# 图像加密算法与实践
## ——基于C#语言实现

Image Encryption Algorithms and Practices with Implementations in C#

孙燮华（Sun Xiehua） 著

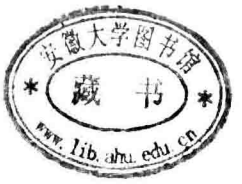
科学出版社

# 图像加密算法与实践

## ——基于 C#语言实现

# Image Encryption Algorithms and Practices with Implementations in C#

孙燮华 (Sun Xiehua) 著




科学出版社

# 前　言

随着 Internet 的兴起，图像、视频等多媒体信息需要在网络上传输，于是产生了图像信息安全问题. 图像加密是首要解决方案，其既可作为图像水印的预处理，又是相对独立的信息安全分支. 目前在国内外的各类研究期刊上，图像加密被广泛关注，是信息安全领域的研究热点之一.

图像加密既属于数字图像处理的范畴，也属于图像通信学科，同时又属于信息安全领域，是密码学的新领域. 它与计算机密码学的许多算法与技术相关，同时又发展了图像加密特有的方案与算法. 其方案与算法除涉及计算机密码学和数字图像处理的理论与算法外，还涉及混沌与分形、编码理论、数据压缩、智能算法、小波与傅里叶分析、神经网络、计算方法与近代数学等许多学科和领域，是一个跨学科、多领域的交叉学科. 因此，全面掌握图像加密理论需要较多的知识与技能.

同时，图像加密既然属于信息安全领域，那么它就不是一个次要的领域. 因为在信息安全领域中，每一个问题都是极其重要的，每一分支领域都是极为重要的领域. 其重要性甚至关系到国家和人民的安全.

关于计算机密码学，国内有卢开澄教授所著的《计算机密码学》，国外有 Schneier 所著的《应用密码学——协议、算法与 C 源程序》. 然而，这些专著尚未涉及图像加密. 鉴于此，我一直计划写一本这方面的专著，以总结自己在中国计量学院指导几届图像加密方向研究生的工作.

本书选择国内外属于SCI收录或在一流期刊发表的典型论文作为讨论材料是很自然的. 因为一般来说，作学术研究需要读论文，尤其需要学习国内外权威期刊最新的和典型的论文，吸收和学习前人和同行的新思想和新方法，这个过程就是所谓的“站在巨人的肩膀上”，以充实自己的研究，获得创新成果，到达新的高度.

那么，将本书写到怎样的深度呢？介绍、分类和分析论文成果是常用的处理方法. 若进一步，选择部分论文实现则为少数著者采用. 若更进一步，将所有论文完全实现则是一件比较困难但很有意义的工作.

常听一些研究生说：“我读懂了论文，但做不出什么结果. ”一篇论文读到什么程度才可以说“读懂”了呢？各人有不同的评判标准. 我认为，至少对于信息学科来说，当能将一篇论文提出的算法或方案等，设计实验并实现论文中的结果

时，可以说已基本读懂了这篇论文. 当实现不了这篇论文的结果时，若能证明论文的算法或方案存在疏忽或错误，更进一步能纠正这些错误，进而实现该论文的结果，或者能证明该论文的这些错误是不可改正的，因而得出“该论文结果实现不了”的结论时，那么就可以说已完全读懂了这篇论文. 总之，要对一篇论文的结果给出明确的回答，能实现、在什么条件下能实现或不能实现；并对论文建立的引理、定理等审查，得出它及其证明是“正确的”或“不正确”的结论. 达到这种程度时，才可以说，基本读懂或是完全读懂了该论文.

本着这个精神，本书介绍、分析并用完整的 C#程序实现了 26 篇论文方案. 对论文中的算法论证作了更为详细的校对. 对有的还进行了修正和补充，直至证明其为错误的并完成相应的修改. 对论文的算法和方案进行编程实现并不容易，有时更是研究的关键障碍之一. 本书将编程代码公开，其目的是与读者交流，抛砖引玉.

由于著者学术水平有限，书中及程序中难免出现错误和疏忽，欢迎读者批评指正. 同时，对本书中被引用论文的作者表示感谢，若在分析和评论中出现不当之处，敬请谅解.

孙燮华

2013 年 2 月于杭州

# 目　录

# 第Ⅰ部分　准备

# 第 1 章　图像加密概论

近年来，随着 Internet 的快速发展，大量公开的和私有的图形和图像等多媒体信息被通过网络传输. 如何安全地传送这些信息成为一个迫切需要解决的问题. 图像加密是其首要的解决方法. 图像加密属于计算机密码学的一个新分支，也属于信息隐藏范畴，又是相对独立的信息安全分支. 本章将简要介绍图像加密发展过程和图像加密的分类及原理等内容.

## 1.1　图像加密的发展和特点

### 1.1.1　图像加密的发展

下面简要介绍图像加密发展中一些引人注目的进展.

1. 基于随机数发生器的图像加密方法(1991)

1991 年，Schwartz [1]提出了用置乱方法(scrambling method)加密图像. 首先在原图像上生成随机点序列. 然后，在序列的每两个相邻点之间画出一些线条. 进而，以相反的模式画图，即将白色改变为黑色，而将黑色改变为白色. 在原图上画了许多相反的线条后，原图就被加密了. 值得注意的是，这些随机点是由随机数发生器的种子确定的，这个种子就是加密方法的密钥. 这种方法简单且快速，但安全性不高，不足以保护图像.

2. 基于 SCAN 语言的图像加密方法(1992)

1992 年，Bourbakis 和 Alexopoulos[2]提出了另一种图像加密方法. 该方法先将二维图像转变为一维序列，使用 SCAN 语言描述这个转变结果，在这种语言中，存在几种 SCAN 字母，每一种字母表示一类扫描次序，SCAN 字母组合的不同类型可以生成各种不同类型的加密图像. 在确定了 SCAN 字母组合后，就产生一个 SCAN 串，这个串确定了对原始图像进行扫描的次序. 然后，按照这种加密方法以确定的次序对原图进行扫描，进而，用这个 SCAN 串对图像进行加密. 因为非法用户不能得到正确的 SCAN 串，所以原图是安全的. 这种方法中没有压缩图像，所以还不是高效的直接加密方法.

3. 使用图像扭曲的加密方法(1993)

1993 年，Kou[3]提出了一种基于图像扭曲(image distortion)的加密方法. 这种方法将一幅密钥图像的相位频谱(phase spectra)加入到原图的相位频谱，得到加密图像. 因为加密图像的相位频谱是随机变化的，所以加密图像是不可辨认的，于是这种方法是安全的.

4. 基于四叉树结构和 SCAN 语言的图像压缩和加密方法(1994)

1994 年，Chang 和 Liou [4]提出了一种图像加密方法，这种方法使用了两项技术达到压缩和加密目的，分别是四叉树结构和 SCAN 语言. 因此，这种方法可以同时压缩和加密图像. 值得注意的是，四叉树是无损数据压缩技术，因此这种加密方法也是无损的，但是它不足以抵抗某些非法攻击，例如，**交错迷惑攻击**(jigsaw puzzle attack)和**邻居攻击**(neighbor attack).

5. 视频图像选择加密方法(1995)

图像经过时频变换后，在频域易于确定关键部分，这种性质在图像压缩上早就得到应用. 1995年，Spanos和Maples [5]仅对MPEG码流的I帧进行加密，提出了选择加密或部分加密图像新算法.

6. 图像分解用于压缩与加密(1996)

1996年，Chen和Li[6]开发了对JPEG图像的部分加密技术，提出了对离散余弦变换(discrete consine transform，DCT)8×8块的部分系数进行加密，这是频域的部分加密技术. 而在空域，Chen和Li[7]提出了用四叉树结构压缩图像的方法，随后仅加密四叉树结构，而其余部分不再加密.

7. 混沌图像加密方法(1997—1998)

Fridrich [8]应用一些可逆混沌映射创建了新的对称分组加密方法. 这种方法本质上适用于大数据量的加密，例如，数字图像的加密. 1998年，Fridrich [9]再次提出用可逆二维混沌映射加密图像，并提出了将混沌映射离散为整数点的一般化方法. 以Baker映射为例，提出了具体的置乱加密方案.

8. 镜像加密方法(1999)

Yen 和 Guo[10]提出了具有镜像(mirror like)的加密算法，其算法分为 7 个步骤，前 3 步生成二值混沌序列，后 4 步将按这个混沌序列用交换函数对图像像素进行

重排，这种方法具有较低的复杂度和较高的安全性且不失真.

9. DNA 及其在图像加密中的应用(2000)

1994 年，Adleman[11]首次提出了 DNA 计算，开创了信息处理的新阶段. 1999 年，Celland 等[12]提出了一种新型的编码方法，将生物化学的核苷酸用做四进制码，而每一个字母用 3 个核苷酸表示. 例如，用 CGA 表示字母 A，用 CCA 表示字母 B. 随后，秘密信息就被编成 DNA 序列. 例如，AB 可用 DNA 串 CGACCA 表示. 在 2000 年，Gehani 等[13]提出了用 DNA 串进行一次一密方法加密图像.

10. 基于混沌序列图像的加密方法(2000)

2000 年，Yi 等[14]给出了一个基于混沌序列的图像加密方法. 首先，用密钥生成实值混沌序列.然后，将它分散到符号矩阵和变换矩阵. 最后，在 DCT 域使用这两个矩阵加密图像. DCT 是有损的数据压缩技术，图像可能出现一些由有损数据压缩和噪声引起的失真. 但是，这种方法仍然可以正确地解密和恢复原图，并达到很高的安全等级.

11. 基于向量量化和密码学及数论的加密方法(2001)

2001 年，Chang 等[15]提出了一种基于向量量化(vector quantization，VQ)和密码学及数论的快速图像加密算法. 在VQ 中，先将图像分解为向量，并按顺序将向量逐个进行编码. 然后，为了提高安全性和减小加/解密的计算复杂性，可采用传统的商业加密系统和一些数论定理. VQ对于低位率图像压缩是一种有效的方法，加快了加密过程并达到很高的安全性.

12. 基于位平面的选择加密方法(2002)

2002 年，Droogenbroeck 和 Benedett [16]对未经压缩的图像和压缩图像(JPEG)提出了选择加密方法. 按照他们的方法，至少在未经压缩的图像 8 个位平面中的 4 或 5 个最小意义的位平面上进行加密，能使图像达到满意的加密效果. 同年，Podesser 等[17]提出了对未经压缩的图像进行选择加密. 该方法与 Droogenbroeck 和 Benedett [16]提出的算法是相反的. Podesser 等的方法仅加密最有意义的位平面，而文献[16]的方法仅加密最小意义的位平面.

13. 应用数字签名和纠错码的图像加密方法(2003)

2003 年，Sinha 和 Singh[18]提出了一项新技术，将原图的数字签名加入到原图的加密图像中. 而图像编码使用了能适当控制错误的纠错码，如 BCH 码. 在接收

端，当图像被解密后，其数字签名可验证图像的认证.

14. 多层图像加密方法(2003)

2003年，Shin等[19]应用二进制相位异或运算和图像分块技术，提出了多层图像加密方案. 多层图像可以分成具有相同灰度层次的二进制图像，并对每一层进行加密操作.

15. 应用T矩阵的图像加密方法(2004)

2004年，Zhang等[20]应用T矩阵对图像进行置乱加密. T矩阵具有简单的保形性，其周期是Arnold矩阵的2倍. 它可用于图像加密和图像水印算法的预处理.

16. 基于混沌神经系统的加密方法(2005)

2005年，Deng等[21]用一个混沌神经系统和Arnold映射完成了图像加密. 这种方法使用了神经网络制造混沌的新技术.

17. 基于模糊逻辑的伪随机比特发生器(2005)

2005年，El-Khamy等[22]利用模糊逻辑设计了新伪随机数发生器，并用于图像加密，它开启了模糊数学在图像加密中的应用.

18. 基于细胞自动机的图像加密方法(2005)

1983年，Wolfram[23]奠定了**细胞自动机**(cellular automata，CA)理论，Nandi等[24]给出CA理论在密码学上的应用. 而在2000年，Panagiotis[25]用细胞自动机进行图像处理，直到2005年，Chen等[26-27]提出用细胞自动机进行图像加密的方案. 随后，大量基于各类细胞自动机的图像加密方法相继被提出.

19. 部分加密用于人脸检测方法(2006)

2006年，Hong和Jung[28]提出了将部分加密应用于作为特征的人脸区域，这是因为人脸是图像或视频最重要的部分. 他们的工作和Rodrigues等[29]的工作丰富了图像加密的应用.

20. 基于独立成分分析的加密方法(2007—2008)

**独立成分分析**(independent component analysis, ICA)产生于源信号的盲分离问题中，该问题仅用 $q$ 个观察到的混合信号来恢复 $p$ 个未知混合信号(源信号)，而这些源信号假定彼此统计独立. Alfalou等[30]和Ito等[31]将ICA引入到图像加密和