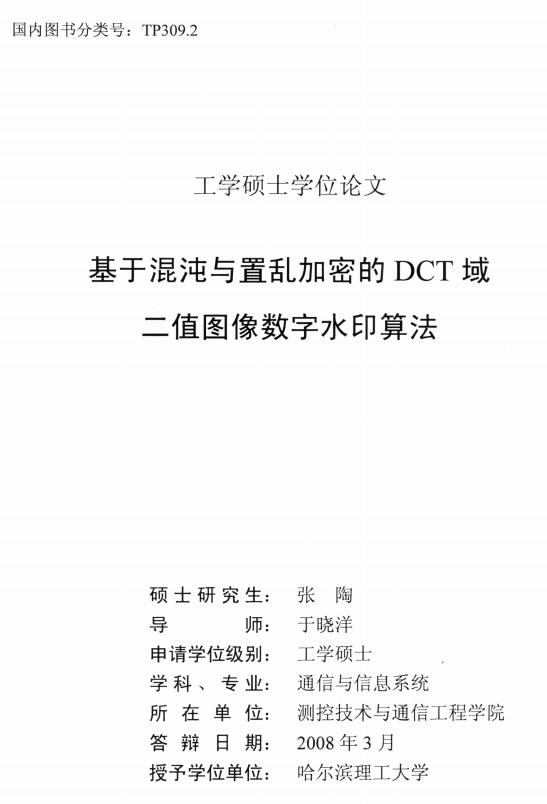
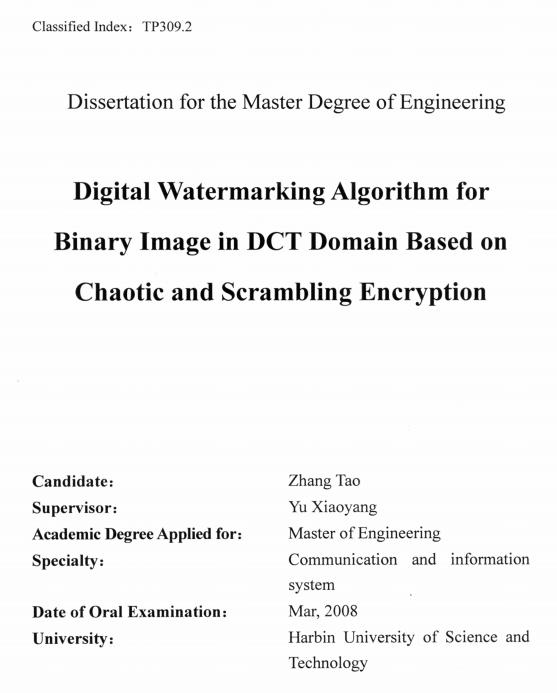
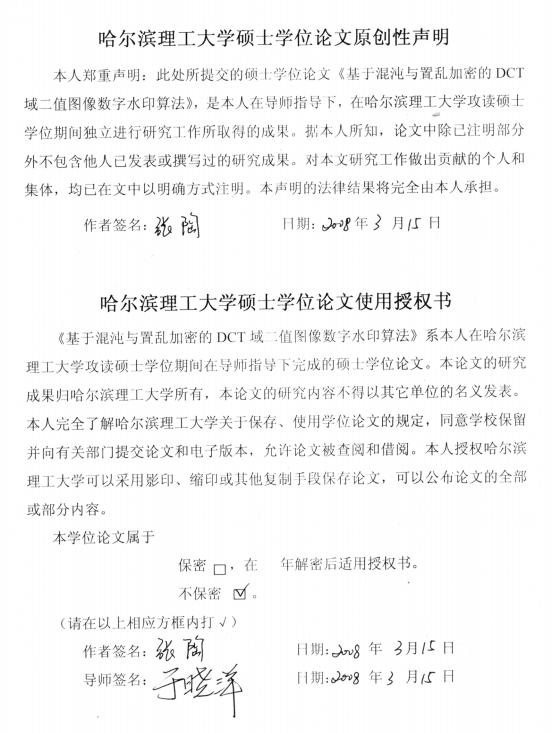
中国知网 https:Www  cnknet



中国知网 https:Www  cnknet



中国知网 https:Www  cnknet



中国知网 https:Www  cnknet

基于混沌与置乱加密的 DCT 域 二值图像数字水印算法

摘要

随着多媒体技术和计算机网络技术的发展，数字产品的版权保护问题显 得尤为重要。数字水印技术作为一种新的版权保护方法，已经受到广大科技 工作者和用户越来越多的关注，研究成果也层出不穷。 其中，虽然对静态图 像水印的研究很多，但这些研究还不够成熟，图像水印在不可见性和鲁棒性 方面很难同时满足。

本文主要针对二值图像数字水印进行了如下研究：

1 ．分析数字水印技术的基本理论，图像数字水印的一般原理及其模 型，对图像数字水印的性能评价、数字水印攻击分析和经典的图像数字水印 算法做了较深入的介绍。

2 ．本文在比较典型水印算法的基础上，提出一种对含有版权信息的原 始水印图像进行双重加密的方法，即首先对原始水印图像进行 Logistic 混沌 序列加密，然后在此基础上进行 Arnold cat 位置置乱加密，使水印信息具有 双重的保密性。

3 ．在前面对水印进行了双重加密的基础上，根据人眼视觉系统对图像 进行块分类，实现基于 DCT 域的二值图像数字水印算法，将不同强度的水 印分量自适应地嵌入到 DCT 的中频系数中，使嵌有水印的图像具有良好的 视觉不可见性。

通过对嵌入水印的图像进行高斯噪声和椒盐噪声、均值滤波、图像剪 切、JPEG 压缩等水印攻击方法，表明了该算法不仅能够保证水印自身的安 全性，同时也具有较好的鲁棒性和视觉隐蔽性，使受保护的数字产品具有双 重安全性。

**关键词** 数字水印；离散余弦变换； Logistic 映射；Arnold cat 变换

- I -

中国知网 https:Www  cnknet

**Digital Watermarking Algorithm for Binary**

**Image in DCT Domain Based on Chaotic and Scrambling Encryption**

**Abstract**

The copyright protection of digital works becomes more and more important with the development of multimedia technique and computer network. As a new method of copyright protection, digital watermark is attracted more and more attention of researchers and users with lots of achievements. Although there are many researches focus on static image, they are not mature enough, the invisibility and robust can’t be satisfied at the same time.

The thesis is mainly focus on the digital watermark of binary image with the following study:

1. Analysis the basic theory of digital watermark technology, and also the general principal and module. Make a detail introduction for the evaluation about the performance of watermark image, attack analysis and the relevant detect methods.

2. A double encryption method for the original image is put forwards based on the comparison of classic watermark algorithm, which encrypted with the Logistic chaotic sequence, then proceeded with Arnold cat position scrambling transformation, to make the watermark information safer.

3. Improve the block classify method based on the comparisons of typical algorithms, embedding the watermark weights with different strength into the middle and low frequency coefficients of DCT domain adaptively according to the classification, to make the embedded image with very good invisibility.

Though the experiments of attacking with Gaussian noise, salt & pepper noise, mean value filleting, cropping and JPEG compression, it indicates that this algorithm can make sure of the security of watermark itself, with excellent robust and invisibility, and also make the double guarantee of the protected digital work.

- II -

中国知网 https:Www  cnknet

**Keywords** digital watermark, Discrete Cosine Transformation, Logistic map, Arnold cat transformation

- III -

中国知网 https:Www  cnknet

**目** 录

**[第](#bookmark2)****[1 章](#bookmark2)****[绪论](#bookmark2)****[3](#bookmark2)**

[1.1 课题背景 3](#bookmark3)

[1.1.1 信息安全的重要性 3](#bookmark4)

[1.1.2 信息隐藏技术的重要性 4](#bookmark5)

[1.2 数字水印技术的国内外研究现状 5](#bookmark6)

[1.2.1 国内研究现状 5](#bookmark7)

[1.2.2 国外研究现状 6](#bookmark8)

[1.3 课题来源及研究内容 8](#bookmark1)

**[第](#bookmark9)****[2 章](#bookmark9)****[图像数字水印技术的基础理论](#bookmark9)** **[9](#bookmark9)**

[2.1 数字水印技术的基本概念 9](#bookmark10)

[2.1.1 数字水印的分类 9](#bookmark11)

[2.1.2 数字水印的应用及特性 11](#bookmark12)

[2.2 图像数字水印的一般原理及理论模型 12](#bookmark13)

[2.3 图像数字水印性能评价标准 14](#bookmark14)

[2.3.1 影响水印鲁棒性的因素 14](#bookmark15)

[2.3.2 水印可见性评价 15](#bookmark16)

[2.3.3 评估水印性能的攻击方法 15](#bookmark17)

[2.4 图像数字水印经典算法 16](#bookmark18)

[2.4.1 空域算法 16](#bookmark19)

[2.4.2 变换域算法 16](#bookmark20)

[2.4.3 压缩域算法 20](#bookmark21)

[2.4.4 生理模型算法 21](#bookmark22)

[2.4.5 NEC 算法 21](#bookmark23)

[2.5 本章小结 22](#bookmark24)

**[第](#bookmark25)****[3 章](#bookmark25)****[二值图像水印的加密](#bookmark25)** **[23](#bookmark25)**

[3.1 混沌加密二值图像水印序列的生成 23](#bookmark26)

[3.1.1 混沌理论 23](#bookmark27)

[3.1.2 Logistic 混沌加密二值图像水印序列的生成 25](#bookmark28)

- 1 -

中国知网 https:Www  cnknet

[3.1.3 实验结果及分析 27](#bookmark29)

[3.2 二值图像水印位置置乱加密 28](#bookmark30)

[3.2.1 位置置乱变换的原理 28](#bookmark31)

[3.2.2 实验结果及分析 29](#bookmark32)

[3.3 本章小结 31](#bookmark33)

**[第](#bookmark34)****[4 章](#bookmark34)****[DCT 域二值图像数字水印算法](#bookmark34)****[32](#bookmark34)**

[4.1 离散余弦变换（DCT）的原理 32](#bookmark35)

[4.1.1 DCT 变换的原理 32](#bookmark36)

[4.1.2 DCT 变换系数的选择 34](#bookmark37)

[4.1.3 基于人类视觉系统的块分类方法 35](#bookmark38)

[4.2 二值图像水印的嵌入方案 35](#bookmark39)

[4.3 二值图像水印的提取方案 37](#bookmark40)

[4.4 实验结果和分析 38](#bookmark41)

[4.5 本章小结 46](#bookmark42)

**[结论](#bookmark43)** **[47](#bookmark43)**

**[参考文献](#bookmark44)** **[48](#bookmark44)**

**[攻读学位期间发表的学术论文](#bookmark45)** **[52](#bookmark45)**

**[致谢](#bookmark46)** **[53](#bookmark46)**

- 2 -

中国知网 https:Www  cnknet

第1章 绪论

1.1 课题背景

信息媒体的数字化为信息的存取提供了极大的便利性，特别是随着计算机 网络通讯技术的发展，数据的交换和传输变成了一个相对简单的过程，人们借 助于计算机、数字扫描仪、打印机等电子设备可以方便、迅速地将数字信息传 输到所期望的地方。但随之而来的副作用是这些数字形式的数据文件或作品使 有恶意的个人和团体有可能在没有得到作品所有者的许可下拷贝和传播有版权 的内容。数字化技术本身的可复制和广泛传播的特性所带来的负面效应，已经 成为信息产业健康持续发展的一大障碍。 目前，数字媒体的信息安全、知识产 权保护和认证问题变得日益突出，已经成为数字世界中一个非常重要和紧迫的 议题。

在全球联网的形势下，网络信息安全是非常重要的，一个国家信息系统的 失控和崩溃将导致整个国家经济瘫痪，进而会影响到国家安全。信息网络上的 攻防技术水平将反映一个国家的科技水平和防范意识。在日常生活中，网上电 子商务等也必须以信息安全技术为基础。对网上各种有重要价值信息的版权保 护本质上也是一种信息安全问题。信息安全涉及信息、加密、信息安全传输、 防病毒、防黑客攻击、用户认证、用户权限分配等诸多方面。目前的版权保护 系统广泛采用对网络资源的访问控制机制，它通过本地网或广域网控制某些 IP 地址或终端的连接，限制某些用户的访问权限，从而有效地防止非法用户对计 算机系统和数据的访问。但是如果用户以合法帐号得到多媒体信息，再对数据 进行非法复制和传播，那么安全访问控制机制就无能为力了。因而信息安全手 段必须是立体的、多层次的，应当针对数据的特性研究相应的信息安全措施。 其中，多媒体信息安全技术的研究主要有两种方法：多媒体信息加密技术和多 媒体信息隐藏技术[1]。

1.1.1 信息安全的重要性

基于文本数据设计的加密算法， 一般是把一段数据流(称为明文)转换成看 起来没有意义的数据(称为密文)，如 DES(Data Encryption Stansard，数据加密 标准) 和 RSA( 根据它的发明者的首位字母命名，即 Rivest ， Shamir 和

- 3 -

中国知网 https:Www  cnknet

Adleman)。由于将明文数据加密成密文数据，使得在网络传递过程中非法拦截 者无法从中获得信息，从而达到保密的目的。虽然可以把多媒体数据作为文本 数据流一样看待，并使用传统的加密算法进行加密，但是，多媒体数据流具有 的特性与文本数据的特性有很大不同。因此， 目前的传统加密方法如 DES 、3- DES 或 RSA 等也很难满足多媒体应用中的实时性等要求。新型的多媒体应用 需要新的数据加密技术。近年来，在这方面的研究取得了一些成果，主要针对 视频数据和图像数据。传统的加密方法一直被认为是在通信研究应用领域中主 要的信息安全手段而受到极大重视。近年来人们逐步认识到其对多媒体内容的 保护和完整性认证也具有一定的局限性。首先，加密方法只用在通信的信道 中，密文数据因其不可理解性妨碍多媒体信息的传播；其次，多媒体信息经过 加密后容易引起攻击者的好奇和注意，并有被破解的可能，而一旦被破解后其 内容完全透明，版权所有者就失去了对盗版的任何控制权；另外，密码学中的 完整性认证是通过数字签名方式来实现的，它并不是直接嵌到多媒体信息之 中，因此无法察觉信息在经过加密之后的再次传播中内容的改变[2，3]。

1.1.2 信息隐藏技术的重要性

信息隐藏的例子层出不穷，从中国古代的藏头诗到中世纪欧洲的栅格系 统，从古希腊的蜡板藏书到德国间谍的密写术等这些都是典型的例子。多媒体 技术的广泛应用，为信息隐藏技术的发展提供了更加崭新的领域。1996 年 5 月 30 日~6 月 1 日，在英国剑桥大学牛顿研究所召开了第一届国际信息隐藏学术 研讨会，标志着一门新兴的交叉学科——信息隐藏学的正式诞生[4] 。信息隐藏 学作为隐蔽通信和知识产权保护等的主要手段，正得到广泛的研究与应用。需 要指出的是，信息隐藏不同于传统的密码学技术，密码技术主要研究将机密信 息进行特殊的编码，形成不可识别的密码形式(密文)进行传递；信息隐藏主要 研究如何将一机密信息秘密隐藏于另一公开的信息中，然后通过公开信息的传 输来传递机密信息。对加密通信而言，可能的监测者或非法拦截者可截取密文 并对其进行破译，或将密文进行破坏后再发送，从而影响机密信息的安全。但 对信息隐藏而言，可能的监测者或非法拦截者难以从公开信息中判断机密信息 是否存在或截获机密信息，从而保证机密信息的安全。信息隐藏技术由于其独 有的特点和优势，己成为当今多媒体信息安全技术的一大重要研究热点。待隐 藏的信息被称为秘密信息，它可以是版权信息或其他秘密数据，比如说一个序 列号；而公开信息则称为载体信息(cover message)，如视频、音频片段。而信

- 4 -

中国知网 https:Www  cnknet

息隐藏过程一般由密钥(Key)来控制，通过嵌入算法将秘密信息隐藏到公开信 息中，而隐蔽载体(隐藏有秘密信息的公开信息)则通过信道传递，最后检测器 利用密钥从隐蔽载体中恢复/检测出秘密信息。信息隐藏技术主要由两部分组 成：信息嵌入算法和隐蔽信息提取/检测算法(检测器)。信息嵌入算法是利用密 钥实现秘密信息的隐藏。隐蔽信息提取/检测算法是利用密钥从隐蔽载体中检 测/恢复秘密信息。在密钥未知的前提下，第三者很难从隐秘载体中得到或删 除、甚至发现秘密信息。信息隐藏技术具有透明性、强壮性、高效性和安全性 等基本特性。信息加密与信息隐藏是从不同的角度提出的信息安全技术，将信 息加密与信息隐藏有机结合，就可进一步提高信息的安全性。此外，需要注意 的是，解决信息安全问题，仅仅依赖于技术和算法(如加密芯片、安全协议等) 等技术手段是不够的，还有赖于第三方认证中心、法制手段、道德观念和保密 措施的完善，这是一个全方位的问题[5]。

1.2 数字水印技术的国内外研究现状

1.2.1 国内研究现状

随着技术信息交流的加快和水印技术的迅速发展，数字水印技术得到了全 世界科研人员极大的关注并迅速发展起来。与此同时数字水印技术在我国也得 到了足够的重视，国内各大研究所和高校也纷纷投入数字水印的研究，其中比 较有代表性的有哈尔滨工业大学的孙圣和、牛夏牧、陆哲明等，天津大学的张 春田、苏育挺等，北京邮电大学的杨义先、钮心忻等，中国科学院自动化研究 所的刘瑞祯、谭铁牛等，他们是国内较早投入水印技术研究且取得较好成绩的 科研单位。现在国内已经出现了一些生产水印产品的公司，其中比较有代表性 的是由中科院自动化研究所的刘瑞祯、谭铁牛等人于 2002 年在上海创办了的 一家专门从事数字水印、多媒体信息和网络安全、防伪技术等软硬件开发的公 司——上海阿须数码技术有限公司，现在这家公司已申请了多项数字水印技术 专利[6]。

1999 年 12 月，我国信息安全领域的何德全院士、周仲义院士、蔡吉人院 士与有关应用研究单位联合发起召开了我国第一届信息隐藏学术研讨会。2000 年 1 月，由国家“863”智能机专家组和中科院自动化所模式识别国家重点实 验室组织召开了数字水印学术研讨会，来自国家自然科学基金委员会、国家信 息安全测评认证中心、中国科学院、 北京邮电大学、国防科技大学、清华大

- 5 -

中国知网 https:Www  cnknet

学、北方工业大学、上海交通大学、天津大学、中国科技大学、北京大学、北 京理工大学、中山大学、北京电子技术应用研究所等单位的专家学者和研究人 员深入讨论了数字水印的关键技术，报告了各自的研究成果。从这次会议反应 的情况上看，我国相关学术领域的研究与世界水平相差不远，而且有自己独特 的研究思路。2000 年 6 月 17 日~18 日于北京，2001 年 9 月 10 日于西安， 2002 年 8 月 24 日~26 日于大连，2004 年 11 月 19 日~21 日于广州中山大学， 2006 年 8 月 7 日~8 月 9 日于哈尔滨，2007 年 11 月 12~14 日于南京分别召开 了第二、第三、第四、第五、第六、第七届信息隐藏学术讨论会，学术会议集 中了国内从事信息隐藏研究的著名专家学者，促进了我国的信息隐藏学术研究 及其应用。2002 年后，国内信息隐藏的研究才日益丰富起来，特别是将信息隐 藏技术与其他领域、其他学科结合的研究已取得了相当大的进展，各种隐藏的 新方法层出不穷，标志着我国对数字水印技术的研究已与国际同步了。

1.2.2 国外研究现状

数字水印的概念是在 20 世纪 90 年代提出的，1993 年 Tirkel 等人发表了一 篇文章，首先提出了电子水印(Electronic watermarking)说法。在他们随后发表 的另一篇题为“A digital watermark”的文章中，正式提出了“数字水印”这一术 语。在这两篇论文中他们针对灰度图像提出了两种向图像最低有效位(LSB： Least Signigicant Bit)中添加水印的方案。一种是使用一个 m 序列来置换图像的 最低有效位，另一种是向图像的最低有效位叠加一个 m 序列，并使用自相关 函数对水印进行检测。这种水印嵌入方法虽然比较简单易行，但是水印的鲁棒 性很差。在开创了对数字水印技术研究的先河之后，对数字水印的研究兴趣在 日益增长。1995 年 Cox 等人提出了一种基于扩频通信的思想，他们把图像进 行离散余弦变换(DCT)将水印嵌入到图像感知上最重要的频域因子中的水印方 案，实验表明该方法具有较好的鲁棒性[7] 。1996 年，Pitas 提出了一种盲水印方 案。该算法虽然是一个盲水印算法的代表，但是它是一种空间域算法，所以它 的鲁棒性有待进一步提高[8]。其后的研究人员在 Pitas 算法基础上进行了改进， 使得算法的鲁棒性进一步提高了。

Benser 等在 1996 年开始了对音频水印技术的研究，在他的文章 “Techniques for date hiding”中提出了相位编码、扩频编码、回声编码以及 LSB 编码等四种经典算法，可以说为数字水印的后续发展奠定了良好的基础。

贝尔实验室的 Maxemchuk 最早开始了对文本文档中数字水印技术的研

- 6 -

中国知网 https:Www  cnknet

究。1994 年他首先提出在数字文档中嵌入标记的方法，以保护电子出版物创作 者的版权利益。他提出了行位移编码、特征和字位移编码等三种方法。1996 年 Bender 等[9]提出了一种与字位移编码有点不同的算法，他利用左对齐调整文档 时附加空格的方法嵌入水印，该算法使用曼彻斯特编码原理，将水印数据信息 嵌入文件中。

视频水印算法按照嵌入水印的数据域分为两种：非压缩域算法和压缩域算 法。对于非压缩域的水印研究始于 1994 年，Matsui 等提出了一种 DCT 域视频 数据嵌入算法，该算法同图像水印算法相似，通过 DCT 系数对每一帧视频图 像的像素值进行变化，因而对剪切、噪声等处理非常脆弱，而且一旦攻击者掌 握了同一帧视频图像的多个不同水印版本，则可以通过比较以得到原始的、未 加水印的图像帧[10] 。Swanson 等对上述视频水印嵌入方法进行了改进，利用分 块 DCT 变换和频率掩蔽特性相结合嵌入水印，提高了水印的鲁棒性。此外， Swanson 等还研究了一种基于内容的数字水印技术，并据此提出了一种多分辨 率的视频水印算法。Langelart 等提出了两种压缩域的水印嵌入算法：一种是替 换帧内编码块 DCT 系数的变长码的方法，另一种是基于丢弃部分压缩视频码 流的方法。Hartung 等研究了 MPFG-2 压缩视频域上的水印算法，将水印嵌入 在 DCT 系数中，并实现了水印的盲检测[11] 。该算法对压缩、轻度旋转、滤波 具有鲁棒性，但对更大程度的旋转，则提取不出水印。

自从第一届国际信息隐藏学术研讨会于 1996 年 5 月 30 日~6 月 1 日，在 英国剑桥牛顿研究所召开以来，SPIE 和 IEEE 的一些重要国际会议也开辟了相 关的专题。随着数字水印技术研究的不断深入，数字水印从研究对象上来己经 涉及到图像水印、音频水印、文本水印、视频水印和三维网格数据水印等多个 方面。

由以上的国内外研究现状可以看出，数字水印仍然是一个不十分成熟的研 究领域，还存在许多亟待解决的问题，其理论基础依然很薄弱，绝大多数水印 算法还是经验性的。存在的问题主要有以下几个方面：

1 ．为了衡量算法的性能，水印系统就要有较好的鲁棒性，但是水印的鲁 棒性和不可觉察性往往很难同时得到满足，如何在两者之间达到一个平衡，是 一个研究的热点问题。

2 ．对水印的加密研究还不够充分。当前嵌入的大多数水印已经都是一些 含有版权信息的有意义的水印，如：文本、声音、图像或视频，但一般有意义 的水印的保密性较差，所以采取一定的加密措施，更好的保护含有一定的版权 信息内容的水印，是当今另一个数字水印研究的热点问题。

- 7 -

中国知网 https:Www  cnknet

1.3 课题来源及研究内容

本文课题来源于国家教育部春晖计划项目中的部分。

当前，对静态图像水印的研究很多，但这些研究还不够成熟，水印在不可 见性和鲁棒性方面很难同时满足，例如，水印的不可见性较好，则是以牺牲水 印的鲁棒性为代价，水印的鲁棒性较好，则水印的不可见性较差，所以对于图 像水印在保障水印不可见性的前提下，应提高图像水印的抵抗各种攻击的稳健 性。因此本文选取静态灰度图像水印系统作为研究对象，研究工作如下：

1 ．以二值图像水印信号为研究对象，充分利用混沌系统具有形式简单、 对初值敏感依赖性和具有白噪声的统计特性，生成经过混沌加密的二值图像水 印序列；

2 ．在原始水印信息经过混沌加密后，再经过一次位置置乱，实现对水印 信息二次加密，既更好地保护了含有版权或其它重要信息的水印，又实现了消 除图像像素空间的相关性，增强水印算法的鲁棒性；

3 ．在对水印信息进行了二次加密的基础上，在 DCT 域对原始图像进行二 值图像的数字水印嵌入和提取。

论文共分为四章，各章的内容安排如下：

第一章：简要介绍信息隐藏概念、数字水印技术国内外研究现状和本文的 研究意义。

第二章：介绍图像数字水印的基本概念、一般理论模型以及图像数字水印 的性能评价方法、数字水印攻击分析方法以及几种典型的数字水印算法。

第三章：介绍了混沌理论及置乱方法的特性，以及如何利用 Logistic 混沌 映射和位置置乱方法对水印数据进行加密。

第四章：具体介绍了一种基于混沌与位置置乱加密的 DCT 域图像数字水 印的嵌入和提取算法。

结论部分，总结全文并提出今后进一步的研究思路。

- 8 -

中国知网 https:Www  cnknet

第2章 图像数字水印技术的基础理论

这一章介绍图像数字水印的一般模型、几种图像数字水印的性能评价方 法、数字水印攻击分析方法以及几种典型的数字水印算法。

2.1 数字水印技术的基本概念

数字水印的思想源于古代的隐写术，是通过一定的算法将一些标志性信息 直接嵌到多媒体内容当中，但不影响原内容的价值和使用，并且不能被人的知 觉系统觉察或注意到水印信息的存在。水印信息可以是作者的序列号、公司标 志或有特殊意义的文本等，可用来识别文件、图像或音乐制品的来源、版本、 原作者、拥有者、发行人或合法使用人对数字产品的拥有权。与加密技术不 同，数字水印技术并不能阻止盗版活动的发生，但它可以判别对象是否受到保 护，监视被保护数据的传播、真伪鉴别、非法拷贝、解决版权纠纷并为法庭提 供证据。

所谓数字水印就是将具有特定意义的标记(水印)，利用数字嵌入的方法隐 藏在多媒体数据(如图像、音频、视频信号等)中而不影响原数据的视觉和听觉 效果，并且这些数字信息可以部分或全部从混合数据中恢复出来，从而成为知 识产权保护和数字多媒体防伪的有效手段。水印通常是不可见或不可察觉的， 它与原始数据(如图像、音频、视频数据等)紧密结合并隐藏于其中，成为原数 据不可分离的一部分，并可以经历一些不破坏原数据使用价值或商用价值的操 作而存活下来。数字水印技术最初的目的是保护静止图像和视频；而现在正广 泛的被应用到其他数字媒体，如三维模型、网上音乐、 DVD 和数字电视广 播。由于数字水印是实现版权保护的有效办法，因此如今已成为多媒体信息安 全研究领域的一个热点，也是信息隐藏技术研究领域的一个重要分支[12]。

2.1.1 数字水印的分类

数字水印技术可以从不同的角度进行划分，最常见的分成如下几类[13]：

1 ．按特性划分 按水印的特性可以将数字水印分为鲁棒数字水印和脆弱 数字水印两类。鲁棒数字水印主要用于在数字作品中标识著作权信息，如作 者、作品序号等，它要求嵌入的水印能够经受各种常用的编辑处理；脆弱数字

- 9 -

中国知网 https:Www  cnknet

水印主要用于完整性保护，与鲁棒水印的要求相反，脆弱水印必须对信号的改 动很敏感，人们根据脆弱水印的状态就可以判断数据是否被篡改过。

2 ．按水印所附载的媒体划分 按水印所附载的媒体，我们可以将数字水 印划分为图像水印、音频水印、视频水印、文本水印以及用于三维网格模型的 网格水印等。随着数字技术的发展，会有更多种类的数字媒体出现，同时也会 产生相应的水印技术。

3 ．按检测过程划分 按水印的检测过程可以将数字水印划分为明文水印 和盲水印。明文水印在检测过程中需要原始数据，而盲水印的检测只需要密 钥，不需要原始数据。一般来说，明文水印的鲁棒性比较强，但其应用受到存 储成本的限制。目前学术界研究的数字水印大多数是盲水印。

4 ．按内容划分 按数字水印的内容可以将水印划分为有意义水印和无意 义水印。有意义水印是指水印本身也是某个数字图像(如商标图像)或数字音频 片段的编码；无意义水印则只对应于一个序列号。有意义水印的优势在于，如 果由于受到攻击或其它原因致使解码后的水印破损，人们仍然可以通过视觉观 察确认是否有水印。但对于无意义水印来说，如果解码后的水印序列有若干码 元错误，则只能通过统计决策来确定信号中是否含有水印。

5 ．按用途划分 不同的应用需求造就了不同的水印技术。按水印的用 途，我们可以将数字水印划分为票据防伪水印、版权保护水印、篡改提示水印 和隐蔽标识水印。票据防伪水印是一类比较特殊的水印，主要用于打印票据和 电子票据的防伪， 一般来说，伪币的制造者不可能对票据图像进行过多的修 改，所以，诸如尺度变换等信号编辑操作是不用考虑的，但另一方面，人们必 须考虑票据破损、图案模糊等情形，而且考虑到快速检测的要求，用于票据防 伪的数字水印算法不能太复杂；版权标识水印是目前研究最多的一类数字水 印，数字作品既是商品又是知识作品，这种双重性决定了版权标识水印主要强 调隐蔽性和鲁棒性，而对数据量的要求相对较小；篡改提示水印是一种脆弱水 印，其目的是标识宿主信号的完整性和真实性；隐蔽标识水印的目的是将保密 数据的重要标注隐藏起来，限制非法用户对保密数据的使用。

6 ．按水印隐藏的位置划分 按数字水印的隐藏位置，我们可以将其划分 为时/空域数字水印、频域数字水印、时/频域数字水印和时间/尺度域数字水 印。时/空域数字水印是直接在信号空间上叠加水印信息，而频域数字水印、 时/频域数字水印和时间/尺度域数字水印则分别是在 DCT 变换域、时/频变换 域和小波变换域上隐藏水印。随着数字水印技术的发展，各种水印算法层出不 穷，水印的隐藏位置也不再局限于上述四种。应该说，只要构成一种信号变

- 10 -

中国知网 https:Www  cnknet

换，就有可能在其变换空间上隐藏水印。

2.1.2 数字水印的应用及特性

数字水印技术的应用前景和应用领域是非常广泛的，可以应用在信息安全 保护的很多方面。目前数字水印技术主要有以下几种应用领域[14]：

1 ．维护所有权(Ownership assertion)：为了表明对数字产品内容的所有 权，所有者 A 用私钥产生水印并将其插入原图像(以图像为例)中，然后即可公 开加载过水印的图像，如果 B 声称对公开的有水印的图像有所有权，那么 A 可以用原图像和私钥证明在 B 声称所有的图像中有 A 的水印，由于 B 无法得 到原图像，B 无法作同样的证明。

2 ．指纹(Fingerprinting)：为了避免未经授权的复制和分发可公开得到的多 媒体内容，作者可在其每个产品中嵌入一个明显的水印(指纹)。如果发现了未 经授权的拷贝,则通过检索指纹来追踪其来源。

3 ．认证和完整性校验(Authentication and integrity verification)：在许多应 用中，需要验证数字内容未被改变、修改或造假。尽管多媒体内容的认证可通 过传统的密码学技术来完成，但利用数字水印来进行认证和完整性校验的优点 在于：认证同内容是密不可分的, 因此简化了处理过程。当对插入了水印的数字 内容进行检验时，必须用唯一的与数据内容相关的密钥提取出水印，然后通过 检验提取出的水印完整性来检验数字内容的完整性。

4 ．内容标识(Content labeling)：此类应用中，插入的水印信息构成了一个 注释，提供有关数字产品内容的进一步的信息。

5 ．使用控制(Usage control)：在一个封闭的系统中，多媒体内容需要特殊 的硬件来拷贝和观看使用，插入水印来标识允许的拷贝数，每拷贝一份，进行 拷贝的硬件会修改水印内容，将允许的拷贝数减一，以防止大规模的盗版。

6 ．内容保护(Content protection)：对水印技术的要求随着应用的不同而不 同，一个水印方案很难满足所有应用的所有要求，因此，数字水印算法往往是 针对某类应用而设计的。

数字水印应具有如下基本特性[15]：

1 ．稳健性 指抗拒各种信号处理操作和恶意攻击，在掩体对象不产生明 显降质的前提下，不导致水印信息丢失的能力。

2 ．不可检测性 指嵌入水印后的数据与原始载体数据具有一致的特性。

3 ．不可感知性 指向数字作品中嵌入的数字水印，是利用人类视觉或听

- 11 -

中国知网 https:Www  cnknet

觉系统的特性，经过一系列隐藏处理，隐藏对象必须没有明显的降质现象，而 嵌入的水印不会引起人的感知。

4 ．隐藏位置的安全性 指必须将水印信息隐藏于掩体对象的内容之中， 而非文件头等处，这样可以防止因文件格式的变换而使水印遭到破坏。

5 ．无歧义性 恢复出的水印或水印判决的结果应该能够确定地表明所有 权，不会发生多重所有权的纠纷。

6 ．计算有效性 水印处理算法应该比较容易用软、硬件实现。尤其是水 印检测算法必须足够快，以满足在产品发行网络上对多媒体数据的管理要求。

2.2 图像数字水印的一般原理及理论模型

从数字通信的角度上来看，水印信号嵌入(编码)可以理解为一个宽带信道 (载体图像)上用扩频通信技术传输一个窄带信号(水印)。虽然水印信号具有一 定的能量，但是分布到信道中任何一个频率上的能量都是很难检测到的。水印 信号的检测(译码)则是一个有噪信道中弱信号的检测问题。

从图像处理的角度看，嵌入到图像中的水印信号可以视为在强背景下叠加 一个弱信号，只要满足叠加的水印信号强度低于人的视觉系统(HVS：Human Visual System)对比度门限这个条件， HVS 就无法感知到信号的存在。由于 HVS 受空间、时间和频率特性的限制，因此可以通过对载体图像作一定的调 整，就有可能在不引起人感知的情况下嵌入一些信息。

水印嵌入过程的一般模型如图 2-1 所示。在本论文中设原始图像为 *I*，水 印信号为 *W*，密钥为 *K*，水印嵌入算法则用下式表示：

'

*I*

= *F*(*I*, *W*, *K*)

(2-1)

上式中 *F* 表示水印嵌入算法，*I* ' 表示嵌有水印的图像[16]。

|  |
| --- |
| 嵌入算 法(*F*) |

|  |
| --- |
| 嵌有水印的图 象*I*' |

水印 (W)

|  |
| --- |
| 原始图 象(*I*) |

密钥 (*K*)

图 2-1 水印嵌入的模型

Fig.2-1 The model of embedding watermark

- 12 -

中国知网 https:Www  CKnet

有三种常用的水印嵌入公式：

*v*1' = *v*1 + *α*× *x*1 (2-2)

*v*1' = *v*1 (1+ *α*× *x*1 ) (2-3)

*v*1' = *v*1 (*eα*×*x*1 ) (2-4)

其中，*v*1 、*v*1' 分别表示原始图像像素和嵌有水印的图像像素； *x*1 表示水印信号 分量；*α* 是嵌入强度因子，它决定水印的嵌入深度， *α* 越大嵌入的水印越深， 水印的鲁棒性越好，可见性越差，即嵌有水印的图像有明显的失真，也就没有 什么使用价值了；如果嵌入强度因子*α* 过小，虽然此时的嵌有水印的图像和原 始图像相似度非常高，但水印的鲁棒性很差，在经历一些图像处理时容易被去 掉，所以*α* 的选取必须考虑图像的性质和人类视觉系统的特性[17]。

水印的提取和检测过程与水印嵌入的过程刚好相反。在有些水印系统中， 水印可以被很精确地检测并分离出来，这一过程被称为水印的提取，如图 2-2 所示。

|  |
| --- |
| 提取算法(*F’*) |

|  |
| --- |
| 提取出的水印 |

原始水印 (*W*) 或原始图象(*I*)

|  |
| --- |
| 待检测 图象 |

密钥 (*K*)

图 2-2 水印提取的模型

Fig.2-2 The model of extracting watermark

例如在完整性确认应用中，必须能够很精确地提取出被嵌入的水印信号， 并且通过水印信号的完整性来确认多媒体数据的完整性。假如提取出的水印发 生了部分的变化，最好还能通过发生变化的水印信号的位置来确定原始数据被 篡改的位置。

- 13 -

中国知网 https:Www  CKnet

图 2-3 是水印检测框图。提取和检测可以作用于任何图像，提取和检测是 可以有原始产品的参与，也可以没有原始产品的参与。

|  |
| --- |
| 待检测 图象 |

|  |
| --- |
| 检测算法(*D*) |

原始水印 (*W*) 或原始图象(*I*)

|  |
| --- |
| 水印相似度 检验(*Sim*) |

水印存 在

密钥 (*K*)

图 2-3 水印检测的模型

Fig.2-3 The model of detecting watermark

2.3 图像数字水印性能评价标准

2.3.1 影响水印鲁棒性的因素

影响水印鲁棒性的因素如下：

1 ．嵌入的信息量 这是一个重要的参数，因为它直接影响水印的鲁棒 性。对同一种水印嵌入方法而言，要嵌入的信息越多，则水印的鲁棒性越差。 被嵌入的信息依赖于各种各样不同的应用场合。

2 ．水印嵌入强度 水印嵌入强度和水印可见性之间存在一个折衷。增加 鲁棒性就要增加水印嵌入强度，相应地也会增加水印的可见性。

3 ．图像的尺寸和特性 图像的尺寸对嵌入水印的鲁棒性有直接影响。除 了图像的尺寸之外，图像的特性也对水印的鲁棒性产生重要影响。

4 ．密钥 尽管密钥的数量不直接影响到水印的可见性和鲁棒性，但它对 系统的安全性起到了很重要的作用。水印算法中，密钥空间(密钥允许取值的 范围)必须足够大，这样可以使穷举攻击法(Exhaustive Search Attack)失效。许 多安全系统不能够抵御一些简单的攻击，往往是因为系统设计者在设计系统时 没有遵循基本的密码学原理。

考虑上述因素，对于公平的测试基准和性能评估，待评估水印方法必须在

- 14 -

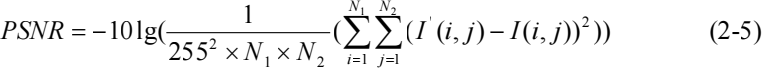
中国知网 https:Www  cnknet

各种不同的测试图像集中进行测试。并且，为了得到在统计上有效和可信的结 果，必须使用不同的密钥和改变水印的不同强度来对水印系统进行评估。若要 对几种水印方法进行比较，则必须确保对所有的待评估方法，嵌入的信息量是 相同的[18，19]。

2.3.2 水印可见性评价

水印可见性和稳健性之间存在着折衷，因而， 正确评估和比较水印系统 时，对水印可见性的考虑就十分重要。对水印可见性的评估可以用定量度量方 法(Quantitatie Metric)或主观测试方法(Subjective Test)。目前，还没有通用的度 量标准，常用的两种定量度量的方法是：一种采用基于普通像素的失真量度量 方法；另一种采用基于人的视觉系统(HVS)的度量方法[20] 。而常用的主观测试 方法是一种基于观测者打分的质量等级评判方法。

在本论文中用峰值信噪 PSNR 来评价嵌有水印图像的质量，公式如下：



其中 *I*' 为嵌有水印图像， *I* 为原始载体图像， *N*1 × *N*2 为图像大小， (*i*, *j*) 代 表原始图像和嵌有水印图像的坐标。这是目前很常用的评价方法。

2.3.3 评估水印性能的攻击方法

在对水印系统进行性能评估的过程中，需要对水印系统进行一些攻击，用 来测试其性能。这些攻击是一个水印系统在实际使用过程中可能会遭受到的， “攻击”的含义包括有意的攻击和无意的攻击。有意的攻击是指为了去除水印 而采取的各种处理方法，这种攻击一般是恶意的；无意的攻击是指含水印的图 像在使用过程中不可避免受到的诸如有损压缩、噪声影响等处理。下面列举这 些攻击类型[21]：

1 ．有损压缩 许多如同 JPEG 和 MPEG 的压缩策略会造成不可恢复的数 据丢失，从而潜在地降低了数据的质量。

2 ．几何变形 几何变形尤其是对于图像视频包含了旋转、平移、缩放和 复制等操作。

3 ．普通的信号处理操作 包含数/模转换、模/数转换、重采样、重量子 化、抖动变形、重压缩、线性滤波、 非线性滤波、色彩缩减、附加像素值偏

- 15 -

中国知网 https:Www  cnknet

移、附加高斯噪声、附加非高斯噪声和像素交换。

4 ．其它有意攻击 印刷和重扫描；重水印；共谋：合法授权的用户用嵌 入不同水印的图像副本，通过一定算法生成未嵌入水印的图像；伪造：合法授 权的用户使用有效的水印来生成嵌入水印图像的副本；IBM 攻击：制作原件的 赝品，使其能够像原件一样使用，其伪造水印也能够被提取。

本论文用有损压缩、剪切、低通滤波、附加噪声等攻击来测试水印系统的 性能。

2.4 图像数字水印经典算法

近年来，对数字水印技术的研究取得了很大的进展，下面将对一些典型的 数字水印算法进行分析，数字水印算法跟数字水印一样有很多种分类方法，按 最主要的特征将目前的数字水印算法分为：空域算法、频域算法、压缩域算 法、生理模型的算法、统计学的算法等[22] 。下面给出的数字水印算法大部分是 针对图像数据(除特别指明，某些算法也适合视频和音频数据)。

2.4.1 空域算法

空域图像水印技术是指在图像的空间域中嵌入水印的技术，空域算法包括 文本水印算法、Schyndel 算法和 Patchwork 算法等。该类算法中最简单和典型 的水印算法是将水印信息嵌入到随机选择的图像点中最不重要的像素位(LSB： least significant bits)上，这里的水印信息是指二值比特序列，这可保证嵌入的 水印是不可见的。由于 LSB 位平面携带着水印，因此在嵌入水印图像没有产 生失真的情况下，水印的恢复很简单，只需要提取含水印图像的 LSB 位平面 即可，而且这种方法是盲水印算法。但是由于使用了图像不重要的像素位，算 法的鲁棒性差，水印信息很容易被滤波、 图像量化、几何变形的操作破坏。另 外一个常用方法是利用像素的统计特征将信息嵌入像素的亮度值中[23]。

针对 LSB 算法出现的缺点，一些研究人员对空域算法进行了改进，使算 法的鲁棒性和安全性得到了提高。

2.4.2 变换域算法

变换域算法包括离散余弦变换(DCT)方法、离散傅立叶变换(DFT)方法、离 散小波变换(DWT)方法等。

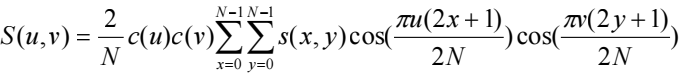
<2.4.2.1> 离散余弦变换**(DCT)**方法 离散余弦变换(Discrete Coisne Transform)简

- 16 -

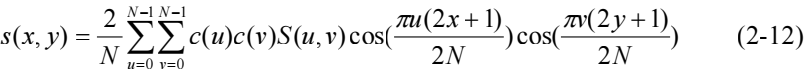
中国知网 https:Www  cnknet

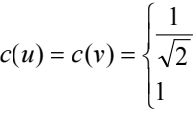
称 DCT。任何连续的实对称函数的傅立叶变换中含有余弦项，因此余弦变换与 傅立叶变换一样有明确的物理意义， DCT 变换避免了傅立叶变换中的复数运 算，它是基于实数的正交变换。变换矩阵的基向量很近似于 Toeplitz 矩阵(系数 矩阵对称且沿着与主对角线平行的任一对角线上的元素都相等)的特征向量， 而 Toeplitz 矩阵又体现了人类语言及图像信号的相关特性，故 DCT 常常被认 为是对语音和图像信号的准最佳变换，同时 DCT 算法较易于在数字信号处理 器中快速实现，因此它目前在图像编码中占有重要的地位，成为一系列有关图 像编码的国家标准(JPEG 、MPEG 、H.261 等)的主要环节。

在数字图像处理中使用的是二维 DCT，对一幅 *N* × *N* 图像 *s*(*x*, *y*)，它的 DCT 变换为：

 (2-11)

反离散余弦变换(IDCT)为：



其中 以上各式中 

, *u* = 0或*v* = 0 *,u,v* = 1*,*2*,...,N-*1

与空域图像水印相比，离散余弦变换(DCT)域图像水印对压缩、滤波和其 他一些数字处理操作具有更强的鲁棒性，同时又与常用的图像压缩标准 JPRG 兼容，因而得到了更为广泛的重视，目前研究得最多、最深入、最成熟的水印 技术是基于 DCT 的数字水印技术。

Hartung 等提出了一种 DCT 域数字水印算法，该类算法中大部分水印算法 采用了跳频扩展频谱通信(spread spectrum communication)技术。算法实现过程 为：首先把原始图像分成 8 × 8 的不重叠像素块，再把像素块进行离散余弦变换 (DCT)，然后将水印叠加到 DCT 域中幅值最大的前 *k* 个系数上(不包括直流分 量)，通常为图像的低频分量。解码函数则分别计算原始图像 *I*和水印图像 *I’*的 离散余弦变换(DCT)，并提取嵌入的水印 *W* ' ，再做相关检验*W* •*W* ' / ·*W* •*W* ' 以确定水印的存在与否。该方法即使当水印图像经过一些常见的几何变形和信 号处理操作而产生比较明显的变形后仍然能够提取出一个可信赖的水印[24]。

由 Cox 等人提出的基于 DCT 变换的扩频水印技术是 DCT 域算法中最具有

- 17 -

中国知网 https:Www  cnknet

代表性的。它将满足正态分布的伪随机序列加入到图像的 DCT 变换后视觉最 重要系数中，利用了序列扩频技术(SS)和人类视觉特性(HVS)。算法原理是先 选定视觉重要系数，再进行修改，最常用的嵌入规则如下：

加法原则：

*v*1' = *v*1 + *αw*1 (2-13)

乘法原则：

*v*1' = *v*1 (1+ *αw*1 ) (2-14)

其中 *v*1 、*v*1' 分别是修改前和修改后的频域系数，*α* 是缩放因子，*w*1 是第 *i* 个 信息位水印。一般地，乘法准则的抗失真性能要优于加法准则。水印的检测是 通过计算相关函数实现的。从嵌入水印的图像中提取*w*1' 是嵌入规则的逆过程， 把提取出来的水印与原始水印作相似性运算，得出的相似值与给定的阈值比 较，可确定是否存在水印[25] 。这是鲁棒性水印的最基本的算法，得到了广泛的 应用。

Tao 等在给定噪声敏感指数的局部感知分类基础上提出了一种自适应 DCT 水印技术[26]。他们将水印嵌入到交流 DCT 系数中，根据默认的 JPEG 格式压缩 表，选择合适的系数，使量化的单位最小，并按下式对系数进行修改：

 = *x*1 + max  (2-15)

其中 *αm* 是当前块的噪声敏感指数， *D*1 是*x*1 的量化单位，5 ≤ *k* ≤ 6 。需要注 意的是在这个算法中水印信息不是随机产生的。作者提出一种局部分类算法， 它将每个块归到 6 个可感知类中去。分类算法利用了 HVS 的亮度掩蔽、边缘 掩蔽和纹理掩蔽效应。按对噪声的灵敏度高低，6 个可感知类型依次为：边缘 的、中等亮度均匀的、低亮度或高亮度均匀的、中等忙的、忙的和非常忙的。 相应的每个可感知类有一个噪声灵敏度指数。水印的恢复同样是利用假设检 测，并需要原始图像和水印的参与。

Podilchuk 等提出了可感知水印的方法。他们使用从视觉模型导出的 JND(Just Noticeable Difference)来确定在图像的各个部分所能容忍的水印信息的 最大强度，从而能避免水印信息对视觉质量的破坏。这个算法使用 Waston 定 义的感知模型。该模型利用频率的亮度敏感性和局部对比掩蔽，对每个 8 × 8 的 DCT 块提供了与图像相关的掩蔽阈值。根据原始图像与待检测图像间的偏差和 水印序列的相关性，就可进行水印检测，即将最大的相关值与给定阈值相比

- 18 -

中国知网 https:Www  cnknet

较，来确定待检测的图像中是否含有水印。实验表明，上述水印方案对 JPEG 格式压缩、剪切、缩放、添加噪声等都有非常好的鲁棒性。但是对含有几何变 形的攻击，则需要在水印检测前对图像进行相应的逆操作[27]。

Barni 等提出了另外一种利用 HVS 掩蔽特性的基于 DCT 的水印算法。在 水印嵌入过程中，对*N*× *N* 的原始图像进行*N*× *N* 的 DCT 变换。对 DCT 系数 按 Zig-Zag 扫描重新排列为一维向量。对向量中开始的 *L* 个系数不作修改，对 第 *L* 个系数后面的 *M* 个系数进行修改来嵌入水印[28]。算法描述如下：

设开始的 *L+M* 个 DCT 系数是 *T*：

*T* = {*t*1, *t*2,..., *tL*, *tL*+1,..., *tL*+*M* } 水印由 *M* 个符合正态分布的实数随机数组成：

*X* = {*x*1, *x*2,..., *xM* } 按下式将水印*X* 嵌入到 *T* 中：

*tL*+1 = *tL*+1 + *α t* *L*+*i* *x*1 , *i* = 1,2,..., *M*

'

(2-16)

(2-17)

(2-18)

其中 *α* 确定了水印的强度。为了增强水印的鲁棒性，可用下式作可视掩蔽：

*y*1'',*j* = *y*1,*i* (1− *β*1,*i* ) + *β*1,*iy*1',*j* = *y*1,*j* + *β*1,*j* (*y*1',*j* − *y*1,*i* ) (2-19)

其中 *β*1,*j* 是考虑到 HVS 特性而引入的加权因子，当嵌入区域对噪声不敏感 时，说明可嵌入水印的强度较高，此时应有 *β*1,*j* ≈ 1, *y*1'',*j* ≈ *y*1',*j* ；当嵌入区域对噪

声敏感时，说明可嵌入水印的强度很低，此时应有 *β*1,*j* ≈ 0,

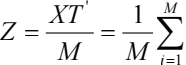
''

*y*1,*j* ≈ *yi* ,*j*

。可简单

地取 *β*1,*i* 为像素*y*1,*j* 处的归一化采样方差，即以*y*1,*j* 为中心的一个 *R* × *R*(文献中 *R*=9)方块的采样方差与所有块方差最大值的比率。

水印检测是通过比较水印和可能变化的 DCT 系数间的相关性 Z 和一个阈 值*TZ*' 而进行的。对待检测的图像*I* ' ，按照与水印嵌入时相似的步骤，获得从第 *L*+1 至第 *L+M* 个 DCT 系数*T* ' ，按下式计算*T* ' 和水印*X* 的相关值：

 *x*1+*Lt*(2-20)

阈值由下式决定：

 (2-21)

实验表明该算法对一些图像处理技术，如 JPEG 压缩、低通滤波、中值滤

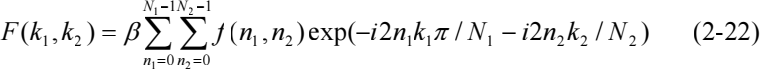
- 19 -

中国知网 https:Www  cnknet

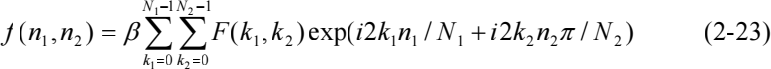
波以及直方图均衡和拉伸等具有较强的鲁棒性。

<2.4.2.2> 离散傅立叶变换**(DFT)**方法 离散傅立叶变换(DFT)在信号处理中己被 广泛研究，在水印领域里也要考虑它。目的是为了提供控制宿主信号频率的可 能性。为了在可视性和健壮性之间获得最后的权衡，选择图像的合适部分来嵌 入水印是非常必要的。

给定一个二维信号*f*(*x,y*) ，DFT 定义为：



其中  。而逆 DFT 定义为：



为了在水印和它的载体之间进行相位调制，DFT 对于设计水印是有用的。这种 变换也应用于将图像分割成多个感觉频段。

Tilki 和 Bcex[33]提出了一种 DFT 变换域音频水印嵌入算法，这种变换的频 谱范围是 0-8kHz。首先对音频信息进行 DFT，然后选择其中频率范围为 2.4- 2.6kHz 的 DFT 系数进行水印嵌入，并用表示水印序列的频谱分类来替换相应 的 DFT 系数。算法选择该频段使得水印被保存在音频信号中具有较强能量的 部分。如果嵌入水印量不是很大并且其幅度相对于当前的音频信号更小，则该 算法对噪声、录音失真及磁带的颤动都具有一定鲁棒性。

<2.4.2.3> 离散小波变换**(DWT)**方法 小波是图像压缩标准“JPEG2000”中的关 键技术。与傅立叶变换一样，小波变换的基本思想是将信号展开成一族基函数 之间的加权和，即用一族函数来表示或逼近信号或函数。这一族函数是通过基 本函数的平移和伸缩构成的。

与其他域水印技术一样，小波域水印也分为水印嵌入、提取(检测)两部 分。几种典型的小波水印方案有：基于低频子带方法，细节分量方法，利用同 图像编码关系的方法等[29]。

2.4.3 压缩域算法

基于 JPEG 、MPEG 标准的压缩域数字水印系统不仅节省了大量的完全解

- 20 -

中国知网 https:Www  cnknet

码和重新编码过程，而且在数字电视广播及 VOD(Video on Demand)中有很大 的实用价值。视频水印研究是当前水印技术研究方向中的一个热点和难点，热 点在于大量消费类数字视频产品的推出，如 VOD 、DVD，使以数字水印为重 要组成部分的数字产品版权保护技术的市场需求更为迫切。难点是由于虽然数 字水印技术近几年得到长足发展，但方向主要是集中于静止图像的水印技术 [38] 。然而在视频水印的研究方面，由于包括时间域掩盖效应等特性在内的更为 精确的人眼视觉模型尚未完全建立，使视频水印技术相对图像水印技术发展滞 后，同时现有的标准视频编码格式又造成了水印技术引入上的局限性。而另一 方面，由于一些针对视频水印的特殊攻击形式(如帧重组，帧间组合等等)的出 现，为视频水印提出了一些区别于静止图像的水印的独特要求。主要的几种针 对 MPEG-2 压缩视频数据流的有代表性的数字水印方案有：将水印信息直接嵌 入到原始视频图像中，形成含水印的原始视频信息，然后进行 MPEG-2 视频编 码；将嵌入过程引入到 MPEG-2 编码器中；直接嵌入水印信息到 MPEG-2 压缩 码流中。

2.4.4 生理模型算法

人的生理模型包括人类视觉系统 HVS(Human Visual System)和人类听觉系 统 HAS。该模型不仅被多媒体数据压缩系统利用，同样可以供数字水印系统 利用。利用视觉模型的基本思想均是利用从视觉模型导出的 JND(Just Noticable Difference)描述来确定在图像的各个部分所能容忍的数字水印信号的最大强 度，从而能避免破坏视觉质量。也就是说，利用视觉模型来确定与图像相关的 调制掩模，再利用其来插入水印。这一方法同时具有好的透明性和强健性。

2.4.5 NEC 算法

该算法由 NEC 实验室 Cox 等人提出，该算法在数字水印算法中占有重要 地位，这一算法提出了强壮水印算法的两个重要原则[30]：

1.水印信息应该嵌入原始数据中对人的感觉最重要的部分。在频谱空间 中，这种重要部分就是低频分量。这样，攻击者在破坏水印的过程中，不可避 免地会引起图像质量的下降。基于同样的道理，一般的图像处理技术也并不去 改变这部分数据。故水印的强壮性大大提高了。

2.水印信息应该由具有高斯分布的独立同分布随机实数序列构成。这使得 水印经受多拷贝联合攻击的能力大大增强。

- 21 -

中国知网 https:Www  cnknet

NEC 系统实现方法是：首先以密钥为种子来产生伪随机序列，该序列具有 高斯 *N*(0, 1)分布，密钥一般由作者的标识码和图像的哈希值组成，其次对图像 做 DCT 变换，最后用伪随机高斯序列来调制(叠加)该图像除直流(DC)分量外的 1000 个最大的系数。该算法具有较强的鲁棒性、安全性、透明性等。由于采用 特殊的密钥，因此可防止 IBM 攻击，而且该算法还提出了增强水印鲁棒性和 抗攻击算法的重要原则，即水印信号应该嵌入原始数据中对人感觉最重要的部 分，这种水印信号由独立同分布随机实数序列构成，且该实数序列应该具有高 斯分布 *N*(0, 1)的特征。

2.5 本章小结

这一章主要介绍了图像数字水印的基本概念、一般原理及其模型，对图像 数字水印的性能评价、数字水印攻击分析和水印相关检测方法也做了较深入的 介绍。给出了本论文所用的评价水印图像质量的方法和水印检测方法。对典型 的图像水印算法也作了简单介绍。

- 22 -

中国知网 https:Www  cnknet

第3章 二值图像水印的加密

本章从水印产生的角度出发，首先介绍混沌系统特性和混沌序列的生成方 法，并实现了一种基于混沌加密的水印生成的算法；接着介绍了位置置乱技 术，并应用位置置乱对水印进行二次加密，为后面阐述的数字水印嵌入算法做 准备。

3.1 混沌加密二值图像水印序列的生成

3.1.1 混沌理论

混沌理论产生于数学与物理领域，它与相对论、量子论一起被誉为二十世 纪三大科学革命。它打破了确定理论和随机理论之间不可逾越的界限，揭示了 自然界及人类社会普遍存在的复杂性，是有序与无序、确定与随机的统一。

混沌理论目前在很多方面都有应用，混沌应用可分为混沌分析与控制和混 沌综合。前者由复杂的人工和自然系统中获得混沌信号并寻找隐藏的确定性规 则，分析或预测系统的动力学特性，进而控制混沌系统到达给定的状态。后者 利用人工产生的混沌从混沌动力学系统中获得可能的功能，如人工神经网络的 联想记忆等。

混沌现象是在非线性动力系统中出现的确定性的、类似随机的过程，这种 过程既非周期又不收敛，并且对初始值有极其敏感的依赖性。随着非线性和混 沌理论的成熟，当前对混沌的研究集中在应用领域，特别是在通信方面的应 用，这是因为混沌系统对初始值有敏感的依赖性，可以提供数量众多的、非相 关、类随机而又确定可再生的信号。

一个一维离散时间非线性动力系统的定义如下：

*xk* +1 = *f* (*xk* ) (3-1)

设 *V* 是度量空间，连续映射*f* : *V* → *V* 。如果*f*满足以下三个条件：

(1)对初值的敏感依赖；

(2)拓扑传递性；

(3)*f* 的周期点在 *V* 中稠密； 则称*f* 是在 *V* 上的混沌映射[31]。

- 23 -

中国知网 https:Www  cnknet

混沌运动是确定性非线性系统所特有的复杂运动形态，出现在某些耗散系 统、不可积保守系统和非线性离散映射系统中。它的运动状态是有限区域且轨 道永不重复、性态复杂的运动。与其他复杂现象相区别，混沌运动有着自己独 有的特征，主要有：

1 ．有界性 混沌是有界的，它的运动轨线始终局限于一个确定的区域， 这个区域称为混沌吸引域。无论混沌系统内部多么不稳定，它的轨线都不会走 出混沌吸引域。所以从整体上来说混沌系统是稳定的。

2 ．遍历性 混沌运动在其混沌吸引域内是各态历经的，即在有限时间内 混沌轨道经过混沌区内每一个状态点。

3 ．内随机性 一定条件下，如果系统的某个状态可能出现，也可能不出 现，该系统被认为具有随机性。混沌的内随机性实际就是他的不可预测性，对 初值的敏感性就造就了它的这一性质。同时也说明混沌是局部不稳定的。

4 ．分维性 指混沌的运动轨线在相空间中的行为特征。分维性表示混沌 运动状态具有多叶、层结构，叶层越分越细，表现为无限层次的自相似结构。

5 ．标度性 是指混沌运动是无序中的有序态。

6 ．适普性 所谓适普性是指不同系统在趋向混沌态时所表现出来的某些 共同特征，它不依具体的系统方程或参数而变。适普性是混沌内在规律性的一 种体现。

7 ．统计特征 正的 Lyapunov 指数以及连续功率谱等。Lyapunov 指数是对 非线性映射产生的运动轨道相互间趋近或分离的整体效果进行的定量刻画。对 于非线性映射而言，Lyapunov 指数表示 n 维相空间中运动轨道沿各基向量的平 均指数发散率，当 Lyapunov 指数小于零时，轨道间的距离按指数消失，系统 运动状态对应于周期运动或不动点；当指数大于零时，则在初始状态相邻的轨 道将按指数分离，系统运动对应于混沌状态；当指数等于零时，各轨道间距离 不变，迭代产生的点对应分岔点(即周期加倍的位置)[32]。

混沌的部分应用如下：

1 ．优化 利用混沌运动的随机性、遍历性和规律性寻找最优点，可用于 系统辨识、最优参数设计等众多方面。

2 ．神经网络 将混沌与神经网络相融合，使神经网络由最初的混沌状态 逐渐退化到一般神经网络，利用中间过程混沌状态的动力学特性使神经网络逃 离局部极小点，从而保证全局最优，可用于联想记忆、机器人的路径规划等。

3 ．图像数据压缩 把复杂的图像数据用一组能产生混沌吸引子的简单动 力学方程代替，这样只需记忆存储这一组动力学方程组的参数，其数据量比原

- 24 -

中国知网 https:Www  cnknet

始图像数据大大减少，从而实现了图像数据压缩。

4 ．高速检索 利用混沌的遍历性可以进行检索，即在改变初值的同时， 将要检索的数据和刚进入混沌状态的值相比较，检索出接近于待检索数据的状 态。这种方法比随机检索或遗传算法具有更高的检索速度。

5 ．非线性时间序列的预测 任何一个时间序列都可以看成是一个由非线 性机制确定的输入输出系统，如果不规则的运动现象是一种混沌现象，则通过 利用混沌现象的决策论非线性技术就能高精度地进行短期预测。

6 ．模式识别 利用混沌轨迹对初始条件的敏感性，有可能使系统识别出 只有微小区别的不同模式。

7 ．故障诊断 根据由时间序列再构成的吸引子的集合特征和采样时间序 列数据相比较，可以进行故障诊断。

8 ．混沌保密通信 利用混沌信号的编码和解码技术实现混沌信号的保密 通讯。此研究己经列入了美国国防的研究计划并正在加紧研制中。

9 ．混沌加密 利用混沌序列的非周期性和伪随机特性，将混沌序列作为 密钥流和原始明文序列进行逐位异或而得到加密密文[33]。

由上面的应用可以看出，人们着重研究了系统如何以有序到新的混沌以及 混沌的性质和特点，并进入应用阶段。90 年代以来，混沌理论与其它学科相互 交错、相互渗透、相互促进，综合发展，形成许多新的研究分支，混沌密码学 就是其中重要应用之一。

3.1.2 Logistic 混沌加密二值图像水印序列的生成

一类非常简单却被广泛研究的混沌动力系统是 Logistic 映射，定义如下：

*xk* +1 = *μxk* (1− *xk* ) (3-2) 其 中 1 ≤ *μ* ≤ 4 ， *xk* ∈ (0,1) 。 混 沌 动 力 系 统 的 研 究 工 作 指 出 ， 当 3.5699456 < *μ* ≤ 4 时，logistic 映射工作处于混沌态。

当 *μ* =4 时，Logistic 映射为*xk* +1 = 4*xk* (1− *xk* ) ，等价于：

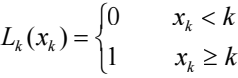
*xk* +1 =  . *kx*. (3-3)

该映射具有 0 均值，自相关及互相关为 0 的特性，而且所产生的混沌序列是非 周期且长度无限的实数序列，只需要截取合适的长度，进而生成二值序列作为 加密序列[34] 。由实值序列生成二值序列的方法有很多种，本文采用阈值门限

- 25 -

中国知网 https:Www  cnknet

法，公式如下:

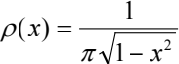
 (3-4)

其中在本文中 *k* 取值为0.5，当 *xk* < 0.5 时取 0，否则取 1。

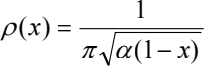
Logistic 映射在区间(－1 ，l)上定义，其形式如下：

*xk* +1 = 1− *μx* (3-5)

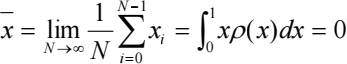
其中 *μ* ∈[0,2] 。若选择参数 *μ* 限制在 [0,2]区间内，则(3-5) 式是从线段 *I* = [−1,1]到它本身的一个非线性映射。当*μ* 逐渐增大时，迭代出现多次突变。 当0 < *μ* < 0.75000 时迭代为稳定的 1 点周期；当 *μ* 增大到 0.75000 时，迭代出 现 2 点周期分岔；当 *μ* 增大到 1.25000 时，出现 4 点周期分岔，这种2*n* 倍周期 分岔随 *μ* 的增大愈来愈快。当 *μ* → *μ*∞ = 1.40115 时，迅速达到周期 *N* → ∞ , 即进入了混沌状态，且混沌序列的概率分布密度函数为：

 −1 < *x* < 1 (3-6)

对于(3-2)式的 Logistic 映射，如果 *μ*=4，概率分布密度函数可以改写为：

 0 < *x* < 1 (3-7)

通过 *ρ*(*x*) ，我们很容易地得到 Logistic 映射所产生的混沌序列中一些很有意义 的统计特性。如 *x* 的时间平均即混沌序列轨迹点的均值是：



关于相关函数，独立选取 2 个初始值*x*0 和*y*0 ，则序列的互相关函数为：



(3-8)

(3-9)

Logistic 序列的以上特性表明：混沌动力系统具有确定性，其遍历统计特 性相当于白噪声，因而可以应用于包括数字通讯和多媒体数据安全等众多应用 领域[35]。其优势可以总结如下：

1 ．形式简单，只要混沌映射的参数和初始条件就可以方便的生成，复制 混沌序列。我们不必浪费空间来存储很长的整个序列。

2 ．初始条件的敏感性， 一般不同的初始值，即使相当接近，迭代出来的

- 26 -

中国知网 https:Www  cnknet

轨迹都不相同。同时，混沌动力系统具有确定性，给定相同的初始值，其相应 的轨迹肯定相同。我们可以轻而易举地获得数量极多的非相关的混沌序列，而 且一般情况下，很难从一般有限长度的序列来推断混沌序列的初始条件。

3 ．具有白噪声的统计特性，可以用于需要白噪声调制的众多场合[36]。

根据以上所述，应用 Logistic 混沌序列对原始水印数据进行加密，只需设 定混沌映射的参数和初始条件就可以方便的实现，同时还具有加密后视觉不可 见性良好以及鲁棒性良好的优点。

待加密的水印*W* 是大小为*M*1 × *M*2 ( *M*1 × *M*2 = *N*1 × *N*2 / 8 × 8 )的二值图像， 每个像素为 0 、1 两种取值。二值图像水印*W* 在嵌入原始载体图像之前，首先 用混沌序列进行加密。加密过程如图 3-1 所示，具体步骤描述如下：

第一步，将二维水印*W* 转换为一维向量*Wa* ( *α* = 1,2,..., *M*1 × *M*2 )的形式；

第二步，设定一个混沌初值*x*0 ，按公式(3-3)进行迭代，得到混沌序列*xk* ， 再按公式(3-4)进行阈值门限法得到 0-1 序列*Lk* (*k* =1,2, … , *M*1 × *M*2 )；

第三步，用生成的 0-1 序列*Lk* 对二值水印图像进行加密，得到加密后的水 印向量序列 *Wm* = *Wa* 田 *Lk* (*m=* 1,2, *… M*1 × *M*2 ) ，田 在这里表示异或运算。混沌 初值*x*0 即为用户的私有密钥 *K*。

随机序 列*xk*

初值 *x*0

混沌迭代

阈值门限法

二值序 列*Lk*

|  |
| --- |
| 二值图象水印  *W* |

|  |
| --- |
| 一维向量  *Wa* |

|  |
| --- |
| 田 |

转化

异或

|  |
| --- |
| 加密的  水印向量 *Wm* |

图 3-1 二值图像水印加密示意图

Fig.3-1 Block diagram of binary image watermarking encryption

3.1.3 实验结果及分析

根据上节阐述的 Logistic 映射加密原理及加密步骤，下面对 256 × 256 的对 原始二值水印图像“哈尔滨理工大学”，如图 3-2 所示，进行混沌加密实验。

- 27 -

中国知网 https:Www  cnknet

|  |
| --- |
|  |

图 3-2 原始二值水印

Fig.3-2 Original binary watermark

在该实验中 *μ* =4，初值 x0=0.7，按照上面所述的加密步骤，进行 Logistic 映射变换后，得到加密之后的图像，如图 3-3 所示。



图 3-3 混沌加密后的二值水印

Fig.3-3 Binary watermark after chaotic encryption

对二值图像数字水印的解密过程是加密过程的逆过程。根据密钥初值*x*0 得 出二值序列*Lk* ，将加密后的水印向量 *Wm* 与*Lk* 进行异或运算，即可以根据一 维向量 *Wa* 得出原始二值图象水印 *W*。

通过实验结果不难看出：二值图像数字水印经过混沌加密后，去除了水印 数据的相关性，增强了水印的秘密性，保证了原始二值图像水印数据具有视觉 的不可见性。经过以上处理的二值图像水印，同时具有初值敏感性和不可逆 性，也即在不知道确切的初值(密钥)的情况下，即使提取出水印信号也无法恢 复出水印图像，从而提高了整个水印系统的安全性。

3.2 二值图像水印位置置乱加密

3.2.1 位置置乱变换的原理

位置置乱技术是随着信息安全与保密技术的发展而发展起来的图像加密技 术。将该技术用于图像水印中，可以使非法使用者无法破译图像的内容，从而 达到提高数字水印的鲁棒性的目的。

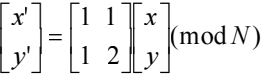
- 28 -

中国知网 https:Www  cnknet

位置置乱中的 Arnold 变换是一种基于图像像素点坐标的空间域变换的加 密方法，是通过 Arnold 变换将原始图像的像素点重新分布，使原始图像变得 杂乱无章，从而达到加密的效果[37]。将 Arnold 的二维变换(即 Arnold cat 变换) 应用到数字图像上，可以通过像素坐标的改变而改变图像像素点的布局，若将 数字图像视为一个矩阵，经 Arnold cat 变换后的图像会变得“混乱不堪”，即可 以应用 Arnold cat 变换实现每个象素点位置的一一置乱，并根据对其中参数以 及迭代次数的保密，达到的加密的效果。但继续使用 Arnold cat 变换，会出现 一幅与原图相同的图像，即 Arnold cat 变换具有周期性。本文就是采用 Arnold cat 变换，对已经经过混沌加密的二值图像数字水印数据进行置乱，从而实现 对水印数据的二次加密的目的。

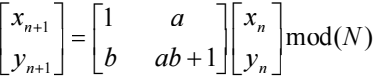
Arnold 变换的定义如下：

设正方形上的某点坐标为(*x*, *y*) ，将坐标点 (*x*, *y*) 变换到另一点(*x*' , *y*') 的变 换为：

 (3-10)

其中 *N* 为正方形的边长。

二维 Arnold 变换又被称为 Arnold cat 变换，其表达式如式(3-11)所示：

 (3-11)

其中 *xn* , *yn* 表示一个 *N*× *N* 图像的原始图像像素点位置，*xn*+1, *yn*+1 表示置乱之 后像素点的位置。*a* 、*b* 是系统的参数，取正整数[38]。公式(3-11)可以通过迭代 把一幅图像的位置进行一对一的换位，从而实现加密的目的。

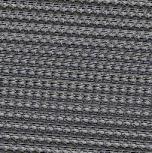
由于 cat 映射具有周期性，周期取决于置乱的参数和次数，而置乱参数和 置乱次数的选择只要根据置乱效果选择适当的整数就可以。这样就可以利用其 周期性进行解密，即对加密后的数据继续进行若干次的 Arnold cat 变换，即可 得到被加密的原始数据。

3.2.2 实验结果及分析

应用 Arnold cat 映射，对 256×256 的灰度图像 Lena 进行位置置乱实验。 令(3-11)式中 *a*=8 ，*b*=14，图 3-4 分别是原始图像经过置乱 1 次、2 次、10 次、 20 次和 128 次所得到的图像。

- 29 -

中国知网 https:Www  cnknet





a)原始图像 b) 经过 1 次置乱 c)经过 2 次置乱

a) Original image b) After one time scrambled c) After 2 time scrambled



d)经过 10 次置乱 e)经过 20 次置乱 f)经过 128 次置乱

d) After 10 times scrambled e) After 20 times scrambled f) After 128 times scrambled

图 3-4 对 Lena 进行位置置乱效果图

Fig. 3-4 The effect picture of scrambling transformation for lena

从图中可以看出，置乱 1 次、2 次和 20 次的图像有明显的条纹，说明条纹 比较集中的地方具有相同或相近的像素值。置乱 10 次的效果要好于置乱 20 次，说明置乱次数并不是越多越好。置乱 128 次还原回原始图像，说明 Arnold cat 映射具有一定的周期性（参数 *a 、b* 不同，周期也不一样），即可以通过不 同图片的置乱周期实现对置乱后的数据解密的目的。

下面对图 3-2 混沌加密后的二值水印进行位置置乱。公式(3-11)中当 *a*=8 、 *b*=14 时，迭代 23 次，对经过 Logistic 映射加密之后的图像进行 Arnold cat 置 乱，效果如图 3-5 所示：

- 30 -

中国知网 https:Www  cnknet



图 3-5 经过位置置乱后的二值水印

Fig.3-5 Binary watermark after position scrambled

从图中可以看出该方法有很 好的置乱效果，进一步提高了水印信息的不 可见性，加强了水印的保密性，更好地提高了整个水印系统的安全性。

3.3 本章小结

本章介绍了混沌系统的概念和特性，详细介绍了经过混沌加密的二值图像 数字水印序列的生成方法，在此基础上，又介绍了对经过混沌的加密的水印图 像进行 Arnold cat变换置乱，以便应用于后面的数字水印算法，为后面 DCT 域 图像数字水印技术的嵌入做准备。

- 31 -

中国知网 https:Www  cnknet

第4章 DCT 域二值图像数字水印算法

本章根据第一、二章的基础知识和第三章介绍的应用混沌及位置置乱理论 对水印进行加密，提出一种基于混沌和置乱加密的 DCT 域图像数字水印算 法，该算法利用混沌序列特有的性质，将含有版权信息的二值图像水印用混沌 序列进行加密，然后将不同强度的水印分量自适应地嵌入到不同图像块 DCT 域中去。通过加入高斯噪声、椒盐噪声以及 JPEG 压缩和剪切等处理操作，结 果表明了该算法具有很好的视觉掩蔽特性和鲁棒性

4.1 离散余弦变换（DCT）的原理

4.1.1 DCT 变换的原理

在现代图像处理技术中，我们通常用到的变换有 DFT ，DCT，沃尔什--哈 达玛变化(WHT)，主成分变换(K-L)等等，这里所说的图像变换指二维正交变 换，它们在图像处理中扮演着重要的角色。如傅立叶变换后平均值正比于图像 灰度的平均值，高频分量指示图像中目标的边缘信息，利用这些性质可以从图 像中抽取特征。又如在变换域中，图像能量往往集中在少数项上，或者说能量 主要集中在低频分量上，这时对低频成分分配较多的比特数，对高频成分分配 较少的比特数，即可实现图像数据的压缩编码。再者，舍弃变换系数矩阵中某 些幅度小的系数，可缩减计算维数，提高计算的速度[39]。

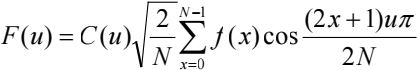
在理论上来说，K-L 变换是图像变换中具有最佳性质的一种，作为标准用 来衡量其它变换性能的好坏，因为它能完全消除子像块内像素间的线性相关 性，经 K-L 变换后各变换系数在统计上不相关，其协方差矩阵为对角阵，因而 大大减少了原数据的冗余度。如果丢弃特征值较小的一些变换系数，那么，所 造成的均方误差是所有正交变换中最小的。但是由于 K-L 变换是取原图各子块 协方差的特征向量作为变换后的基向量，因此 K-L 变换的变换基是不固定的， 使用起来很不方便，一般只将它作为理论上的比较标准，实际上用得最多的还 是 DCT，它的性能最接近 K-L 变换，而 DFT 和 WHT 要差一些。离散余弦变 换是最小均方误差条件下得出的较优的正交变换，由于离散傅立叶变换要对 n 点像素(对一维来讲)做周期延拓，故一般在周期间的接点处会引入一个突变， 这意味着将导致较大的高频系数，即能量不能充分集中于低频部分。而离散余

- 32 -

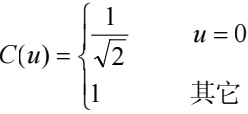
中国知网 https:Www  cnknet

弦变换相当于做 2n 点的离散傅立叶变换，它先将原 n 点像素做偶对称扩展后 再做周期延拓，因此边界处没有突跳，能量可更集中。另外，它有固定基，它 的性能最接近 K-L 变换，因而它是变换法的主流，现有的三个国际编码标准都 选中了 DCT[40]。

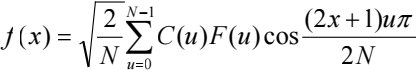
一维 DCT 的定义如下：设{*f*(*x*) *x* = 0,..., *N* −1}为信号序列集合，其离散余 弦的正变换定义为：

 (4-1)

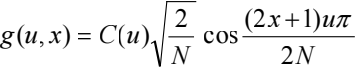
式中，*x* = 0,..., *N* −1 ，*u* = 0,..., *N* −1 。 其中

 (4-2)

其逆变换定义为：

 (4-3)

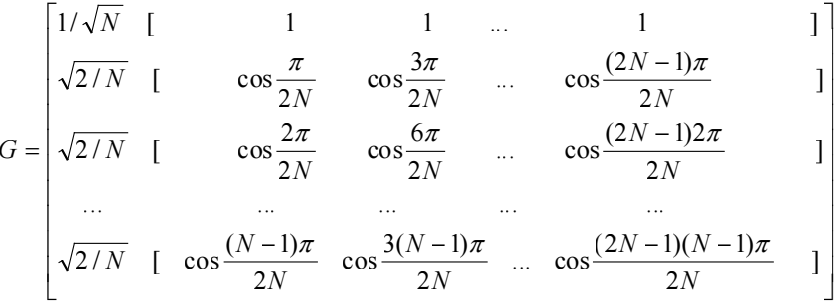
式中，*x* = 0,..., *N* −1 ; *u* = 0,..., *N* −1 。 可见一维 DCT 的正反变换核都是

 (4-4)

将变换式展开整理后，可以写成矩阵形式：

*F=G f* (4-5)

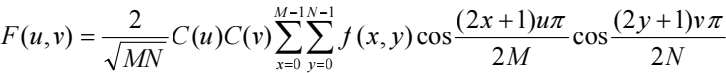
其中



将一维离散余弦 DCT 变换的定义推广到二维离散余弦 DCT 变换，设 {*f* (*x*, *y*) *x* = 0,..., *M* −1; *y* = 0,..., *N* −1}为二维图像信号序列集合，其正变换为：

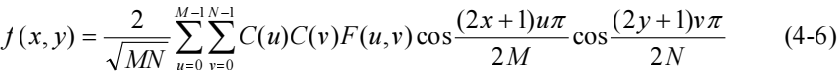
- 33 -

中国知网 https:Www  cnknet



其中 C(*u*) , C(*v*) 的定义同前；

*x* = 0,..., *M* −1; *y* = 0,..., *N* −1;*u* = 0,..., *M* −1;*v* = 0,..., *N* −1。 二维 DCT 的逆变换为：



其中 *x* = 0,..., *M* −1; *y* = 0,..., *N* −1;*u* = 0,..., *M* −1;*v* = 0,..., *N* −1。

二维 DCT 是目前最常用的有损数字图像压缩系统——JPEG 的“核心 ”， 因此 DCT 域的数字水印受到了广泛的重视[41]。

4.1.2 DCT 变换系数的选择

DCT 域水印算法是将图像进行 DCT 变换，选择某些变换后的 DCT 系数进 行小幅度的改动，从而实现水印信号的嵌入。变动不同的 DCT 系数对水印系 统的整体性能有着不同的影响。

数字水印的两个最基本的要求是：1 ．水印的不可见性；2 ．水印要具有一 定的抗攻击能力，即嵌入水印的图像在经过一般的图像处理后，图像中的水印 应该继续存在[42]。这两个要求直接影响到水印嵌入的系数的选择。

一方面，一般的图像处理均发生在图像频谱的高频区域中，例如对图像进 行 JPEG 压缩，它保留了图像的低频信号，而将一部分的高频信号滤掉。如果 水印嵌入在高频，虽然其不可见性效果很好，但水印经过图像处理后容易被删 除，其鲁棒性差，因此变换域的水印算法不能将水印信号嵌入到图像的高频区 域中。

另一方面，图像的主要能量集中在它的低频系数上，低频系数直接影响到 人眼的视觉效果[43] 。在低频系数中嵌入水印信号，由于低频系数携带了图像的 大部分的能量，图像受到攻击时，攻击者一般要保证图像的质量不能下降得太 厉害，这样大部分的低频系数仍然保留，嵌入它们的水印信号因此存活下来， 这样能够保证水印的鲁棒性。但是在嵌入的过程中要修改低频系数，对图像重 要信息会造成破坏，就会降低图片的视觉效果。

所以本文采用折中的办法：选择中频系数，寻求不可见性与鲁棒性的兼 顾。本文选取 DCT 中频作为水印嵌入区域，问题就简化为如何在水印的不可 见性与鲁棒性平衡的情况下，把水印嵌入到图像的中频系数中。

- 34 -

中国知网 https:Www  cnknet

4.1.3 基于人类视觉系统的块分类方法

人类视觉系统 HVS(Human Visual System)对图像所具有的频率掩盖、亮度 掩蔽和对比度掩蔽等特性表明：背景亮度越亮，纹理越复杂，人类视觉对其轻 微变化就越不敏感，只要嵌入水印信号低于 HVS 的对比度门限(CST：Contrast Sensitivity Threshold) ，HVS 就无法感知到信号的存在。它具有如下三个特性： 1 ．人眼对不同灰度具有不同的敏感性， 通常对中等灰度最敏感，而且向低灰 度和高灰度两个方向非线性下降； 2 ．对图像平滑区的噪声敏感，而对纹理区 的噪声不敏感；3 ．边缘信息对于人眼非常重要，必须保护边缘的质量不受大 的损害[44]-[46]。因此，可以利用 HVS 特性选取不同的嵌入强度因子以获得更好 的视觉掩蔽性。

根据上述特性，把 DCT 块分成 5 类，使本章水印算法具有更好的视觉不 可见性和鲁棒性。分类方法描述如下：

设原始载体图像*I*(*i*, *j*)(1 ≤ *i* ≤ *N*1,1 ≤ *j* ≤ *N*2 ) 为*N*1 × *N*2 个像素大小，每个像 素为 0-255 灰度等级的灰度图像。首先将 *I* 分割成互不重叠的 8 × 8 的子块 *In* (*i*, *j*) ，*B* 为原始载体图像所分的块数，且满足 *B=*(( *N*1 × *N*2 )/(8× 8))；然后对 每一个子块*In* (*i*, *j*) 进行 DCT 变换，得到*In* (*u*, *v*) ，最后计算每个子块的灰度(或 者亮度)的均值和方差，并以此作为块分类的依据；均值较小的块对应图像的 平滑区域，均值较大的块则可能是纹理区域或者边缘，其中纹理区域的方差较 小而边界区域的方差较大。按上述方法可将所有图像块分为五类：第一类是亮 度较低，纹理简单，HVS 对像素值的改变较为敏感，所嵌入的水印分量强度 最小；第二类亮度中等，纹理中等，嵌入的水印分量强度较小；第三类亮度较 高、纹理复杂，且不是边缘， HVS 对像素值的改变的敏感性最弱，叠加的水 印分量最大；第五类亮度较高，纹理复杂，且是边缘， HVS 对其中像素值的 改变的敏感性较强，叠加的水印分量较小；其余为第五类[47]。

4.2 二值图像水印的嵌入方案

前文已经为水印的嵌入做了细致的准备工作，包括： 1 ．对原始水印信息 进行混沌加密；2 ．对混沌加密后的水印信息进行置乱，实现二次加密；3 ．选 择适当的 DCT 嵌入系数，在水印信息嵌入的不可见性和鲁棒性之间寻求平 衡；4 ．根据人眼视觉系统特性，将原始图像块分成五类，以保证寻求水印嵌 入的不可见性的前提下兼顾水印的鲁棒性。

- 35 -

中国知网 https:Www  cnknet

下面介绍水印的嵌入方案。

水印嵌入过程由以下五个的基本步骤组成，如图 4-1，具体描述如下：

原始水 印数据

加密的水 印向量 *Wm*

|  |
| --- |
| 原始图 像 *I* |

|  |
| --- |
| 水印嵌 入算法 |

|  |  |
| --- | --- |
|  | 块分类选 取不同 α |

|  |
| --- |
| DCT，计  算均值、 方差 |

经过二次加 密的水印

|  |
| --- |
| IDCT，得  到嵌有水印  图像*I*' |

图 4-1 水印嵌入框图

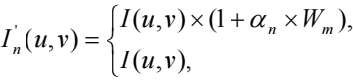
Fig.4-1 Block diagram of embedded watermarking

第一步，把原始图像*I*(*i*, *j*)(1 ≤ *i* ≤ *N*1,1 ≤ *j* ≤ *N*2 ) 分成 8 × 8 大小不重叠的子 块，对每个子块进行 DCT 变换，并计算每个子块的方差和均值，然后根据这 些值对图像块进行分类，确定嵌入强度因子*α* 。

第 二 步 ， 是 把 原 始 的 具 有 版 权 信 息 的 二 值 数 字 水 印 图 像 *W*(*u*, *v*) (1 ≤ *u* ≤ *M*1 ,1 ≤ *v* ≤ *M*2 , *M*1 \* *M*2 = *N*1 \* *N*2 / 8\*8) 的系数矩阵变换成一个 长为*M*1 \**M*2 的 *Wm* 向量，用公式(3-3)产生一个混沌密码序列，截取合适的长 度，本文取序列长度为 2000，并按公式(3-4)阈值门限法将它转化为 0-1 序列 *Lk* (1 ≤ *k* ≤ *M*1 \* *M*2 ) ，利用序列 *Lk* 对水印图像进行加密，得到加密序列 *Wm* = *Wa* 田 *Lk* ，田 表示异或运算。

第三步，用公式(3-11)对经过混沌加密的二值图像数字水印进行位置置乱 变换，置乱 23 次，置乱参数取 *a*=8 、*b*=14，实现对水印信息的二次加密。

第四步，对 DCT 系数进行分类，选取 2000 个中频系数，并采用式(4-7)将 加密序列*Wm* 嵌入到原始图像的 DCT 中频系数中：



[*u*, *v*] ∈ [4,1][2,3] 其它

(4-7)

其中 *αn* 是块分类后不同种类块的嵌入强度因子。

第五步，对每块进行离散余弦反变换(IDCT)，得到嵌有水印的图像*I*' 。

- 36 -

中国知网 https:Www  cnknet

4.3 二值图像水印的提取方案

由于本章水印算法在提取水印时需要原始载体图像，故水印为非盲水印， 水印提取过程与水印嵌入的过程刚好相反，如图 4-2，具体步骤描述如下：

初值 *x*0



|  |
| --- |
| 提取出二值 水印 *W*’ |

|  |
| --- |
| 水印向 量*Wa*' |

经过位置  置乱

产生混沌序 列，得到*Lk*

|  |
| --- |
| 田 |

|  |
| --- |
| 提取出的密 码序列*Wm*' |

|  |
| --- |
| 嵌有水  印的图  像 *I*’ |

|  |
| --- |
| DCT，计  算均值、 方差 |

|  |
| --- |
| 水印提 取算法 |

|  |
| --- |
| 原始图像 *I*  经 DCT 变  换 |

|  |
| --- |
| 块分类， 选取不同  α |

图 4-2 水印提取框图

Fig.4-2 Block diagram of extracted watermarking

首先把嵌有水印的图像*I*'和原始载体图像*I* 进行 8 × 8 的分块，对每一块进 行 DCT 变换，计算水印图像*I*'每个 DCT 块的亮度均值和方差，根据所得的方 差和均值对嵌有水印图像 *I’*进行块分类，然后按照公式(4-8)，提取加密的水印 向量：

*Wm*' = (*In*' (*u*, *v*) / *In* (*u*, *v*) −1) /*αn* ， [*u*, *v*] ∈ [4,1][2,3] (4-8)

其次把提取的向量*Wm* ' ，利用 Arnold cat 变换的周期性进行第一次解密， 得 到 *Wa* ' ； 再 利 用 混 沌 密 钥 进 行 解 密 ， 得 到 二 次 解 密 的 水 印 序 列 *Wa* ' ' = *Wa* '田*Lk* 。

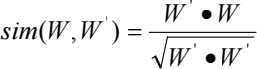
最后将*Wm* ' 转化为 2-D 的形式，得到提取出的二值水印图像*W*' 。

- 37 -

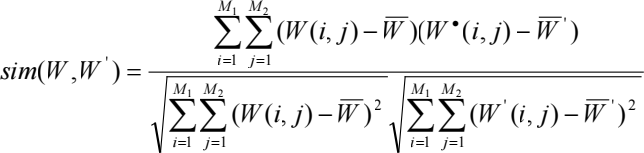
中国知网 https:Www  cnknet

计算原始混沌水印与提取出的混沌水印的相似度。设置 一个阈值 (threshold)*T*，当 *sim*(*W*, *W*' ) 大于阈值时，可判断测试图像中含有水印，反之， 则可说明不存在水印。

在本论文中用归一化相关性来比较提取出的水印与原始水印的相似度，公 式如下：

 (4-9)

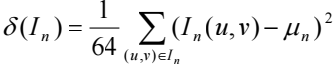
或

 (4-10)

式中，*W* 表示原始水印信息， *W*' 表示提取的水印信息， • 表示内积， *W* 是向 量*W* 的均值，*W* ' 是向量*W*' 的均值[48]。

4.4 实验结果和分析

在实验中，混沌序列的初值设为 0.7。按如下公式确定子块的方差：

 (4-11)

其中 *μn* 为第 *n* 块*In* 的平均灰度(亮度) ，*δ*(*In* ) 为第 *n* 块*In* 的 DCT 系数(直流系 数除外)的方差，设四个阈值*T*1 、*T*2 ( *T*1 <*T*2 ) ，*S*1 、*S*2 ( *S*1 < *S*2 )；如果 *μn* <*T*1 ，认 为亮度较低，纹理简单，则是第一类；如果*T*1 *< μn < T*2 ，且 *S*1 < *δ*(*In* ) < *S*2 ，认 为亮度中等，纹理中等，则是第二类；如果 *μn >T*2 ，且*δ*(*In* ) < *S*1 ，认为亮度较 高，分类复杂，且不是边缘, 则是第三类；如果 *μn > T*2 ，且 *δ*(*In* ) > *S*2 亮度较 高，纹理复杂，且是边缘，则是第四类；其余的为第五类。实验中四个阈值 *T*1 、*T*2 、*S*1 、*S*2 分别取 600 、1200 、500000 、1500000。

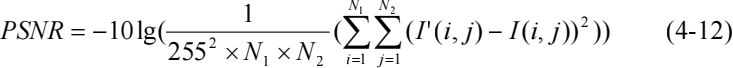
根据上面分类的结果选取不同的水印嵌入强度因子 *a* ，*a* 决定水印的嵌入 深度，*a* 越大嵌入的水印越深，水印的鲁棒性越好，可见性越差，即水印图像 有明显的失真，产生块效应，也就没有什么使用价值了，如果嵌入强度因子 *a*

- 38 -

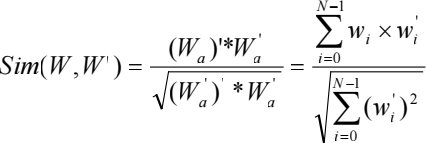
中国知网 https:Www  cnknet

过小，虽然此时的嵌有水印的图像和原始公开图像相似度非常高，但水印的鲁 棒性很差，在经历一些图像处理时容易被去掉，故在实验中五类块的 *a* 分别取 值为 0.01 、0.1 、0.6 、0.1 、0.1。

为了能更好的客观地衡量图像质量和判断水印是否存在，本章分别用峰值 信噪比和相似度来评价它们，在这里我们用相关系数来衡量相似度。嵌入水印 图像*I*'相对原始载体图像*I* 的峰值信噪比 *PSNR*(Peak signal-to-noise ration)：



提取的水印*Wm* ' 相对原始水印*W* 的相似度(Similarity)：

 (4-13)

公式中*Wa* 是原始水印 *W* 一维向量矩阵，(*Wa* )' 是矩阵*Wm* 的转置，*Wa* ' 是提取水 印*W* ' 的一维向量矩阵， (*Wa*' )' 是矩阵*Wa* ' 的转置，\*是矩阵乘法， *wi* 是矩阵*Wa* 中的元素(*i* = 0 *N* −1) ，*wi*' 是矩阵*Wa*' 的元素(*i* = 0 *N* −1) 。

以上只是两个客观指标，可作为判断水印嵌入的参照，实际应用中还要结 合主观视觉效果来衡量。

实验采用原始载体图像为 512 × 512 的标准灰度测试图像，原始水印是 48 × 48 的二值图像，如图 4-3—图 4-16 所示，是一组水印嵌入和提取的实验效 果图片。

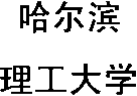


图 4-3 原始图像 图 4-4 原始二值水印

Fig. 4-3 Original image Fig. 4-4 Original birary watermark

- 39 -

中国知网 https:Www  cnknet

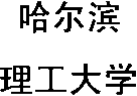


图4-5 嵌有水印的图像 图4-6 从图4-5中提取的水印

Fig. 4-5 Embedded watermark image Fig. 4-6 Extracted watermark from 4-5

图 4-5 是嵌有水印的图像，从视觉上来看，原始图像和嵌有水印的图像几 乎是区别不开来的，峰值信噪比为 49.227，也即本文的水印具有很好信息隐藏 效果，并且可以无失真的提取出二值图像水印，如图 4-6。在本章实验检测器 输出的曲线中，嵌入二值水印图像加密序列处的峰值为 43.023，而其他处的检 测响应很小，说明嵌有水印的图像中含有水印。从图 4-7 到图 4-16 中可以得到 以下结论：

1 ．抗噪声 图 4-7—图4-10 证实了水印抵抗高斯和椒盐噪声的能力。虽 然加了噪声的水印的图像与原始图像相比较，图像质量有所下降，峰值信噪比 分别为 *PSNR*=29.75 和 *PSNR*=26.265，但可以提取出二值图像水印，检测器的 响应也很强。说明了该算法具有较好的抗噪性能。

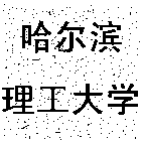


图 4-7 加入高斯噪声的图像 图 4-8 从图 4-7 中提取的水印

Fig. 4-7 Image after average Gaussian Noise Fig. 4-8 Extracted watermark from 4-7

- 40 -

中国知网 https:Www  cnknet

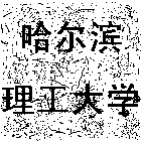


图 4-9 加入椒盐噪声的图像 图 4-10 从图 4-9 中提取的水印

Fig. 4-9 Image after Adding Salt&Pepper Noise Fig. 4-10 Extracted watermark from 4-9

2 ．均值滤波 图 4-11—图 4-12 是对嵌有水印图像进行均值滤波测试的结 果，从视觉上来看，图像依然很清晰，峰值信噪比为 *PSNR*=38.054，检测器的 输出也很高为 36.376，提取出的二值图像水印可识别，从而证明水印具有比较 好的抗均值滤波能力。



图 4-11 均值滤波的图像 图 4-12 从图 4-11 中提取的水印

Fig. 4-11 Image after Mean value filtering Fig. 4-12 Extracted watermark from 4-11

3 ．抗剪切 图 4-13—图4-14 是对嵌有水印的图像进行 20%剪切得到的测 试结果，虽然图像的质量有明显下降，峰值信噪比为 *PSNR*=13.745，但能提取 和检测到水印图像。说明该算法具有较强的抗剪切能力。

- 41 -

中国知网 https:Www  cnknet





图 4-13 20%剪切后的图像 图 4-14 从图 4-13 中提取的水印

Fig. 4-13 Image after Cropping 20% Fig. 4-14 Extracted watermark from 4-13

4 ．抗 **JPEG** 压缩 图 4-15—图 4-16 是对嵌有水印的图像进行 30%JPEG 压缩的测试图，可以看出压缩后的图像和原始图像在视觉上的降质并不是很 大，峰值信噪比为 *PSNR*=13.745，且能提取出较好质量的二值图像水印，检测 器还有较强的响应，输出值为 38.212，可见本章的算法的抗 JPEG 压缩性能较 好，即水印的稳健性较好。

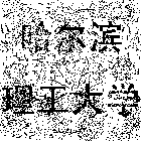


图 4-15 30%JPEG 压缩图像 图 4-16 从图 4-15 中提取的水印

Fig. 4-15 Image after 30% JPEG Compression Fig.4-16 Extracted watermark from 4-15

如图 4-17—图 4-24 所示，是另一组对比实验图像，在这组实验中增强了 对嵌入水印的图像的干扰。所选取的水印图像与上一组实验相同，为“哈尔滨 理工大学”。通过对嵌入相同水印、经过同类但不同强度的干扰后，所提取的

- 42 -

中国知网 https:Www  cnknet



图 4-17 原始图象 图 4-18 嵌入水印的图像

Fig. 4-17 Original image Fig. 4-18 Embedded watermark imag

水印进行对比，可以更好地说明该算法的特点。这组图片选择了对嵌入水印后 的图象进行了加入加强的高斯噪声，进行 50%JPEG 压缩以及 40%的剪切之 后，提取出的水印图像与上一组实验做对比。



图 4-19 加入高斯噪声的图像 图 4-20 从图 4-19 中提取的水印

Fig. 4-19Image after adding Gaussian Noise Fig. 4-20Extracted watermark from 4-19

- 43 -

中国知网 https:Www  cnknet



图 4-21 50%JPEG 压缩图像 *PSNR*=40.621

Fig. 4-21 Image after 50% JPEG compression

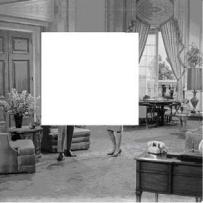


图 4-23 40%剪切后的图像 *PSNR*=12. 475

Fig. 4-23 Image after Cropping 40%

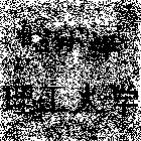


图 4-22 从图 4-21 中提取的水印

Fig. 4-22 Extracted watermark from 4-21

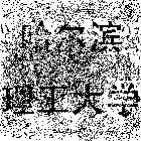


图 4-24 从图 4-23 中提取的水印

Fig. 4-24 Extracted watermark from 4-23

由这组实验图像可以看出：该算法有较好的抗噪性和抗剪切性，但是该算 法在经较高的 JPEG 压缩后，图像的降质很明显，而且所提取的水印可见性效 果不好，说明该算法经过 JPEG 压缩后鲁棒性还有待提高。

通过上面的分析，可以看出本章的混沌与置乱加密的图像数字水印算法具 有一定的抗攻击能力，特别是对噪声污染、 JPEG 压缩，以及均值滤波等均具 有较强的鲁棒性，嵌入的二值图像水印都能提取和检测出来，且提取出的二值 图像水印具有可辨别性。总结该算法优点如下：

1 ．利用了混沌系统以及位置置乱对具有版权信息的二值水印进行加密，

- 44 -

中国知网 https:Www  cnknet

使水印本身具有密码学意义下的双重安全性。

2 ．结合了人类视觉系统的掩蔽特性。在嵌入水印时利用了人类视觉系统 的亮度掩蔽性和纹理掩蔽特性，既保证了透明性又提高了水印的鲁棒性。

3 ．把原始图像块分成五类，自适应的把水印嵌入到 DCT 中频系数中，具 有很好的视觉不可见性。

4 ．能够经受住添加高斯噪声、椒盐噪声、低通滤波、图像裁剪以及 JPEG 压缩等方式的攻击。

上面这些优点还可以通过与 DCT 域未经改进的同类方法对比得出。这里 选择未经加密的水印数据在 DCT 域低频进行嵌入的算法，所得到的嵌有水印 的图像，做为比较对象[49] 。进行与本章实验相同的图像处理操作，并对水印检 测器的输出响应进行比较，如表 4-1 所示。未经改进的 DCT 域同类方法所得 到嵌有水印图像在经过高斯噪声污染、椒盐噪声污染、图像剪切、 JPEG 压缩 时，检测器的输出分别为 21. 371 、18.792 、8.256 、42.342，而本章算法所得 到的嵌有水印图像在经过相同的处理时，检测器的输出分别为 28.256 、 38.848 、40. 269 、37.221，从这些值中可以发现本章算法嵌入的水印在抗高斯 噪声、椒盐噪声、图像剪切的效果显优于未经改进的算法。但本章算法的水印 抗 JPEG 有损压缩的能力较弱，这是本章算法有待改善的地方。

表4-1 水印算法的比较

Table 4-1 Comparison between different watermarking algorithms

|  |  |  |
| --- | --- | --- |
| 算法类型  图象处理操作 | 本章算法的输出 响应 | 未改进的  DCT 域算法  输出响应 |
| 0 ．1%高斯噪声 | 28.256 | 21.371 |
| 1%椒盐噪声 | 38.848 | 18.792 |
| 三分之一剪切 | 40.269 | 8.256 |
| 60%JPEG 压缩 | 37.221 | 42.342 |

- 45 -

中国知网 https:Www  cnknet

4.5 本章小结

本章在结合和改进前人算法的基础上，提出了一种具有较强鲁棒性的数字 水印算法，该算法将具有版权信息的水印本身进行了混沌加密和位置置乱，这 样水印攻击者即使获得水印数据，但由于不知道密钥及置乱次数而不能提取正 确的水印信息，从而为数字作品提供了双重保险；利用人类视觉系统(HVS)的 特性对图像 DCT 系数块进行分类，然后自适应地把加了密的二值图像水印嵌 入到 DCT 域的前两个中频系数上。实验表明，用该算法嵌入的水印可保证较 好的不可见性，同时对高斯和椒盐噪声、均值滤波、图像剪切、 JPEG 有损压 缩等水印攻击方法具有较好的鲁棒性。

- 46 -

中国知网 https:Www  cnknet

结论

本文认真比较几种典型的图像数字水印算法的优缺点，并在此基础上提出 了一种基于混沌与置乱加密的二值图像数字水印算法。

该算法首先利用混沌系统对初值敏感的依赖性的特性，实现了对具有版权 信息的二值图像水印数据进行加密处理；接着利用位置置乱方法，又对经过混 沌加密后的水印进行了置乱变换，从而实现了对原始水印信息的双重加密；再 结合人类视觉系统 HVS 的亮度和纹理掩蔽的特性对原始图像块分类后，将加 密过的水印数据自适应地嵌入到 DCT 中频系数中。该算法使水印数据本身具 有密码学意义下的双重安全性，保证了水印的隐蔽性，并提高了水印的鲁棒 性。通过一系列图像攻击实验表明， 该算法能够较好地经受诸如添加高斯噪 声、椒盐噪声、低通滤波、图像剪裁以及 JPEG 压缩等方式的攻击，在版权保 护和认证方面，具有很好的实用性。

但是，通过对比实验也可以看出，该算法在嵌入二值图像水印的信息量方 面没有突破；该算法在遭受较强的 JPEG 压缩的时候，鲁棒性并不理想，因此 在满足水印系统的隐蔽性和鲁棒性方面还有待进一步平衡。

- 47 -

中国知网 https:Www  cnknet

参考文献

[1] 王炳锡，陈琦，邓峰森．数字水印技术[M] ．西安：西安电子科技大学出 版社，2003 ：11 .

[2] Tirkel A.Z. Osborne C.F.A Digital Watermark[C]. First IEEE International Image Processing Conference, 1994: 86-90.

[3] Shi, B.Bhargava. Light-weight MPEG Video Encryption [C]. Proceedings of the ACM Multimedia96, 1996: 210-229.

[4] 黄继武．一种自适应图像水印算法[J] ． 自动化学报，1999 ，25(4) ：476- 482 .

[5] Cox I.J, Matt L Miller. A Review of Watermarking and the Importance of Perceptual Modeling[C]. SPIE Proceeding on Human Vision and Electronic Imaging, 1997: 92-99.

[6] 易开祥．数字图像加密与数字说技术研究[D] ．浙江：浙江大学（博士学 位论文），2001 ：103-110 .

[7] Cox I.J, Miller M.L. The First 50 Years of Electronic Watermarking[J]. EURASIP J. of Applide Signal Processing, 2002,2: 126-132.

[8] Pitas I. A Method for Signature Casting on Digital Images[J]. IEEE International Conference on Image Processing, 1996,3: 215-218.

[9] Schyndel R G van, Tirkel A.Z, Osborne C.F. A Digital Watermark[J]. First IEEE International Image Processing Conference, 2004, 2: 86-90.

[10] Matsuik,Tanaka K. Video-steganography[J]. How to Secretly Embed a Signature in a Picture. IMA Intellectual Property Project Proceedings, 1994, 1: 187-206

[11] Jayewardena A, Lenders P. Embedding Multi Resolution Binaryimages Into multi Resolution Watermark Channels in Wavelet domain[C]. Proceedings of the IEEE ECASSP00, 2000: 1983-1986.

[12] 罗大光等．一种基于图像最高位 MSB 的水印嵌入算法[J] ．计算机应用， 2005 ，24(12) ：88-89.

[13] 崔晓瑜．数字水印技术的研究[D] ．北京：北京大学（博士学位论文）， 2006 ：46-49 .

[14] Matsuik, Tanaka K. Video-steganography[J]. How to Secretly Embed a

- 48 -

中国知网 https:Www  cnknet

Signature in a Picture. IMA Intellectual Property Project Proceedings, 1994, 1: 187-206.

[15] 黄继武，YunQ. Shi，姚若河．基于块分类的自适应图像水印算法[J] ．中 国图像图形学报，1994 ，4 ：640-643 .

[16] 刘炎，施鹏飞．一种基于 HVS 的数字水印算法[J] ．计算机工程与应 用，2001 ，17 ：133-139 .

[17] 汪春生，程义民，王以孝．一种基于块分类的图像水印算法[J] ．微型机 与应用，2002 ，6 ：54-57 .

[18] Sviatoslav Voloshynovskiy, Oleksiy Koval, Kivanc M. The edge process model and its application to information hiding capacity analysis[C].IEEE Transactions on Signal Processing,2006,54(5):1813-1825.

[19] Chandramouli R, Subbalakshmi P. Current trends in steganalysis: a critical survey[C].Special Session on Image Forensics,2005,20(5):254-257.

[20] Hans Oltmans. Secure graphical data storage by full spectrum image coding. optical security and counterfeit deterrence techniques[C],IEEE Transactions on Signal Processing,2006,6075(5):60750A-1-60750A-13.

[21] 钟伟，余松煌，马希俊．基于分块 DCT 的自适应水印算法[J] ．红外与激 光工程，2000 ，29(5) ：22-26 .

[22] 刘锋．基于静态图像的数字水印技术的研究[D] ．杭州：杭州浙江工业大 学（硕士学位论文），2004 ：25-27 .

[23] Tsekeridon S, Pitas I. Embedding. Selg-Similar Watermarks in the Wavelet domain[C]. IEEE Int. Conf. On Acoustics: Systems and Signal Processing, 2007: 1967-1970.

[24] Hartung F, Girod B. Watermarking of Uncompressed and Compressed Video[J]. Signal Processing, 1998, 66(3): 283-301.

[25] Cox I.J, Miller M.L. Secure Spread Spectrum Watermarking for Multimedia[J]. IEEE Transactions on Image Processing, 1997, 6(12): 1673-1687.

[26] Tao B, Dickinson B. Adaptive Watermarking in the DCT Domain. International Conf. On Accoustics[J]. Speech and Signal Processing, 1997, 4: 2985~2988.

[27] 杨义先，钮心忻，任金强．信息安全新技术[M] ．北京:北京邮电大学出 版社，2002 ：45-76.

[28] 易开祥，石教英． 自适应二维数字水印系统[J] ．中国图像图形学报， 2001 ，6 ：444-449.

- 49 -

中国知网 https:Www  cnknet

[29] 张志明，王磊，郑应平， 一种基于混沌序列的时空域数字水印算法计算 机应用研究[J] ．2003 ，20(4) ：52-54 .

[30] 王慧琴，李人厚，王志雄．基于 DCT 域的加密二值图像数字水印新算法 [J] ．小型微型计算机系统，2003 ，24 ：103-106 .

[31] 王丽娜，杨景辉，张焕国，于戈．基于混沌与细胞自动机的数字水印模 式[J] ．电子学报，2006 ，32 ：580-582 .

[32] 吕金虎，陆君安，陈士华．混沌时间序列分析及其应用[M] ．武汉：武汉 大学出版社，2006 ：98-104 .

[33] 吴星升，王介生，刘慎权．图像的排列变换[J] ．计算机学报， 1998， 2l(6) ：514-519 .

[34] 易开祥，孙鑫，石教英．一种基于混沌序列的图像加密算法[J] ．计算机 辅助设计与图形学报，2000 ，12(9) ：672-676 .

[35] 王毅．基于混沌序列的图像加密研究[J] ．计算机工程与应用， 2002， 20 ：99-102 .

[36] 唐秋玲，覃团发，陈光旨．混沌图像加密[J] ．广西大学学报， 1999， 24(l) ：61-64 .

[37] 沈永增，刘锋，计建炳，王其聪．一种新的灰度水印嵌入算法[J] ．计算 机工程与应用，2005 ，4 ：56-57 .

[38] 刘瑞祯，谭铁牛．基于奇异值分解的数字图像水印方法[J] ．电子学报， 2001 ，2 ：88-95 .

[39] 丁玮，齐东旭．数字图像变换及信息隐藏与伪装技术[J] ．计算机学报， 2006 ，12(9) ：838-843 .

[40] 张志勇．精通 MATLAB 6.5 版[M] ．北京：北京航空航天大学出版社， 2003 ：28-32 .

[41] 齐东旭 ．分形及计算机生成[M] ．北京：北京科学出版社， 1994 ：59- 63 .

[42] 伯晓晨，沈林成，常文森．一种新的盲图像水印检测算法[J] ．计算机学 报，2001 ，24(12) ：1279-1286 .

[43] 王慧琴，李人厚，王志雄．基于混沌加密的频率域数字图像水印算法 [J] ．计算机应用研究，2002 ，l：71-73 .

[44] 汪春生，程义民，王以孝．一种基于块分类的图像水印算法[J] ．微型机 与应用，2002 ，6 ：54-57 .

[45] 茅耀斌，卓成春，王执锉，戴跃伟．一种基于人眼视觉特性的图像水印

- 50 -

中国知网 https:Www  cnknet

方案[J] ．厦门大学学报(自然科学版) ，2001 ，40(增刊)：232-235 .

[46] 蔡汉添，何军辉．一种基于 DCT 中频的图像水印技术[J] ．华南理工大学 学报(自然科学版) ，2001 ，29(12) ：57-60 .

[47] 齐东旭，邹建成 ．一类新的置乱变换及其在图像信息隐蔽中的应用 [J] ．中国科学(E 辑) ，2000 ，30(5) ：440-447 .

[48] 丁玮，闫伟齐，齐东旭．基于置乱与融合的数字图像隐藏技术及其应用 [J] ．中国图像图形学报，2000 ，5(A)(8) ：644-649 .

[49] 王慧琴，李人厚，王志雄．基于 DCT 域的加密二值图像数字水印新算法 [J] ．小型微型计算机系统，2003 ，19 ：71-73 .

- 51 -

中国知网 https:Www  cnknet

攻读学位期间发表的学术论文

[1] 张陶，于晓洋．基于混沌加密的 DCT 域二值图像数字水印算法[J] ．国外 电子测量技术，2008 ，3 ：(已录用) .

- 52 -

中国知网 https:Www  cnknet

致谢

在攻读硕士期间，从课程学习、论文选题到具体的研究工作，我都得到了 导师于晓洋教授的悉心指导和鼓励。于老师渊博的知识、严谨的治学态度以及 谦虚的为人使我受益匪浅，他也潜移默化地对我在学业、择业甚至面对生活的 态度方面都产生了积极而深远的影响。研究生期间，我所取得的每一点进步都 离不开于老师给我的指导和帮助。

我还要感谢张健老师，在我的论文写作过程中，张老师做了大量的指导工 作，为我提出了许多中肯而宝贵的意见，并给予了很大的耐心与支持，在未来 的日子里，我会一直默默地记在心中。

我还要对实验室的同学们以及寝室的朋友表示感谢，在共同的学习与生活 中我们互相帮助、彼此鼓励，度过了愉快的研究生学习时光，并结下了深厚的 友谊，将令我难以忘怀。还要对我的好友张雪萍表示感谢，她对我诚恳、细致 的帮助令我十分感动。

在此，谨向这些鼓励、关怀、帮助过我的老师以及朋友们致以崇高的敬意 和深深的感谢。

- 53 -

中国知网 https:Www  cnknet