信息科学技术学术著作丛书

数字图像置乱技术

邵利平 著

科学出版社

信息科学技术学术著作丛书

数字图像置乱技术

邵利平　著

科学出版社
北京

内 容 简 介

本书主要介绍作者在数字图像置乱领域所取得的独创性研究成果，包括雪崩图像置乱变换、基于矩阵变换的置乱逆问题求解、2 维双尺度矩形映射、基于多尺度三角映射的变尺度置乱、迷宫置乱以及改进 Tangram 方法的图像置乱方法。

本书可供数字图像安全领域的研究生和科技人员学习，也可供相关领域科技人员参考。

图书在版编目(CIP)数据

数字图像置乱技术/邵利平著．—北京：科学出版社，2016

(信息科学技术学术著作丛书)

ISBN 978-7-03-047776-7

Ⅰ．数… Ⅱ．邵… Ⅲ．数字图象处理-研究 Ⅳ．TN919.8

中国版本图书馆 CIP 数据核字(2016)第 052973 号

责任编辑：魏英杰 纪四稳 霍明亮 / 责任校对：蒋 萍

责任印制：张 倩 / 封面设计：陈 敬

科 学 出 版 社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

文林印务有限公司印刷

科学出版社发行 各地新华书店经销

*

2016 年 3 月第 一 版 开本：720×1000 1/16

2016 年 3 月第一次印刷 印张：15 1/2

字数：320 000

定价：98.00 元

(如有印装质量问题，我社负责调换)

《信息科学技术学术著作丛书》序

21世纪是信息科学技术发生深刻变革的时代，一场以网络科学、高性能计算和仿真、智能科学、计算思维为特征的信息科学革命正在兴起。信息科学技术正在逐步融入各个应用领域并与生物、纳米、认知等交织在一起，悄然改变着我们的生活方式。信息科学技术已经成为人类社会进步过程中发展最快、交叉渗透性最强、应用面最广的关键技术。

如何进一步推动我国信息科学技术的研究与发展；如何将信息技术发展的新理论、新方法与研究成果转化为社会发展的新动力；如何抓住信息技术深刻发展变革的机遇，提升我国自主创新和可持续发展的能力？这些问题的解答都离不开我国科技工作者和工程技术人员的求索和艰辛付出。为这些科技工作者和工程技术人员提供一个良好的出版环境和平台，将这些科技成就迅速转化为智力成果，将对我国信息科学技术的发展起到重要的推动作用。

《信息科学技术学术著作丛书》是科学出版社在广泛征求专家意见的基础上，经过长期考察、反复论证之后组织出版的。这套丛书旨在传播网络科学和未来网络技术，微电子、光电子和量子信息技术、超级计算机、软件和信息存储技术，数据知识化和基于知识处理的未来信息服务业，低成本信息化和用信息技术提升传统产业，智能与认知科学、生物信息学、社会信息学等前沿交叉科学，信息科学基础理论，信息安全等几个未来信息科学技术重点发展领域的优秀科研成果。丛书力争起点高、内容新、导向性强，具有一定的原创性；体现出科学出版社“高层次、高质量、高水平”的特色和“严肃、严密、严格”的优良作风。

希望这套丛书的出版，能为我国信息科学技术的发展、创新和突破带来一些启迪和帮助。同时，欢迎广大读者提出好的建议，以促进和完善丛书的出版工作。

中国工程院院士
原中国科学院计算技术研究所所长
李国杰

序

当前信息技术已进入了互联网＋大数据时代，数据爆炸趋势日益加剧，对于数据的加工与处理，无疑成为当前面临的重大问题。

在数字化时代里，所要加工处理的数据类型种类繁多，但可将其归纳为文字、语音与图像三种基本形式。图像形式的数据，与文字、语音相比较，信息量大、更为生动形象和具体，约占数字化时代里的70%。直观理解而言，“千言万语不及一张图”、“百闻不如一见”、“耳听为虚，眼见为实”，足以说明图像这种数据形式的重要性。

对于数字图像如何处理，就成为当前数据处理的一个重要分支。在图像处理中，数字图像的安全性更是至关重要的一个环节。数字图像安全主要涉及隐密术、数字水印、信息分存、可视密码和加密技术等。

图像加密技术是集数学、密码学、信息隐藏、通信、控制、信号处理、计算机、光学、物理学和医学等多学科交叉的研究课题，邵利平博士重点研究了轻量级的图像加密方法，即数字图像置乱技术。

这本书是邵利平博士研究工作的一个阶段性小结。全书对数字图像置乱技术相关内容进行了重点剖析，作者将自己的重要研究成果奉献给读者，这对于该项技术的研究与利用必将起到积极的推动作用。

先利敏

西安交通大学教授

前　言

在数字图像加密领域，研究最为广泛和灵活的一类轻量级图像加密方法，就是在同一空间内对图像的重编码技术，即数字图像置乱技术。随着计算机技术的飞速发展，数字图像置乱技术已成为数字图像安全传输和保密的必备手段与主要处理环节，结合不同的认知背景和技术领域，人们提出了多种多样、灵活多变和行之有效的图像置乱方法，包括：基于离散元素序列的图像置乱方法、基于扫描路线的图像置乱方法、基于遍历矩阵的图像置乱方法、基于迭代函数系统的图像置乱方法、基于离散混沌映射的图像置乱方法、基于中国拼图（Tangram 方法）的图像置乱方法和基于矩阵变换的图像置乱方法等。

对置乱稍加改进，即可用于隐密术、数字水印、信息分存和可视密码技术中，用于对秘密图像实现不同级别的安全保护。同时置乱技术在保护图像的同时，也提高了被保护图像的抗攻击能力，结合图像修复技术，可有效地提高恢复图像的可辨识质量。但现有的数字图像置乱研究也存在以下问题：①偏重特殊映射的讨论，没有遵守柯克霍夫准则，将密码体制建立在保密加密方法的基础上，是一种古典密码体制；②偏重于周期性讨论，将置乱恢复建立在周期性恢复的基础上，即通过逐次正向迭代对置乱图像进行恢复，计算代价较高；③对于基于离散元素序列的图像置乱方法，将加密参数建立在离散序列的基础上，加密参数选择受限，加密参数少且过于简单；④对于基于扫描路线的图像置乱方法，需提供额外的代价生成扫描曲线；⑤对于基于遍历矩阵的图像置乱方法，需提供额外代价建立遍历矩阵；⑥对于基于 Tangram 方法的图像置乱方法，如何有效地降低计算代价，避免中间参数的直接传递和如何进行大数据量的恢复参数隐藏是制约其真正实用价值的关键；⑦对于基于矩阵变换的图像置乱方法，部分文献要求变换行列式的绝对值为 1，并不具有普遍性，借助简单可逆变换阵叠加得到复杂变换阵的逆变换阵，并非必要；⑧对于亚仿射和拟仿射变换，可供选择的变换数量较少；⑨一些图像置乱算法关注的图像过于特殊且只能用于规则图像区域置乱。

针对数字图像置乱领域的研究现状并结合作者的研究工作，本书主要围绕着下列研究问题展开：①传统的基于高维矩阵变换的图像置乱方法，对攻击不具备全局扩散能力；②传统的基于矩阵变换的图像置乱方法用周期对置乱图像恢复，代价高昂，而通过逆变换对置乱图像恢复，已有方法未解决变换阵任意且规模较大情况下，$\mathbf{Z}_N$ 上的逆变换阵求解问题；③基于 2 维矩阵变换的图像置乱方法不具备直接处理任意矩形图像的能力，且通过逐次正向迭代对置乱图像恢复，代价较高；④传统的图像置乱方法通常局限在特定的尺度上，且不具备同时改变图像位置和灰度相关性的能力；

⑤传统的图像置乱方法一般用于规则图像区域置乱，而不能用于任意不规则封闭连通区域置乱；⑥传统基于 Tangram 方法的图像置乱方法计算代价较高。

针对以上研究问题，本书主要完成的研究工作如下。

(1) 提出雪崩图像置乱变换。该置乱变换可通过逆变换对图像进行置乱，通过正变换对置乱图像进行恢复，因而可减少由置乱图像恢复为原始图像的迭代次数，同时理论和实验表明雪崩置乱变换在受到各种攻击时的强脆弱性。结合雪崩图像置乱变换给出一种基于细粒度分块重构的多信道图像信息分存算法。实验表明，结合雪崩图像置乱变换实现细粒度分块重构的多信道图像信息分存算法可有效地甄别攻击，提高分发子信息的利用率。在分发子信息受到攻击时，也能充分利用分发子信息中未受损部分，最大可能性地重构秘密图像。

(2) 将实数域伴随矩阵求逆、杜里特尔分解和克劳特分解求逆、高斯-约当消去法求逆推广到 $\mathbf{Z}_N$，给出任意变换阵在 $\mathbf{Z}_N$ 上的求逆算法和简化求逆算法。所提方法可用于得到任意变换阵在 $\mathbf{Z}_N$ 上的逆变换阵，从而可直接对置乱图像恢复而不必计算可恢复周期。对大规模矩阵在 $\mathbf{Z}_{256}$ 上求逆的 CPU 耗时实测数据表明所提算法对大规模矩阵求逆的可用性；对 2 维、3 维和 n 维矩阵置乱图像的恢复实验表明所提算法对置乱图像恢复的有效性。

(3) 提出 2 维双模线性映射用以解决任意矩形图像的直接置乱问题，并给出 2 维双模线性映射周期性存在判据，用以选择合适的变换阵系数，使得在不增加额外的存储空间和计算代价的基础上，可用于任意矩形图像置乱，并且存在可恢复周期。为降低变换阵系数搜索代价，探讨一类特殊的 2 维双模线性映射，即 2 维双尺度三角映射，并解决 2 维双尺度三角映射的逆映射构造问题。在此基础上，给出用于任意矩形图像置乱的 2 维双尺度矩形映射，并证明 2 维双尺度矩形映射是任意 2 维双模线性映射满足一一映射的充分必要条件，然后结合 2 维矩阵变换和 2 维双尺度三角映射两类特殊映射的逆映射，给出 2 维双尺度矩形映射的逆映射。实验结果表明所提映射对任意矩形图像置乱的有效性，对矩形图像置乱和恢复的低代价性，以及对剪切、擦除和 JPEG 有损压缩攻击的鲁棒性。

(4) 提出多尺度三角映射及其逆映射用以解决图像的变尺度置乱问题。为提高尺度空间的可伸缩性，给出 $m$ton 映射。结合所提出的 $m$ton 映射，给出一种灵活的具有变尺度置乱能力的基于多尺度三角映射的图像置乱方法。同传统的图像置乱方法相比，所提方法可对任意图像在多个不同的尺度空间上置乱。在像素位置空间上，可改变像素的位置相关性；在像素色彩空间上，可改变像素的灰度相关性；在像素位置和色彩空间上，可同时改变像素的位置和色彩相关性。理论和实验表明，所提出的基于多尺度三角映射的图像置乱方法具有灵活的变尺度置乱能力，对图像置乱和恢复的低代价性，同传统的置乱方法相比，具有较好的一次置乱性能。

(5) 提出基于迷宫的 2 维、3 维封闭连通区域的数字图像置乱方法，用于对图像上任意指定的 2 维和 3 维封闭连通区域置乱。同传统置乱方法相比，所提出的置乱

方法具有灵活的不规则区域置乱能力，对置乱区域选择具有普适性，不仅可用于传统置乱方法所针对的正方形和矩形图像区域置乱，也可用于人为指定的具有复杂边界的 2 维和 3 维封闭连通区域置乱。

(6) 提出一种基于改进 Tangram 方法的图像置乱方法，用于降低传统 Tangram 置乱方法的计算代价。同传统方法不同，所提方法是将秘密图像划分的不重叠小块按 8 个等距变换直接和对应位置的公开图像子块进行最小二乘法匹配，找到残差最小的等距变换和匹配参数，从而将秘密图像转换成公开图像。理论和实验表明，同传统的 Tangram 方法相比，改进方法易于实现且避免了全局匹配，每个公开图像子块只与对应位置的秘密图像子块的 8 个等距变换小块进行匹配，实际编码时间远低于 Tangram 方法，公开图像可满足一定的辨识要求且重构密图视觉质量清晰，因而相对于传统 Tangram 方法具备较高的实际应用价值。

全书总共分为 8 章。第 1 章绪论，对图像置乱和与图像置乱密切相关的图像加密技术进展以及国内外研究现状进行研究和分析。第 2 章给出基于高维矩阵变换的雪崩图像置乱变换，在此基础上，结合雪崩图像置乱变换，给出一种基于细粒度分块重构的多信道图像信息分存算法。第 3 章将实数域的伴随矩阵求逆方法、杜里特尔分解、克劳特分解和高斯-约当消去法推广到 $\mathbf{Z}_N$，解决任意变换阵在 $\mathbf{Z}_N$ 上的逆变换阵求解问题。第 4 章确定可用于任意矩形图像置乱的 2 维双模线性映射的存在性，在此基础上研究一类特殊的映射，即 2 维双尺度三角映射，最终确定可用于任意矩形图像置乱的一般形式，即 2 维双尺度矩形映射，并解决其逆映射构造问题。第 5 章针对变尺度置乱问题，结合 $m$to$n$ 映射和多尺度三角映射，给出一种灵活的具有变尺度置乱能力的基于多尺度三角映射的图像置乱方法。第 6 章给出基于迷宫的 2 维、3 维封闭连通区域图像置乱算法，用于对图像上任意指定的 2 维和 3 维封闭连通区域进行置乱。第 7 章给出一种基于改进 Tangram 方法的数字图像置乱方法。第 8 章给出结语。

另外，借此机会也特别感谢澳门大学和北方工业大学的齐东旭教授研究团队所发表的大量研究论文，作者从中汲取了很多营养，也深受启发。感谢清华大学覃征教授，本书的部分研究成果的取得，得益于作者在西安交通大学读博期间，覃征教授对作者的指导和提供的宽松科研环境。特别感谢西安交通大学贾晓琳和张选平老师在作者读博期间及工作以后对作者的帮助。本书的出版得到了陕西师范大学计算机科学学院的大力支持与帮助，这里对全体同事表示衷心的感谢。同时感谢作者的研究生杨璐、欧阳显斌、祝莹、李苑梦、陈文鑫、谢贤文、张从飞、何思雨和唐子龙在本书写作与出版过程中所提供的力所能及的帮助。十分感谢江西理工大学方旺盛教授、张小红教授、李雯教授、李淑芝教授、曾传璜副教授、廖列法副教授、郑剑副教授、李江华副教授，赣南师范大学的黄贤通教授，以及上海教育考试院卢致杰博士对作者一直以来的帮助。魏英杰副编审对本书的出版付出了辛苦努力，在本书出版之际，向他表示衷心的感谢！

本书的出版得到了国家自然科学基金(项目编号:61100239)、陕西省自然科学基金(项目编号:2011JQ8009)和陕西师范大学中央高校基本科研业务费(项目编号:GK201402036)的资助。

由于置乱技术所涉及的技术十分宽泛和复杂,在本书撰写过程中也查阅了大量文献,希望尽可能地避免错误,但由于作者能力有限,疏漏或不足在所难免,恳请广大读者提出宝贵意见。

作 者

主要符号表

$\mathbf{N}^+$	自然数集
$-\mathbf{N}^+$	自然数集所有元素与-1的乘积构成的集合
$\mathbf{Z}^+$	整数集
$\mathbf{Z}^+/-\mathbf{N}^+$	非负整数集
$\mathbf{R}^+$	实数集
$\mathbf{Z}_N=\{0,1,\cdots,N-1\}$	模N上的剩余类集
$\boldsymbol{s}$	粗斜体变量表示序列
$\in$	属于
$\cap$	交运算
$\cup$	并运算
$\mathbf{Z}_N^+=\{1,\cdots,N-1\}$	$\mathbf{N}^+\cap\mathbf{Z}_N$，剩余类集$\mathbf{Z}_N$上非零元素构成的集合
$-\mathbf{Z}_N^+=\{-N-1,\cdots,-1\}$	剩余类集$\mathbf{Z}_N$上非零元素与-1的乘积构成的集合
$\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\cdots$	矩阵
$\boldsymbol{A}^*,\boldsymbol{B}^*,\boldsymbol{C}^*,\cdots$	实数域伴随矩阵
$\boldsymbol{A}^{-1},\boldsymbol{B}^{-1},\boldsymbol{C}^{-1},\cdots$	实数域逆矩阵
$\boldsymbol{A}^{\mathrm{T}},\boldsymbol{B}^{\mathrm{T}},\boldsymbol{C}^{\mathrm{T}},\cdots$	矩阵的转置
$\boldsymbol{A}_N^*,\boldsymbol{B}_N^*,\boldsymbol{C}_N^*,\cdots$	$\mathbf{Z}_N$上的伴随矩阵
$\boldsymbol{A}_N^{-1},\boldsymbol{B}_N^{-1},\boldsymbol{C}_N^{-1},\cdots$	$\mathbf{Z}_N$上的逆矩阵
$\boldsymbol{A}=(a_{i,j})_{M\times N}$	$M\times N$矩阵，且元素为$a_{i,j}$
$\boldsymbol{A}=(\ )_{M\times N}$	$M\times N$矩阵
$\boldsymbol{A}_{M\times N}$	$M\times N$矩阵$\boldsymbol{A}$
$\boldsymbol{I}$	单位矩阵
$\lvert\boldsymbol{A}\rvert$	$\boldsymbol{A}$的行列式
$M_{i,j}$	$\boldsymbol{A}=(a_{i,j})_{N\times N}$中元素$a_{i,j}$所对应的余子式
$A_{i,j}$	$\boldsymbol{A}=(a_{i,j})_{N\times N}$中元素$a_{i,j}$所对应的代数余子式
$M_{Ni,j}$	$\boldsymbol{A}=(a_{i,j})_{N\times N}$中元素$a_{i,j}$在$\mathbf{Z}_N$上对应的余子式
$A_{Ni,j}$	$\boldsymbol{A}=(a_{i,j})_{N\times N}$中元素$a_{i,j}$在$\mathbf{Z}_N$上对应的代数余子式
$\boldsymbol{A}^{[k]}=(a_{i,j}^{[k]})_{M\times N}$	第k个时刻的矩阵状态

$\boldsymbol{A}(k),k\in\{1,2,\cdots,N\}$	N 阶方阵 $\boldsymbol{A}$ 的顺阶 k 阶主子式
$\boldsymbol{A}(N)=\lvert\boldsymbol{A}\rvert,j\in\{1,2,\cdots,N\}$	N 阶方阵 $\boldsymbol{A}$ 的顺阶 N 阶主子式，即 $\boldsymbol{A}$ 的行列式
$\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z},\cdots$	黑斜体变量表示向量
$\boldsymbol{X}^{\mathrm{T}},\boldsymbol{Y}^{\mathrm{T}},\boldsymbol{Z}^{\mathrm{T}},\cdots$	向量的转置
$\boldsymbol{X}=(x_0,x_1,\cdots,x_{n-1})\in N^n$	N^n 空间的向量，且 $x_i\in\mathbf{Z}_N,i\in\mathbf{Z}_n$
$\boldsymbol{X}^{\mathrm{T}}=(x_0,x_1,\cdots x_n)\in d_0\times d_1\times\cdots\times d_{n-1}$	$d_0\times d_1\times\cdots\times d_{n-1}$ 空间的向量，且 $x_i\in\mathbf{Z}_{d_i},i\in\mathbf{Z}_n$
$\boldsymbol{X}^{[k]}=(x_0^{[k]},x_1^{[k]},\cdots,x_{n-1}^{[k]})$	第 k 个时刻的向量状态
$\boldsymbol{X}^{[k]}=(x_i^{[k]})_N,i\in\mathbf{Z}_N$	第 k 个时刻的向量状态
a_N^{-1}	a 在 $\mathbf{Z}_N$ 上的逆元
$\dot{a}_N$	a 在 $\mathbf{Z}_N$ 上的补
Card( )	集合元素的势
Ceil( )	向上取整运算
Gcd( )	求最大公因子
G_N( )	整数在 $\mathbf{Z}_N$ 上的规格化函数
Getheight( )	得到矩阵的高
Getwidth( )	得到矩阵的宽
Getlength( )	得到序列的长度
Lcm( )	求最小公倍数
Floor( )	向下取整运算
Rand_initial( )	随机数初始化函数
Random( )	随机数生成函数
min( )	求最小函数
max( )	求最大函数
$\varphi(N)$	小于 N 且和 N 互质的整数数量
$m!=1\times2\times\cdots\times m,m\in\mathbf{N}^+$	m 阶乘
$\mathrm{C}_m^n=\dfrac{m!}{(m-n)!\,n!}$	从 m 个元素任取 n 个元素的组合数
$+_N$	模 N 加
$-_N$	模 N 减
$\times_N$	模 N 乘
$\div_N$	模 N 除

$\equiv_N$	模 N 等
∞	无穷大
XOR	异或加密
Δ	整数偏差
$(a_{i,j}^{<+\Delta>})_{M\times N}$	矩阵元素 $a_{i,j}$ 处引入整数偏差 Δ 的误差矩阵
$(a_{i,j}^{<f+\Delta>})_{M\times N}$	对 $a_{i,j}$ 处引入整数偏差 Δ 的 $M\times N$ 矩阵，经过映射 $\boldsymbol{f}$ 产生的误差阵
$x\in(a,b)$	$a<x<b$，开区间
$x\in(a,b]$	$a<x\leqslant b$，左开右闭区间
$x\in[a,b)$	$a\leqslant x<b$，左闭右开区间
$x\in[a,b]$	$a\leqslant x\leqslant b$，闭区间
$<a_{l-1},a_{l-2},\cdots,a_0>$	由 $a_{l-1},a_{l-2},\cdots,a_0$ 构成的序列
$<a_{l-1},a_{l-2},\cdots,a_0>_m$	l 位 m 进制数，从高位到低位依次为 $a_{l-1},a_{l-2},\cdots,a_0$，且 $a_i\in\mathbf{Z}_m,i\in\mathbf{Z}_l$
$\mathbf{Z}_M\times\mathbf{Z}_N$ $=\{0,1,\cdots,M-1\}\times\{0,1,\cdots,N-1\}$	定义在剩余类集 $\mathbf{Z}_M,\mathbf{Z}_N$ 上的笛卡儿运算
$a\mid b$	a 是 b 的因子

目　　录

1 绪　论

1.1 研究背景

人类社会发展到今天，一直没离开过人类相互间以及与外界环境间发送、传递和接收的信息。从最早的洞穴图画、语言文字、金鼓号角、狼烟烽火到后来的电报电话、电台传真、广播电视直至今天的因特网、E-mail 和各种各样的即时通信软件，人们总是在寻找最快捷、最便利和最有效的通信方式。人类所能获取的信息包括很多种，如文字、符号、数据、语音、图形和图像等，但都可将其归纳为文字、语音和图像 3 种基本形式。同语音和文字相比，图像所蕴含的信息量更大，更为生动、形象和具体，占人类从外部世界所获取信息的 70%，“千言万语不及一张图”，“百闻不如一见”和“耳听为虚，眼见为实”都是对图像重要性的直观理解。

20 世纪末到 21 世纪初，伴随着计算机软硬件技术的发展和因特网的广泛应用，信息技术已普遍应用于各行各业，并与人们的日常生活和工作发生联系。但与此同时，信息的非法窃取和篡改、信息在使用过程中有意或无意地遭受破坏，以及计算机病毒和网络黑客的破坏行为，给信息发送、传递和接收带来了严重威胁。作为信息的主要传播载体，图像的安全性也倍受人们关注。

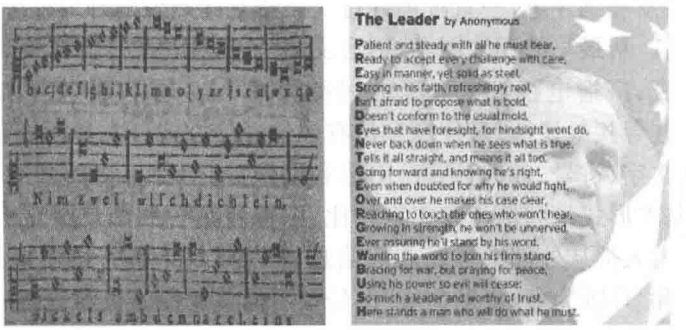
先进技术往往是把“双刃剑”，在方便人们的同时，也给人们的生活带来了负面影响。在数字化时代，一方面，低代价的数字化图像摄取设备和功能强大的图像编辑软件急剧增长和快速普及，使得编辑、修改和存储数字图像变得简单有趣；另一方面，也使得任何计算机用户可随心所欲地对数字图像移花接目，从而给人们对整个世界的认知带来严重威胁。

尽管大多数人对数字图像修改，只是为了增强图像效果，娱乐的成分大些，如人们所熟知的“网络小胖”恶搞图集。但也不乏一些人出于不同的目的，有意或无意地散布一些逼真虚假的图片来混淆视听，导致媒体公信力丧失和挫伤人们对数字图像真实性的信心，如近年来沸沸扬扬的“广场鸽”事件、“华南虎”事件、“藏羚羊”事件和“草坪鸽”事件等。一些失实的数字图像，一旦应用于军事、政治和外交，将会影响、误导和改变整个军事进程，诱发新的军事冲突，导致政治风波和外交失和，如美国议员 Kerry 总统竞选风波、热比娅闹剧、伊拉克战争时期的伊战俘假图事件和“硬纸板”士兵事件。

当前，数字化时代已将人们带入一个所见未必真实的世界里，数字图像安全至关重要，因此必须开展图像安全研究。数字图像安全主要涉及隐密术、数字水印、

信息分存、可视密码和加密技术等。

所谓隐密术就是将机密信息隐藏于另一公开的载体中，以不引起攻击者的注意，然后通过公开信息来传递秘密信息。图 1-1(a)是《信息隐藏技术——隐写术与数字水印》一书中给出的利用音乐乐谱来传递秘密信息的例子。图 1-1(b)是巴基斯坦教科书中曾经出现的藏头诗“the leader”，将该首诗的每行首字母顺次连接起来，则刚好显示为“PRESIDENT GEORGE W BUSH”，即美国前总统乔治·沃克·布什。



(a) (b)

图 1-1 隐密术举例：(a)利用乐谱传递秘密信息的例子；(b)“the leader”藏头诗

所谓数字水印就是嵌入数字作品中的一种标记。根据嵌入水印在受到攻击时的不同特性，可进一步将水印分为稳健水印和脆弱水印，其中稳健水印用于对数字作品声明版权，脆弱水印用于对数字作品认证和篡改定位。图 1-2 是 DCT 域稳健水印的例子。所采用的方法是：①对载体图像在 YCrCb 空间上的亮度分量按 8×8 分块进行 2 维 DCT 变换；②对每个分块主对角线上的第 2 个 DCT 系数对 12(质量因子为 50 时，在该位置的亮度量化值)进行奇偶量化，植入 2 值水印形成含水印图像。

(a) (b) (c) (d) (e)

图 1-2 DCT 域稳健水印举例：(a)256×256 的 24 位载体图像 lenna；(b)32×32 的 2 值图像水印；(c)嵌入水印后的载体图像；(d)对含水印图像进行质量因子为 50 的 JPEG 压缩攻击；(e)攻击后提取的 2 值水印