

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

前言

第 I 部分 准备

第 1 章 图像加密概论	3
1.1 图像加密的发展和特点	3
1.1.1 图像加密的发展	3
1.1.2 图像加密的特点	8
1.2 图像加密的分类	9
1.2.1 图像加密分类(一)	9
1.2.2 图像加密分类(二)	12
1.3 图像加密分析	12
1.3.1 攻击类型	12
1.3.2 Kerchoffs 原理	13
1.4 图像加密原理	13
1.4.1 图像置乱加密原理	13
1.4.2 图像序列加密原理	14
1.5 本书内容安排	14
1.5.1 关于编程与运行环境	15
1.5.2 关于本书程序的结构与组成	15
参考文献	16
第 2 章 算法基础	21
2.1 Arnold 变换	21
2.1.1 二维 Arnold 变换	21
2.1.2 广义 Arnold 变换	26
2.1.3 三维 Arnold 变换	27
2.1.4 n 维 Arnold 变换	28
2.2 模运算	29

2.2.1	模运算的性质	29
2.2.2	模算术运算	30
2.2.3	模算术的性质	30
2.3	混沌变换	31
2.3.1	Logistic 映射	32
2.3.2	Chebyshev 映射	34
2.3.3	Baker 映射	34
2.3.4	Henon 映射	36
2.3.5	Lorenz 映射	36
2.3.6	Chen 超混沌系统	36
2.4	图像像素的重排	37
2.4.1	n 维图像的一维序列表示	38
2.4.2	n 维图像与 k 维图像之间的转换	40
2.5	图像时频变换	40
2.5.1	DCT 变换	40
2.5.2	提升 Haar 小波变换	41
	参考文献	46

第 II 部分 空域图像加密

第 3 章	置乱加密	51
3.1	RGB 平移置乱加密	51
3.1.1	加密思想	52
3.1.2	加密算法	52
3.1.3	算法实现与实践	54
3.1.4	相关研究	59
3.2	Henon 混沌置乱加密	59
3.2.1	加密思想	59
3.2.2	加密算法	60
3.2.3	算法实现与实践	62
3.2.4	相关研究	64
3.3	SCAN 模式加密	64

3.3.1	SCAN 模式	64
3.3.2	SCAN 加密方案	67
3.3.3	算法实现与实践	70
3.3.4	相关研究	74
3.4	二值图像修正 SCAN 加密	75
3.4.1	二值图像四叉树表示与修正 SCAN 语言	76
3.4.2	加密方案	80
3.4.3	算法实现与实践	82
	参考文献	87
第 4 章	灰度加密	89
4.1	灰度 DES 加密	89
4.1.1	DES 算法	89
4.1.2	算法实现与实践	92
4.1.3	相关研究	94
4.2	Hill 矩阵加密	94
4.2.1	Hill 加密算法	94
4.2.2	自可逆矩阵	100
4.2.3	自可逆矩阵 Hill 加密方案	103
4.2.4	算法实现与实践	104
4.2.5	相关研究	106
4.3	混沌序列加密	106
4.3.1	混沌映射序列加密方案	107
4.3.2	算法实现与实践	109
4.3.3	相关研究	116
4.4	细胞自动机方法	117
4.4.1	细胞自动机简介	117
4.4.2	基本细胞自动机	119
4.4.3	图像加密算法	121
4.4.4	算法实现与实践	121
4.4.5	相关研究	123
4.5	随机格加密	123

4.5.1	随机格	124
4.5.2	二值图像随机格加密	125
4.5.3	灰度图像随机格加密算法	129
4.5.4	算法实现与实践	130
4.5.5	相关研究	134
4.6	基于遗传算法和混沌的图像加密	134
4.6.1	遗传算法的基本概念和思想	134
4.6.2	加密方案	136
4.6.3	算法实现与实践	139
4.6.4	相关研究	145
	参考文献	145
第 5 章	混合加密	148
5.1	Arnold-Chen 混沌序列加密	148
5.1.1	Arnold 映射和 Chen 混沌系统	148
5.1.2	Arnold-Chen 混沌序列加密方案	149
5.1.3	算法实现与实践	149
5.1.4	相关研究	151
5.2	复合混沌加密	152
5.2.1	复合混沌	152
5.2.2	加密方案	152
5.2.3	算法实现与实践	154
5.2.4	相关研究	158
5.3	Baker 序列加密	158
5.3.1	离散化 Baker 映射	158
5.3.2	加密方案	160
5.3.3	算法实现与实践	161
5.3.4	相关研究	164
5.4	位平面置乱加密	164
5.4.1	位平面置乱	165
5.4.2	加密方案	167
5.4.3	算法实现与实践	171

5.4.4 相关研究	174
5.5 三维 Arnold 混沌映射加密	175
5.5.1 三维 Arnold 映射	175
5.5.2 三维混沌映射加密方案	175
5.5.3 算法实现与实践	180
5.5.4 评注和相关研究	185
5.6 基于 DNA 的加密	186
5.6.1 DNA 序列	186
5.6.2 基于 DNA 的加密方案	189
5.6.3 算法实现与实践	192
5.6.4 相关研究	198
参考文献	198

第Ⅲ部分 频域图像加密

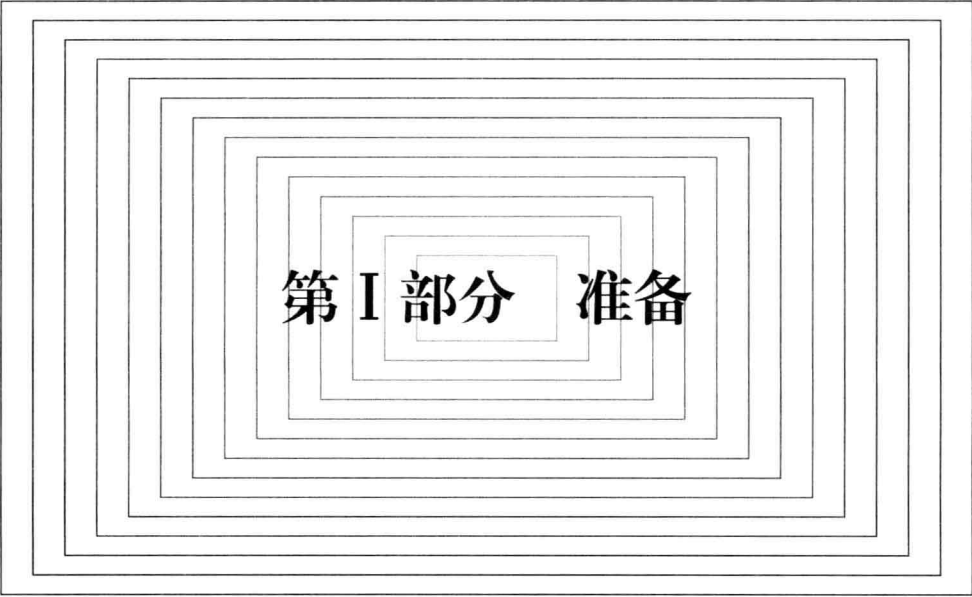
第 6 章 频域置乱与数据加密	203
6.1 Haar 域置乱加密	203
6.1.1 二维混沌映射和离散小波变换	203
6.1.2 加密方法	204
6.1.3 算法实现与实践	204
6.1.4 相关研究	207
6.2 基于 Fibonacci p -编码的图像置乱	208
6.2.1 P -Fibonacci 和 P -Lucas 变换	208
6.2.2 颜色空间及其转换	212
6.2.3 频域置乱算法	212
6.2.4 算法实现与实践	213
6.2.5 相关研究	220
6.3 矩阵变换加密	220
6.3.1 正交基和可逆矩阵	220
6.3.2 加密方案	223
6.3.3 安全性分析	225
6.3.4 算法实现与实践	225
6.3.5 相关研究	229

6.4 Haar 域序列加密	230
6.4.1 密钥的生成	230
6.4.2 小波域图像表示	230
6.4.3 加密方案	231
6.4.4 算法实现与实践	232
6.4.5 相关研究	235
参考文献	235
第 7 章 频域混合加密	237
7.1 选择加密与流加密	237
7.1.1 选择加密与 RC4 算法	237
7.1.2 加密方案	238
7.1.3 算法实现与实践	241
7.1.4 相关研究	245
7.2 DCT 域多层块置乱加密	245
7.2.1 多层块置乱	245
7.2.2 多层块置乱加密方案	247
7.2.3 算法实现与实践	249
7.2.4 相关研究	253
参考文献	253

第IV部分 图像加密分析与测试

第 8 章 图像加密分析与攻击	257
8.1 对二值压缩图像的已知明文攻击	257
8.1.1 对 2DRE 压缩算法与加密算法的分析	257
8.1.2 模拟攻击算法实现与实践	261
8.2 对 Arnold-Chen 加密方案的攻击	269
8.2.1 选择明文攻击方案	269
8.2.2 已知明文攻击方案	270
8.2.3 关于仿真攻击方案	272
8.2.4 选择明文攻击算法实现与实践	274
8.2.5 已知明文攻击算法实现与实践	275

8.3 对复合混沌加密方案的攻击	285
8.3.1 差分选择明文攻击	285
8.3.2 差分选择明文攻击算法实现与实践	287
8.4 对 Baker 序列加密方案的攻击	292
8.4.1 选择密文攻击方案	293
8.4.2 仿真攻击的实现	300
8.4.3 仿真攻击算法设计与实现	301
参考文献	308
第 9 章 图像加密评估与测试	309
9.1 密钥空间分析	309
9.1.1 加密密钥数量分析	309
9.1.2 密钥灵敏度测试	310
9.2 统计分析	310
9.2.1 加密图像的直方图分析	311
9.2.2 相邻像素的相关性分析	312
9.2.3 信息熵测试	313
9.3 扩散性测试	315
9.3.1 像素改变率	316
9.3.2 一致平均改变强度	316
9.3.3 雪崩效应	317
9.4 其他测试	317
9.4.1 置乱程度评估	317
9.4.2 混乱和扩散程度评估	319
9.4.3 加密质量的测试	320
参考文献	323



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 cosine 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,Celand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]用一个混沌神经网络和 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