻击等方法逐一破译，就连早期 Fridrich 的工作也难于幸免。但是，在这种图像加密与图像破译的争鸣中，图像密码系统的研究工作持续高速发展。

2010 年，Wang 等提出了结合神经元模型的图像加密算法[30]；Tong 等研究了一种新型组合混沌系统，并证实了该混沌系统的最大 Lyapunov 指数比 Logistic 的最大 Lyanpunov 指数大[31]；Ye 提出了一种位位置扰乱的图像加密算法[32]；Liao 等提出了借助正弦波形离散值变换像素点灰度值的方法[33]；Yang 等提出了图像加密和明文图像认证的算法，但是在密钥分配方面存在缺陷[34]；Ye 提出了借助 Toeplitz 和 Hankel 矩阵进行像素位置置乱的算法[35]；Wang 等提出了借助 DNA 编码变换进行图像加密的算法[36]。

2011 年，Zhang 等借助 Tent 映射实现了图像像素点的全置乱处理[37]；Jolfaei 等提出了基于简化的 AES 的图像密码算法[38]；Ye 提出了借助混沌小波函数进行图像加密的算法[39]；Patidar 等提出借助图像整行和整列操作加快处理速度的方法[40]；Ye 提出了融合异或运算和加模 256 运算的扩散算法[41]；Fu 等提出了借助 Arnold 映射进行图像位位置置乱的方法[42]；Rao 等提出了使用 Brahmagupta-Bhāskara 方程和 Logsitc 映射的图像加密算法，其同时使用了同或运算和异或运算[43]；Zhu 等提出了一种新的借助猫映射进行位位置扰乱的算法[44]。

2012 年，Zhu 等提出了明文关联的密码序列生成方法[45]，并改进了 Tent 映射，使其状态空间由(0,1)缩小为$(q,1-q)$，q 为小的正小数。例如，$q=0.1$；Akhshani 等引入了量子 Logistic 映射进行图像加密[46]；Kanso 等提出了基于三维猫映射进行彩色图像加密的算

法[47]；Wang 等提出了魔方置乱和动态查找表方法扩散的图像加密算法[48]；El-Latif 等提出了基于多项式混沌的图像像素位位置扰乱的算法[49]；Abdullah 等引入基因交叉算法进行图像加密[50]；Fu 等使用 Chirikov 标准映射和 Chebyshev 映射进行图像置乱和扩散，扩散中同时使用了异或运算以及求和取模运算[51]；Ye 等提出基于离散 Arnold 映射和行列循环偏移的图像加密算法[52]；Mirzaei 等提出将图像分成 4 幅子图像进行并行加密的算法[53]。

2013 年，Song 等构造了一种耦合映射格子并用于图像加密[54]；Zhang 等结合超混沌和 DNA 编码序列进行图像加密[55]；Zhou 等组合 Logistic 映射、Sine 映射和 Tent 映射成为一个参数可控系统作为密码发生器[56]；El-Latif 等借助量子混沌系统产生密码序列，并使用了提升小波变换进行变换域置乱[57]；Yang 等进行了量子 Fourier 变换下的图像加密预研工作[58]；Ping 等提出了使用二维元胞自动机的图像加密算法[59]；Behnia 等借助 Jacobian 椭圆混沌映射生成密码序列[60]；Zhang 等提出了一种明文关联的扩散算法[61]；Tong 分析了 $f(x)=0.5-4x^2$ 的混沌特性并用其产生密码序列[62]；Zhou 等设计了基于量子交换电路的量子图像扰乱算法[63]；Nandeesh 等提供了多种扫描方式下的位位置扰乱技术[64]。

2014 年，Fouda 等提出了基于分段线性混沌映射(PWLCM)和线性 Diophantine 方程(LDE)的图像加密算法，使用了 256 位长的外部密钥[65]；Zhang 等提出了基于位立方体旋转的置乱算法[66]；Wang 等提出基于 Brownian 运动的置乱算法[67]；Zhang 等提出基于时空混沌的图像加密算法[68]；Zhang 等[69]提出 Zhang 等[55]的图像密码方案的选择明文攻击方法；Zhou 提出了组合两种一维混沌映射得到新的混沌系统的方法，并将其用于图像加密[70]；Norouzi 等提出了基于 salsa20 Hash 函数的图像加密算法，使用了 512 位长的外部密钥[71]；Ye 提出了基于正弦波和混沌系统的图像加密算法[72]；Wang 等提出了基于动态 S 盒的图像加密算法[73]；Yang 等提出了基于混沌 Josephus 矩阵的图像置乱算法[74]；Hussain 借助 Tent 映射、时空混沌和 S 盒实现了图像加密处理[75]；Wu 等模拟水波纹实现了图像置乱与扩散算法[76]。

2015 年，Cheng 等提出了置乱与扩散同时进行的图像密码算法[77]；Hua 等提出了基于随机选择量子门电路的量子图像加密算法[78]；Wang 等提出了基于 Langton's Ant 元胞自动机的图像加密算法[79]；Zhou 等实现了 Arnold 映射的量子版本并用其进行图像加密变换[80]；Wang 等提出了基于行互换和列互换的图像加密算法[81]；Som 等提出了使用 4 个一维混沌映射(Logistic 映射、Tent 映射、正弦映射和立方映射)进行图像扩散的算法[82]；Murillo-Escobar 等提出了借助优化的一维 Logistic 状态序列进行图像加密的算法[83]；Hua 等提出了借助二维 Logistic 调制映射进行图像加密的算法[84]；Liu 等提出了借助 Hénon 映射产生密码序列的方法[85]；Khan 等提出了一种新型的 S 盒，并使用了 Tinkerbell 映射产生密码序列[86]；Tong 等提出了借助带扰动的混沌映射生成密码序列的方法[87]；Zhao 等进行了公钥与私钥融合加密光学图像的尝试[88]；Seyedzadeh 等提出了基于二维 Logistic 映射和量子 Logistic 映射进行图像加密的算法，其中，同时应用了异或运算以及求和取模 256 运算[89]；Chen 等使用了动态更新混沌状态序列作为密码序列的方法进行图像加密处理[90]。

2016 年，Hua 等提出了组合 Logistic 映射和正弦映射的新混沌映射，并用其产生密码序列[91]；Zhang 等提出了基于二维 Logistic 映射和可更新 S 盒的图像加密算法[92]；Assad

等提出了基于二维猫映射的图像像素位置乱算法[93]；Zhang 等提出了基于动态 DNA 编码算法的图像加密方法[94]；Murugan 等研究了基于 Henon 映射的置乱方法和基于 Lorenz 系统的扩散方法[95]；Diaconu 使用了一种新型的双变元混沌系统进行图像加密[96]；Guesmi 等提出了借助 SHA2 和 DNA 序列的图像加密算法，其中使用了 Lorenz 系统生成密码序列[97]；Parvin 等提出了一种密文有损情况下成功还原原始图像的图像密码算法[98]；Wu 等提出了一种基于二维离散小波变换和六维超混沌系统的图像加密算法[99]；Rostami 等提出了一种基于 DNA 序列和 Logistic 映射的图像加密算法[100]；Zhu 等提出了两个二维组合混沌系统，并将其用于产生密码序列[101]；Devaraj 等提出了基于变型标准映射和动态 S 盒进行图像加密的算法[102]；Li 等提出了基于混合元胞自动机的图像加密算法[103]；Liang 等提出了仿射变换的量子实现版本，并将其用于量子图像加密[104]；Yang 等提出了基于一维量子元胞自动机的量子图像加密算法[105]；Liu 等提出了基于 DNA 编码 S 盒的图像加密算法[106]；Ye 等提出了基于 SHA3 的块图像加密算法[107]。

2017 年，Chai 等提出了基于 DNA 序列和正弦波动的图像加密算法[108]；Çavuşoğlu 等提出了一种新的混沌系统，并用其构造了 S 盒[109]；Hu 等提出了基于 DNA 计算的图像加密算法[110]；Pak 等组合一维 Logistic 映射、正弦映射、Chebyshev 映射的新型混沌系统，并将其用于图像加密[111]；Chai 等提出了基于 Chua 混沌系统、元胞自动机和 DNA 编码的图像加密系统[112]；Wang 等提出了基于分段线性混沌映射(PWLCM)和 DNA 编码的图像加密系统[113]；Li 等提出了基于 Tent 映射的图像加密系统[114]；Li 等提出了一种量子彩色图像加密算法[115]；Zhu 等提出了一种二维组合超混沌系统及其图像加密应用方法[116]；Chai 等提出了加密过程中的动态等价密钥选择算法[117]；Chai 提出了基于 SHA2 和组合混沌系统的图像加密算法[118]；Hu 等提出了基于 Lorenz 系统、Chen 超混沌系统和 DNA 序列的图像加密算法[119]；Belzai 等提出了基于 S 盒和多个混沌系统的图像加密系统[120]。

2010 年至今，仍有大量图像密码系统方面的研究工作聚焦于混沌密码发生器的研究，可见密码序列在图像密码系统中的重要地位，现有的研究思路集中在发掘新型混沌系统上，这方面的未来研究工作可能需要深入考虑计算机的有限字长效应；一些学者在研究 S 盒构造方法及其非线性特性，这是一个重要的研究方向，S 盒和查找表是实时的图像密码系统必不可少的组成构件，这方面的工作可能需要基于有限域进行深入研究；一些学者提出了基于 DNA 序列的图像密码系统，这些工作正如 Rostami 等学者[100]指出的，实质上是一种模 4 的二进制序列运算，这方面的大量研究工作被证实是不安全的，可能需要结合未来 DNA 计算机的数据结构和遗传算法进行深入有效的研究；一些学者开始探索基于量子图像的量子加密算法，由于量子计算机仍处于萌芽阶段，所以这部分工作最近几年内都将属于预研性质的研究工作，可能需要投入更多的研究人员和研究资源；图像加密与解密系统结构方面的研究工作也取得了一定的进展，学者们普遍重视明文关联的等价密钥生成算法和明文关联的加密系统的设计，这方面的研究工作属于图像密码学的核心工作，如果致力于设计类似 AES 这类数据加密标准算法的图像加密标准算法，形成全球统一的图像加密标准，可能需要在图像加密系统结构与算法上进行深入的研究。显然，任何一个科学领域的研究工作都应该是有始无终的，即使未来产生了图像加密标准，图像加密研究工作也只是有了一个参照标准，相应的研究工作也会持续发展下去。

下面谈一下我们科研小组在图像密码学领域的粗浅认识和研究工作[121-139]。首先，在

图像密码系统的系统结构研究方面，研究了基于“扩散—置乱—扩散”结构的图像密码系统，其中，两个扩散操作都是明文无关的，而置乱操作是明文关联的，以提高图像密码系统的处理速度，在最新的研究成果中，还研究了基于“遮盖—扩散—扩散—置乱”型的图像密码系统和欺骗性图像密码系统及其与遮盖性图像密码系统的关系。其次，在图像密码算法研究方面，研究了明文关联的置乱算法，研究了加密算法与解密算法相同的图像密码算法并给出了严格的证明，最新的一项研究工作实现了基于卷积运算的扩散算法。然后，在图像密码系统算法实现研究方面，研究了基于 MATLAB 语言、C 语言和 C＃语言进行图像密码系统实现的方法，形成了以 MATLAB 语言快速图像密码系统实现和统计特性分析以及敏感性分析、以 C 语言和 C＃语言进行加密效率与安全评价的体系方法，设计了 C 语言进行图像加密算法设计的框架工程，并开发了基于 C＃语言进行图像加密的工程项目。最后，在图像密码系统性能评价方面，研究了计算 NPCR 和 UACI 的理论值的统计方法和算法程序，不但计算出了两幅随机图像间的 NPCR 和 UACI 值，而且可以计算任意图像与随机图像间的 NPCR 和 UACI 值，从而使得密文敏感性分析和解密系统的密钥敏感性分析成为可能。此外，还研究了块平均变化强度(Blocked Average Changing Intensity，BACI)指标，理论上 BACI 指标比 NPCR 和 UACI 指标更具有说明性，同时，理论上给出了计算 BACI 的统计方法。

在未来的研究工作中，我们科研小组将继续使用 MATLAB 和 C＃语言作为研究工具，在图像密码系统的新型系统结构设计、新型密码发生器、新型加密算法设计、新型性能评价指标和图像加密应用技术等方面开展深入的研究，培养优秀的信息安全专业研究生，用更安全、更快速的图像密码系统服务于大众通信和国家安全。

1.2 准备工作

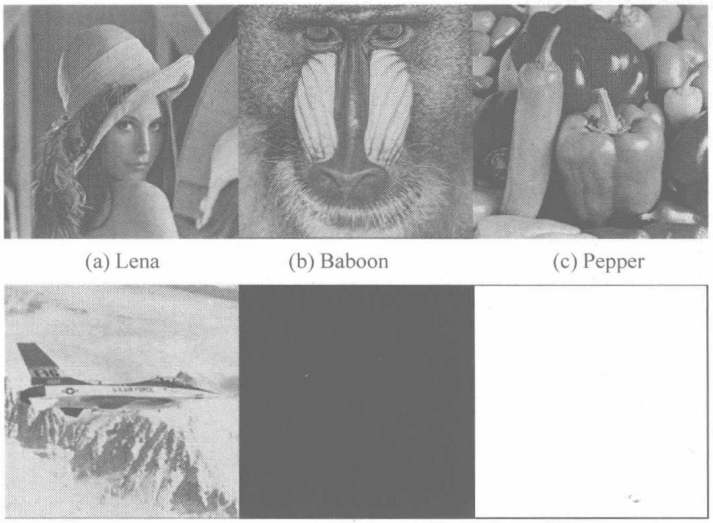
全书仿真使用的计算机配置为 Intel Core i7-4720HQ 四核处理器(主频为 2.60GHz)、32GB DDR3L 1600MHz 内存、128GB SSD 固态硬盘(＋1TB 机械硬盘)、Windows 10(64 位)操作系统，使用的软件包括 Eclipse C/C++(MinGW 编译器)、Visual Studio 2017(社区版)、MATLAB R2016a(版本号：9.0.0.341360，64 位)、Mathematica 11、Word 2017、Visio 2017 和福昕 PDF 阅读器等。由于篇幅限制，书中给出的算法程序主要是 MATLAB 代码和 C＃代码以及部分 C 代码。

1.2.1 常用的灰度图像

书中使用的图像来自 USC-SIPI 图像库(http://sipi.usc.edu/database/)。不失一般性，仿真实验仅使用了 USC-SIPI 中的 4 个灰度图像，即 Lena、Baboon、Pepper 和 Plane，以及全黑图像和全白图像，这些图像的大小均为 256×256 像素，如图 1-1 所示。

1.2.2 MATLAB R2016a 数学软件

仿真使用了 MATLAB R2016a 数学软件(在实际应用中，发现版本 R2016a 比 R2015a 和 R2017a 的运算速度都快一些)，版本号为 9.0.0.341360。除了 Simulink 和 GUI 工作方式外，MATLAB 主要有命令行方式和程序代码方式。本书主要使用程序代码工作方式，即编写.m 文件形式的函数和程序代码。

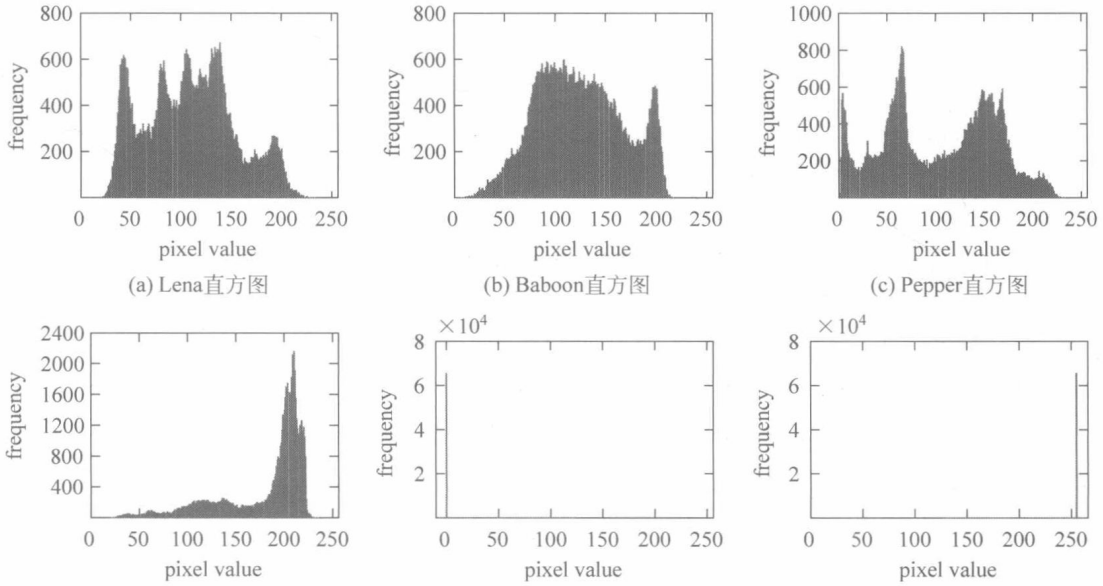


(a) Lena (b) Baboon (c) Pepper

(d) Plane (e) 全黑图像 (f) 全白图像(不含边框)

图 1-1 仿真实验使用的图像

下述程序绘制了图 1-1(a)～(d)所示的图像直方图，如图 1-2(a)～(d)所示。图 1-2(e)、(f)分别为全黑图像直方图和全白图像直方图。



(a) Lena直方图 (b) Baboon直方图 (c) Pepper直方图

(d) Plane直方图 (e) 全黑图像直方图 (f) 全白图像直方图

图 1-2 图 1-1 中各图像的直方图

【程序 1-1】 绘制图像直方图函数 myDrawHistogram. m。

```
function y = myDrawHistogram(x)
x = double(x); p = x(:);
 % %
y = hist(p,256); hist(p,256);
pm = myMax(y);
```

```
    k = ceil((pm + 50)/200);
    tk = 200;
    if k > 10
        tk = 400; k = ceil(k/2) * 2;
    end
    % %
    xlabel('pixel value'); ylabel('frequency');
    axis([0 256 0 k * 200]);
    set(gca,'xtick',0:50:256,'ytick',0:tk:k * 200);
    set(gca,'fontsize',12,'fontname','times new roman','tickdir','out');
    set(gcf,'position',[400 100 300 220],'color','w');
    % %
        function mm = myMax(v)
            mm = max(v);
        end
    end
```

【程序 1-2】 绘制图像直方图程序 pc001.m。

```
    % pc001.m
    clear; clc; close all;
    % %
    P1 = imread('Lena.tif');
    P2 = imread('Baboon.tif');
    P3 = imread('Pepper.tif');
    P4 = imread('Plane.tif');
    % %
    figure(1); myDrawHistogram(P1);
    figure(2); myDrawHistogram(P2);
    figure(3); myDrawHistogram(P3);
    figure(4); myDrawHistogram(P4);
```

程序 1-1 为自定义的 MATLAB 函数 myDrawHistogram，函数以 function 关键字开头（第 1 行），函数名作为文件名，输入和输出参数均为矩阵或向量，以 end 关键字结尾（第 21 行）。第 2 行将输入图像 x 转化为 double 类型数据，然后按列排列成一个列向量 p；第 4 行将图像的直方图保存在 y 中，并绘制直方图；第 12～16 行设置直方图的坐标和样式；第 18～20 行为函数 myDrawHistogram 可调用的内部函数。“%%”表示该行为分隔线，“%”表示该行为注释。

程序 1-2 中，第 2 行的 clear 表示清除工作区的变量，clc 表示清除命令窗口显示的命令，close all 表示关闭图形输出窗口；第 4～7 行依次读入 Lena、Baboon、Pepper 和 Plane 图像；第 9～12 行依次调用 myDrawHistogram 函数绘制 Lena、Baboon、Pepper 和 Plane 的直方图，figure(1)表示创建标号为 1 的图形输出窗口。

由图 1-2 可知，这些图像的直方图具有明显的波动特征。一般地，由图像的直方图还原出原始图像是非常困难的，而当图像具有平坦的直方图时，还原操作几乎是不可能的。

1.2.3 Eclipse C 集成开发环境

Eclipse C/C++集成开发环境是目前 C/C++程序设计的最佳开发平台，可以免费从官方网址（https://www.eclipse.org/）上下载安装包，接着，还要从网址（http://www.mingw.org/）

上下载 MinGW 编译连接器安装包。然后，先安装 Eclipse C/C++集成开发环境，再安装 MinGW 编译连接器。下面给出本书使用的 C 工程框架，后续算法只在该 C 工程框架基础上修改 algr. c、algr. h 和 main. c 文件即可。

启动 Eclipse C/C++集成开发环境，选择菜单命令 File|New|C Project，在弹出的对话框中输入工程名 myCPFrame，选择 MinGW GCC 作为 Toolchains，如图 1-3 所示。在图 1-3 中单击 Finish 按钮进入 Eclipse 工作窗口。

图 1-3 Eclipse 新建工程对话框

在 Eclipse 工作窗口中，通过菜单命令 File|New|Source File 和菜单命令 File|New|Header File 可分别创建源代码文件和头文件。myCPFrame 工程包含的文件见表 1-1。

表 1-1 myCPFrame 工程包含的文件

序号	文件名	作 用
1	main. c	主程序文件，实现图像的加密与解密
2	includes. h	总的头文件
3	imReadWrite. c	图像数据读写程序文件，实现从硬盘图像数据文件中读取图像数据至内存数组，或将内存数组写入硬盘图像数据文件
4	imReadWrite. h	图像数据读写头文件
5	algr. c	算法程序文件，实现图像的加密与解密算法
6	algr. h	算法头文件
7	zlxdatatype. h	自定义数据类型头文件
8	glena256x256. dat	Lena 图像数据文件，其数据为 256×256 矩阵，元素间由一个空格间隔，行间由一个回车符分隔
9	MyCipher. txt	密文图像数据文件(程序运行输出结果)
10	MyRecover. txt	解密的图像数据文件(程序运行输出结果)