分类号 UDC

密级\_ 编号\_

**华中師範大学** **硕士学位论文**

**基于二维码图像的信息** **隐写算法研究**

学位申请人姓名： 宋梦丽

申请学位学生类别： 全日制硕士

申请学位学科专业： 信号与信息处理

指 导 教 师 姓 名 ： **吴建斌副教授**

https www.cnki.net

**硕士学位论文**

MASTER'S THESIS



**硕士学位论文**

**基于二维码图像的信息** **隐写算法研究**

**论文作者：宋梦丽**

**指导教师：吴建斌副教授** **学科专业：信息与通信工程** **研究方向：信息隐藏**

**华中师范大学物理科学与技术学院** **2022年5月**

**中国知网** [**https://www.cnki.net**](https://www.cnki.net)

硕士学位论文

MASTER'S THESIS



**Research on Information**

**Steganography Algorithm Based**

**on QR Code Image**

*A Thesis*

Submitted in Partial Fulfillment of the Requirement

***For the Academic Papers on Information and Communication Engineering***

**By**

**Song Meng Li**

**Postgraduate Program**

**College of Physical Science and Technology Central China Normal University**

**Supervisor:Wu Jianbin**

**Academic Title:Associate Professor** Signature] 5 的 I

Approved May,2022

中国知网 https://www.cnki.net

中国知网 s://www.cnki.net

硕士学位论文

MASTER'S THESIS



**摘** **要**

互联网已经逐渐成为人们获得信息的重要渠道，但由于其具有开放性与共享性， 这会导致重要的机密信息在传递过程中可能出现被盗取、泄露等风险。如何借助互 联网等公有信道传输秘密信息一直是信息安全领域的研究热点。

为实现秘密消息的安全传输，信息隐藏技术被引入到该领域并受到了极大关注。 该技术通过特定的算法将机密信息嵌入到载体中，借助含密载体在公有信道中的传 输实现秘密消息的安全传递。二维码作为一种重要的信息传递载体，在生活中已经 被广泛应用，扫码支付、电子验票、会议签到、信息填写等均可以通过识别二维码 进入链接来操作。从信息隐藏的角度看，二维码图像已具备作为载体传输秘密消息 的各个特点，具有容错率强、信息容量大以及传递渠道广等优势。有鉴如此，本文 将重点研究基于二维码图像隐写算法，改进了Z-Xing 开源库，并利用该算法实现 了一个原型隐蔽通信系统。主要工作如下：

(1)通过改进Z-Xing 开源库，生成不同版本 (Version) 的二维码，增加二维 码图像隐写载体选择的多样性。目前生成二维码常用到的开源库Z-Xing 仅能生成 不同大小的二维码，无法定义更详细的信息。本文在此基础上进行改进，可以确定 生成二维码的版本及纠错级别。二维码共有4个纠错级别，纠错等级越高，容错率 越强。版本越大，可以在嵌入的秘密信息容量也就越大。

(2)针对现有二维码信息隐写算法中隐藏容量小、含密图像质量偏低等问题， 本文利用二维码丰富的纹理分布优势，将二维码图像利用DCT 从时域变换到频域 中，通过设定相应的规则修改其频域系数，并采用STC 编码根据失真函数以最小化 失真的方式嵌入秘密信息，含密图像重新恢复时域后二维码图像内容不变。实验证 明，使用本文隐写算法时，含密二维码图像具有极高安全性，且二维码载体中秘密 消息嵌入量较高，为秘密信息的隐藏提供了相当大的空间，有利于秘密通信的实际 应用。

(3)利用本文设计的信息隐写算法，实现一个隐蔽通信系统。该系统能够根 据秘密信息的长度选择合适Version的二维码载体进行秘密信息的嵌入，接收方能 够通过含密二维码准确快速的提取出秘密信息，从而实现隐蔽通信的目的。

**关键词：** **信息隐藏；载体图像；二维码图像；隐蔽通信**

I

**中国知网** [**https://www.cnki.net**](https://www.cnki.net)



硕士学位论文

MASTER'S THESIS



**Abstract**

The Internet has become an important channel for people to obtain information. However,due to the openness and sharing nature of the Internet,there may be risks such as theft and leakage of confidential information during the transmission process.How to transmit secret information through public channels such as the Internet has always been a research hotspot in the field of information security.In order to realize the secure transmission of secret messages,information hiding technology has been introduced into this field and has received great attention.This technology embeds the confidential information into the carrier through a specific algorithm,and realizes the safe transmission of the confidential message by means of the transmission of the confidential carrier in the public channel.As an important information transmission carrier,QR code has been widely used in daily life.Scan code payment,electronic ticket verification, meeting check-in,information filling,etc.can all be operated by identifying the QR code to enter the link.From the perspective of information hiding,QR code images have the characteristics of being a carrier to transmit secret messages,and have the advantages of strong fault tolerance,large information capacity,and wide transmission channels.In view of this,this thesis will focus on the study of image steganography algorithm based on two-dimensional code,improve the Z-Xing open source library,and use this algorithm

to realize a prototype covert communication system.The main works are as follows:

(1)By improving the Z-Xing open source library,QR codes of different versions (Version)are generated to increase the diversity of steganographic carrier choices for QR code images.At present,the open source library Z-Xing commonly used to generate QR codes can only generate QR codes of different sizes,and cannot define more detailed information.This thesis improves on this basis,and can determine the version and error correction level of the generated QR code.There are 4 error correction levels in the QR code.The higher the error correction level,the stronger the error tolerance rate.The larger the version,the larger the amount of secret information that can be embedded.

(2)Aiming at the problems of small hidden capacity and low quality of dense images in the existing two-dimensional code information steganography algorithms,this thesis takes advantage of the rich texture distribution of two-dimensional codes to transform the

l|

**中国知网** [**https://www.cnki.net**](https://www.cnki.net)



硕士学位论文

MASTER'S THESIS



two-dimensional code images from the time domain to the frequency domain using DCT.,modify its frequency domain coefficients by setting corresponding rules,and use STC coding to embed secret information in a way that minimizes distortion according to the distortion function.Experiments show that when using the steganography algorithm in this thesis,the encryptedtwo-dimensional code image has extremely high security,and the embedded amount of the secret message in the two-dimensional code carrier is high, which provides a considerable space for the concealment of secret information,which is conducive to secret information,Practical application of communication.

(3)Using the information steganography algorithm designed in this thesis,a covert communication system is realized.The system can select the appropriate version of the two-dimensional code carrier to embed the secret information according to the length of the secret information.

**Keywords:** information hiding;carrier image;two-dimensional code image;covert

**communication;**

**ⅢI**

**中国知网** [**https://www.cnki.net**](https://www.cnki.net)



硕士学位论文

MASTER 'STHESIS



**目** **录**

**摘** **要** I

**Abstract** Ⅱ

**第** **1** **章** **绪论** [1](#bookmark1)

1.1 研究背景及意义 [1](#bookmark2)

1.2 国内外研究现状 [2](#bookmark3)

1.2.1 隐写术研究现状 [2](#bookmark4)

1.2.2 二维码图像信息隐藏技术研究现状 [3](#bookmark5)

1.3 主要研究内容 [5](#bookmark6)

1.4 论文的结构与安排 [6](#bookmark7)

**第** **2** **章** **相关理论及技术** [7](#bookmark8)

2.1 隐写术 [7](#bookmark9)

2.1.1 隐写术的基本原理 [7](#bookmark10)

2.1.2 隐写术的基本特征 [10](#bookmark11)

2.1.3 隐写算法的性能评估 [11](#bookmark12)

2.2 隐写分析介绍 [14](#bookmark13)

2.2.1 图像特征构造与提取 [14](#bookmark14)

2.2.2 分类器训练与分类 [15](#bookmark15)

2.2.3 隐写分析评价指标 [17](#bookmark16)

2.3 二维码图像 [17](#bookmark17)

2.3.1 二维码图像组成及其符号结构 [17](#bookmark18)

2.3.2 二维码图像生成过程 [18](#bookmark19)

2.3.3 纠错编码原理 [20](#bookmark20)

2.3.4 生成载体二维码 23

2.4 本章小结 24

**第3章** **以二维码为载体的隐写算法** 25

3.1 信息嵌入算法 25

3.1.1 信息恢复机制 25

3.1.2 嵌入算法设计 27

3.1.3 算法实现 33

3.2 信息提取算法 37

3.3 本章小结 40

**第** **4** **章** **隐写算法性能测试** 41

4.1 隐藏容量分析 41

4.2 不可感知性分析 44

4.3 鲁棒性分析 47

4.4 抗检测分析能力 54

4.4.1 隐写分析过程 54

**中国知网** **https :// www.cnki .net**



硕士学位论文

MASTER 'S THESIS



4.4.2 隐写分析结果 55

4.5 本章小结 57

**第** **5** **章** **隐写系统实现** 59

5.1 系统界面设计 59

5.2 系统功能测试 62

5.3 本章小结 65

**第** **6** **章** **总结与展望** 66

6.1 工作总结 66

6.2 未来展望 67

**参考文献** 68

**攻读硕士期间发表的论文** 72

**致** **谢** **73**

中国知网 https :// www. cnki . net



硕士学位论文

MASTER'STHESIS



**第1章绪论**

**1.1研究背景及意义**

随着信息技术的飞速发展，互联网逐渐成为人们获得信息的重要渠道。但由于 互联网具有开放性与共享性，这会导致机密信息在传递过程中可能出现被盗取、泄 露等风险，如何借助互联网等公有信道传输秘密信息一直是信息安全领域的研究热 点 。

信息保护的传统方法是使用密钥对通信内容加密，加密后的数据在没有解密的 情况下通常是乱码，无法被直接识别，以此达到保护信息目的[1¹。但是，加密后的 信息表现为杂乱无章的字符，传输过程中很容易引起第三方的怀疑。为了改进加密 算法传输中的安全性问题，信息隐藏技术逐渐被应用。隐写术作为信息隐藏技术的 一个重要分支， 一直倍受研究者关注，该技术是将秘密信息采用某种编码方式嵌入 到载体中后，并借助载体的传输来实现秘密信息的传递[2³。与加密技术相比，隐写 术可以减少第三方的怀疑，使秘密信息在公共信道的传输过程中更有保障。

隐写术的载体可以是图像、音视、视频、文本等[3]。其中，基于图像的信息隐 写技术是最早从实验室摇篮发展成为实用的产品，已经成为国家安全机构和企业单 位传递秘密信息的主要技术手段。从目前公开发表的研究来看，图像信息隐写大多 以纹理丰富的自然风景图像或者人物图像为载体4,这是因为此类图像的冗余稍多， 嵌入秘密信息时，对其造成的影响较小。但是，含密图像在公共信道传输过程中如 何降低非合作方的怀疑仍需要考虑。

近年来，二维码作为传递信息的手段之一，在我国呈现了爆发式增长的趋势， 已然为我国现代化信息建设的重要支撑s。 评价隐写术性能好坏的一个重要指标是 不易察觉性，即在保证含密图像质量的前提下，传输过程中也应当尽量规避第三方 的怀疑。若将二维码图像作为载体传递信息，即使被嵌入秘密信息后会引起不同程 度的残缺和破损，但只要能保证其外观大致不变，在各种应用场景下也不会引起非 合作方的怀疑。基于此，本文将重点研究基于二维码的隐写算法，主要关注隐写容 量、不可见性和鲁棒性等指标。

1

**中国知网** [**https://www.cnki.net**](https://www.cnki.net)



硕士学位论文

MASTER'S THESIS



**1.2国内外研究现状**

**1.2.1** **隐写术研究现状**

隐写术根据载体种类不同，可以分为基于文本、音频、视频以及图像等载体的 隐写技术[6],由于本文旨在研究基于二维码图像的信息隐写算法，因此，重点对图 像信息隐写展开介绍。

图像信息隐写技术中，常将秘密信息嵌入在图像的空域或变换域两种不同的位 置。空域信息隐藏技术中最早的是LSB replacement算法7,该技术用秘密信息流 代替图像像素的最低位，嵌入容量较大，但是生成的载体图像会有明显的直方图统 计特征，且遭遇攻击时鲁棒性不高。为改进这一缺点，有学者提出LSB Matching 算法对载体图像的最低有效位置进行“±1”操作[8],该算法可以改进含密图像直 方图特征明显的特点。但在隐写分析技术中，SPAM features通过1阶和2阶马尔可 夫链对图像的相邻像素差值建模[9],把样本转移概率矩阵的子集作为隐写分析的检 测特征，可以检测出LSB Matching算法。为提高含密图像安全性，Kuo 等人采用一 组中的n个载体像素来嵌入秘密信息[10],嵌入阶段不再修改全局统计特性，载体 像素点数变为原来的1/2,此方法可以生成质量较高的含密图像，但嵌入容量偏低。 近些年，Pan 等人根据相邻像素到绝对值的技术，通过与相应的数据位进行比较来 对秘密信息进行隐写[11],一定程度上提高了秘密信息的隐藏容量，嵌入具有一定 的规律性，难以抵抗隐写分析的检测。为提高秘密信息的隐蔽性，减少对图像特征 的改变，有不少学者研究将载体图像转换至变换域上进行操作。

变换域的信息隐藏中，最常离散余弦变换(Discrete Cosine Transform,DCT)=12、 散小波变换(Discrete Cosine Transform,DWT)[13] 、DCT、离散傅里叶变换(Discrete Fourier Transform,DFT)[14]。注意到JPEG 、MPEG 等图像压缩标准与DCT 变换 相兼容，因此在以上不同域的变换方法中，基于DCT 域变换的隐写方法运用最广 泛I15 。Xu 将载体图像的DCT 系数分为8×8块，利用密钥Key 随机选取图像块， 在频域的中频系数中嵌入秘密信息[16],可以一定程度上抵抗隐写分析检测，但嵌 入的信息量较少。后有学者提出的F5 算法采用湿纸编码的思想实现隐写算法的安 全性-17],但其在信息嵌入时对载体图像的修改呈规律性，容易被第三方攻破。为 解决这一问题，李海涛等人在F5 算法的基础上，根据量化系数绝对值，将信息嵌 入到非零DCT 系数上[18],保证对图像的修改无规律， 一定程度上提高了安全性， 但是该方法嵌入容量会有所降低。GUOLJ 等人考虑数字图像统计模型的相对变化 来细化均匀嵌入=19',针对JPEG 图像分析不同系数的一阶、二阶统计量的CV 系数，

2

**中国知网** [**https://www.cnki.net**](https://www.cnki.net)



硕士学位论文

MASTER'S THESIS



采用所有DCT 系数作为嵌入单元，通过简单的将附加的舍入误差与非边信息UERD

相结合，使用统一的函数失真处理，与原来的均匀嵌入失真相比，嵌入能力有所提 高。Weng等人基于DWT 域上的预测生成方法(prediction-generating-method,PGM),

设计一种预测误差扩展算法，应用PGM 生成含密图像[20],该隐写算法下图像的质 量有所提升，但是抵抗统计分析的能力有待提升。

为了增强抗隐写分析能力，刘明明等人提出一种基于生成对抗网络的无载体信 息隐藏算法[21],以秘密信息为驱动生成含密图像进行传递，可抵抗隐写分析的检 测，但可隐藏的信息容量低。Zhou 等使用更快区域的卷积神经网络 (Faster Region-based Convolutional Neural Networks,Faster-RCNN)来检测和定位图像中的 对象，并利用选中对象的标签表达秘密消息[22-,该方法可以抵抗隐写分析能力， 降低第三方的怀疑。LiQ 将秘密信息嵌入到载体图像中得到合成图像，然后利用该 合成图像作为第一个生成模型的输入来获得含密图像[23],该算法具有更高的安全 性以及鲁棒性，但信息隐藏容量与有载体隐写算法相比仍有差距。

在以上算法中均选用自然界图像作为载体图像，嵌入的信息量与抗隐写分析能 力难以达到较好的平衡状态。因此，就有学者开始探索如何在保证含密图像质量的 同时，嵌入大量的秘密信息。考虑到二维码图像需要借助扫描设备才能获得其要表 达的信息，与自然界图像有着本质的不同，且二维码具有一定的容错率，在外界对 其进行一定程度的“破坏”时仍然可以识别出信息。基于此，很多学者为了提高隐 写算法的性能，展开了基于二维码图像信息隐写技术的研究。

**1.2.2二维码图像信息隐藏技术研究现状**

近年来二维码图像在社交平台上广泛使用，如何利用二维码作为载体构建秘密 消息的传递渠道逐渐成为隐写领域的研究热点。很多学者在从事基于二维码的隐写 算法研究，这些研究主要集中在三个方面：①将秘密信息编码成二维码后作为水印 嵌入到其他载体中；②自然图像隐写算法用于二维码图像；③二维码图像作为载体 传递秘密信息。

早有Hsu FH将二维码作为可见水印嵌入到灰度载体图像中24],通过向像素 值中添加正的随机值方法完成消息的嵌入，可使用特定设备扫描获取水印信息，但 该方法下可见水印安全性难以保障。Panyavaraporn J等将二值图像作为水印嵌入到 选择的频域子带中，提出了一种基于小波变换的QR 码水印算法25],安全性有所 提高，但遭受几何失真、剪切等攻击时秘密信息无法正确提取。Chen L等提出了一 种结合二维码和提升小波的盲水印方法，将待嵌入的水印图像进行二维码编码以及 混沌处理，再嵌入到提升小波变换后的载体图像中[26],此算法获得的含密图像在

3

**中国知网** [**https://www.cnki.net**](https://www.cnki.net)



硕士学位论文

MASTER'S THESIS



传输过程中安全性有所提高，但其计算复杂度较大。Lee YL等提出了一种二维码 作为安全水印信息的数字水印方法27],它将秘密信息编码为二维码后，“注入” 到载体图像的YcbCr的Y 通道中，该算法保证水印的不可见性，但生成的含密图像 视觉质量不高。Shashikiran BS等提出一种混合域隐写算法，秘密信息采用DES 加 密算法加密编码二维码图像，然后使用DWT 和随机位二进制搜索 (Random Bit Binary Search,RBBS)技术[28]将此二维码图像嵌入到载体图像，从而实现多级安全。 Pan JS提出的算法中，通过DWT-SVD 利用物质搜索状态 (state of Matter Search, SMS) 算法来寻找合适的嵌入因子[29],并通过调整嵌入因子强度进行修改嵌入不 同频域水印的强度，从而保证二维码图像具有更高的PSNR 值。

除了将二维码图像作为水印之外，也有学者将二维码图像作为秘密信息传递的 载体进行研究。Survase P等提出了一种基于QR 码的图像隐写算法，将二维码进行 DWT 变换后嵌入水印信息30],该方法侧重于水印嵌入后的图像质量，在鲁棒性方 面考虑有所欠缺。为了提高鲁棒性，严文博等研究出一种针对JPEG 格式的二维码 隐写算法31,该算法在嵌入信息之前，将二维码载体与纹理丰富的图像进行融合 提高消息嵌入量并保障了物流信息的隐私，但含密图像为二维码与自然图像的融合， 与常见二维码结构有所不同，传输过程中可能引起非合作方的怀疑。Chow YW等 为了增加秘密信息在传输时的安全性，利用二维码的纠错机制设计出秘密共享方案 32],将一个秘密信息编码和分发到多份，防止秘密信息集中，达到分散风险的目 的，但是隐藏方法只是通过简单的异或技术，易被攻击者识别，安全性较低。后有 学者利用二维码中R-S 纠错码特性，每个数据块B 中包含K 个数据符，利用伪随 机数G 产生随机序列R, 然后根据随机序列在数据块中随机选择K/2 个符号构成比 特流S, 若秘密信息m,≠S,2, 则s, 取反，否则S₂ 不变。待所有秘密信息嵌入后 可得到新的数据块B'[33]。该算法测试40个二维码，具有较高安全性，但是容量偏 低。同样，傅俊利用R-S 纠错码特性，提出一种基于LSB 匹配的信息隐藏方法，将 QR 码数据划分为若干对放入候选池，然后采用密钥K, 随机的从候选池选取模块 对嵌入秘密信息，直至候选池模块对为空[34,该算法的含密图像质量与文献[27] 相比有所提升，但是在嵌入容量方面相差无几，没有明显提高。LiM 等根据二维码

结构特点，将二维码的定位图形叠加在半色调图像上生成一个包含定位图形的新半 色调图像[35,在读取该图像时可以利用二维码定位功能准确纠正图像，有效解决 秘密信息的准确提取以及高精度图像校正的问题。

上述采用二维码作为载体进行信息隐藏时，其嵌入和提取方法均参照了自然图 像信息隐藏的相关思路，但二维码是由黑白模块组成，和自然图像之间存在一定差

4

**中国知网** [**https://www.cnki.net**](https://www.cnki.net)



硕士学位论文

MASTER'S THESIS



异36。采用二维码作为载体进行隐写时，更应该关注二维码特殊结构和生成方法， 结合二维码的特点来设计合理的隐写算法。正是基于这一点，有学者提出利用二维 条码空白区域宽度大小进行信息隐藏。Wu 等人通过调整二维码模块中水平和垂直 的内部边界，以两个模块对作为消息嵌入的单元[37,该算法下的含密二维码可抵 抗常见攻击，且其消息隐藏量与二维码版本相关，Version 40的二维码载体图像可 隐藏约14000bit 消 息 。Zhou 等人基于二维码编码原理，选择数据码字中的冗余部 分，通过位替换的方式嵌入秘密信息38],保证了载体二维码可识别出原本信息， 传输中有较高安全性，但该方法嵌入信息量有限。Zhang 等人同样利用二维码的纠 错机制，将秘密信息以随机的方式嵌入到二维码矩阵中的随机位置[39],含密图像

传输过程中第三方只能扫描出公共信息，可实现秘密信息的传递，但是随机嵌入的 方法会降低二维码的识别率。Lin PY基于二维码的纠错能力设计了三重模块组，改 变一个模块可以嵌入2位秘密信息[40],提高了秘密信息的嵌入量，但是含密图像 在传输过程中鲁棒性较低，很难抵抗常见攻击。Huang PC等人在开发修改方向 (Exploiting Modification Direction,EMD)方法[41³上加以改进，将秘密信息转换 为八进制数据流，并将载体二维码内容转换为二进制位流，设定相应的规则改变二 维码数据对的过程中将秘密信息嵌入42],该方法可保证含密图像的安全性，但是 信息隐藏容量偏低。

综上所述，在当前二维码信息隐藏研究现况下，现有的算法中信息隐藏容量以 及隐写算法安全性均有待提高。基于上述讨论，本文选用二维码图像为载体，以隐 藏信息为主要目的，设计出一种基于二维码图像的信息隐写算法。

**1.3主要研究内容**

二维码作为新时代信息传递的媒介，已经越来越深入人们的生活，并且不同领 域的二维码发展呈现出不同的特点。本文主要以信息隐藏为主要目的，为了提高含 密图像在公有信道中的安全性，选用二维码作为载体，研究一种新的秘密消息隐写 方法，并利用该算法实现一个隐蔽通信系统。主要工作如下：

(1)了解二维码图像特性以及二维码编码原理。由于目前Z-Xing 开源库项目 只能生成和识别二维码，不能修改其版本以及纠错级别。本文在此基础上加以改进， 可以生成不同Version不同纠错级别的二维码图像，完成二维码的编码解码工作。

二维码是由不同数量的黑白模块组成，从Version 1-40,信息存储量逐渐增加，秘密 信息可嵌入的容量也在提高。与自然图像信息隐藏不同，本文选择二维码图像作为 载体可以根据秘密信息的长短去选择不同Version二维码作为载体图像。

5

**中国知网** [**https://www.cnki.net**](https://www.cnki.net)



硕士学位论文

MASTER'S THESIS



(2)针对目前基于二维码图像信息隐写算法存在的嵌入量小、图像质量低等 问题，提出一种新的基于二维码特性的隐写算法。该算法利用二维码丰富的纹理分 布，设定相应的规则来通过修改其频域系数并采用STC 编码方式，以最小化失真的 方式嵌入秘密信息，含密图像重新恢复时域后二维码图像内容不变。通过测试与验 证，该算法将大量秘密信息嵌入进二维码载体后，得到的含密二维码质量较高，且 依然能够识别出二维码公共数据内容，传输过程中不易引起第三方怀疑。

(3)利用设计的信息隐写算法，实现一个隐蔽通信系统。该隐蔽通信系统可以 实现秘密信息的嵌入以及提取和保存。经过测试与验证，该系统具有可执行性以及 较强隐蔽性。

**1.4论文的结构与安排**

本文共分为6个章节，每章节内容安排如下：

第1章，绪论。首先简要概括选题的研究背景和研究意义，接着详细介绍关于 隐写术以及二维码图像隐写的国内外研究现状，最后总结了本文主要的研究内容和 文章整体的结构安排。

第2章，相关理论和技术。首先从隐写术的基本框架、隐写术常见特征以及其 评价指标三个方面对隐写术进行了阐述，其次简单介绍了隐写分析技术，再次介绍 了二维码的图像特性和编码原理，最后介绍如何改进开源库Z-Xing 生成不同版本 的二维码图像。

第3章，基于二维码图像的隐写算法。首先介绍二维码结构特性，确定了秘密 信息的嵌入区域，接着秘密信息的介绍嵌入规则和提取步骤。最后对提出的算法进 行实验，证实了算法的有效性。

第4章，性能测试与实验分析。从信息隐写技术的三个评价指标：容量、鲁棒 性、安全性进行分析，并评估本文算法的性能。从隐写分析的角度去测试本文隐写 算法的抗检测能力，并与其他基于二维码图像信息隐写算法的性能做出对比。

**第5章，隐写系统的设计与实现。从系统的界面设计和系统的功能实现两个方** **面展开介绍。**

**第6章，总结和展望。对本文的工作做出概括，并针对目前研究工作分析不足** **之处，给出下一步的研究方向。**

6

**中国知网** [**https://www.cnki.net**](https://www.cnki.net)

硕士学位论文

MASTER"S THESIS



**第2章相关理论及技术**

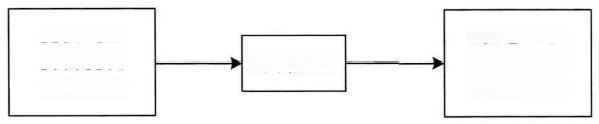
本章主要对隐写技术和二维码图像特性两部分展开介绍。第一部分是隐写术的 理论知识，包括其基本原理、常见特征以及隐写性能评价指标，因后续需要分析隐 写算法的抗检测性能，所以本部分也对隐写分析技术做出简单介绍；第二部分主要 阐述二维码图像特点，包括二维码模块结构以及纠错原理，最后生成不同版本的二 维码图像为秘密信息的隐藏做好准备工作。

**2.1** **隐写术**

隐写术主要将机密信息嵌入到一个看似无关联的载体中，并且含密载体在公有 信道上传输时应尽量减少第三方的注意，从而保证接收方可以恢复出秘密信息。本 节将从隐写术基本原理，隐写术主要特征以及常用的性能评估方法对其展开介绍。

**2.1.1** **隐写术的基本原理**

加密技术主要是将秘密信息编码成密文的形式，从而达到数据保护的目的。其 模型如图2. 1所示：

11100101

10001101

10001110

明文

密钥加密

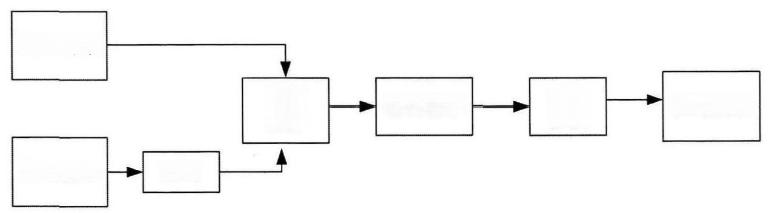
#@#¥!#\*

#&\*\*¥#\*# &\*&@#¥%\*

密文

图2.1信息加密框架

由信息加密框架可知，要传递的明文经过密钥加密后会变成无规则的密文，传 输过程中很容易引起第三方注意，攻击者则可以对消息进行解密或者破坏，从而影 响机密信息的安全传输。



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 载体对象 |  |  |  |  |
|  | 隐写 算法 | 含密载体 | 提取 算法 | 秘密信息 |
| 秘密信息 | 加密 |  |  |  |

图2.2隐写术的基本框架

与信息加密技术不同，隐写术既隐藏了消息的内容，又隐藏了消息的存在。图 7

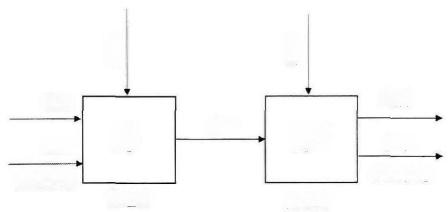
**中国知网** [**https://www.cnki.net**](https://www.cnki.net)

硕士学位论文

MASTER'STHESIS



像隐写的基本框架如图2.2所示，通常情况下为了增加秘密信息的安全性，在信息 嵌入之前会使用密钥进行加密处理。密钥隐写原理如图2.3所示：



载体

嵌入 秘密信息

接收方

载体

提取 秘密信息

*fF*

发送方

*fp- ¹*

隐写

密 钥

密钥

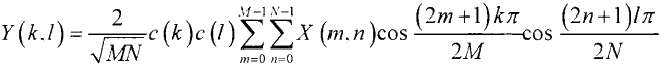
图2.3密钥隐写原理图

密钥包括对称密钥和非对称密钥。对称密钥是指发送者加密信息和接收者解密 信息的整个过程中使用的是相同密钥，常用到的算法有AES 、DES 、3DES 等 ， 此 类密钥加密解密速度比较快，但是安全性偏低。非对称密钥加密过程中发送者使用 公钥去加密，接收者则使用私钥解密-6³,常用到的算法有RSA、DSA、ECC 等 ， 非对称密钥安全性较高，但是计算复杂并且加密解密速度稍慢。

秘密信息根据其嵌入方式不同，本文主要在变换域中对秘密信息采用自适应的 方法嵌入。

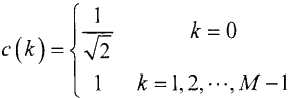
(a) 变换域算法是指将秘密信息嵌入数字作品的某一个变换域系数中[43],通 常进行的变换有DFT 、DCT 、DWT 等 ， 以DCT 域变换为例，经过DCT 变换原理 如下：

数字图像X(m,n) 是 具 有M 行 N 列的一个矩阵，为了同时减弱或者除去图像数 据相关性，运用二维DCT 变换，将图像从空间域转换到DCT 变换域。二维离散余 弦变换定义如下：



公 式 中 ，m,k=0,1…,M-1:n,l=0,1…,N-1

其中，



(2.1)

(2.2)



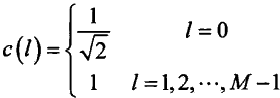
8

中国知网 https://www.cnki.net

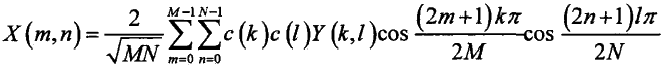
硕士学位论文

MASTER'S THESIS





二维逆离散余弦变换(IDCT)的定义如下：



式 中 ，m,k=0,1…,M-1;n,l=0,1…,N-1

(2.3)

(2.4)

基于DCT 变换编码中，图像是先经过8×8分块，再经过DCT 之后得到DCT 系数，然后按照zig-zag次序从低频到高频排序成一维向量Y{y₁,y₂,…,yMxx}, 并 取 出序列中第L+1 到L+M 的系数部分，得到YL={vL+1,yL+2,…,yL+M},从而完成秘密 消息比特流的嵌入。

(b) 自适应隐写算法中的STC 编码是目前主流的隐写编码，它可以做到最小

化失真并且逼近嵌入率的上限[44]。STC 主要算法原理是选择最优的嵌密载体以及 奇偶校验矩阵H。假设载体对象为x=(x₁,x₂, … ,xn), 含密对象为y=(y1,y₂, … ,yn),

m 为嵌入秘密信息嵌入与提取。STC 编码的过程可用以下公式表示：

*y=Emb(x,m)=arg min D(X,Y)* (2.5)

译码过程中使得以下式子成立：

*Hy⁷=c* (2.6) 式(2 . 6)中，c 为要传递的消息串，H 为校验矩阵，由高为h, 宽 为w 的基础

矩 阵 Âxw生成，原始载体的长度为n, 其 中n=w\*c,c 为秘密消息的长度。

寻找向量y, 使得下列式子失真之和相加最小：

 (2.7)

式(2 . 7)中，D(x,y) 是对实际总失真的估计，载体x与载体y 的大小为n×n, p, 即单点失真函数，此函数需要隐写设计者对其进行定义，本文在后文隐写中有对 该函数的设计。

校验矩阵Hxw由以下组成：

9

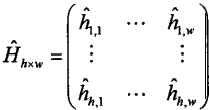
中国知网 <https://www.cnki.net>



硕士学位论文

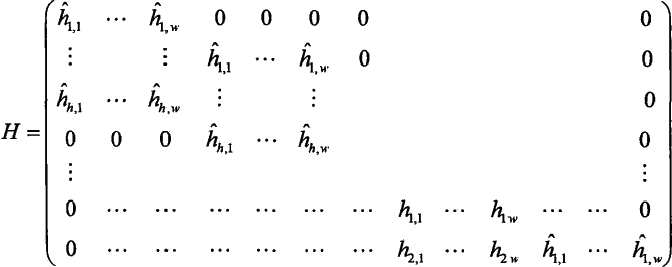
MASTER'S THESIS





(2.8)

然后将基础矩阵按照对角线方向不断地重复，可以得到校验矩阵H, 若最后复 制不完整也不会影响校验和提取。校验矩阵H 可以表示如下：



(2.9)

STC 编码可以看作通过逐步修改x 或者逐步构造y 使得Hy⁷=c 并且满足失真 和最小。其中在逐步构造提取方程时，STC 每次通过新加入w 个y 中元素传输一

个消息比特C, 依次构造以下等式，并记录有效解y,, 与修改叠加量e,。

(h,,…h,)(v,…,y)²=(h,…,h,)(x₁+e,…,x,+e.)²=c (h,,…h,)(v,…,yz)=(h,,…,h,)(x₁+e,…,xz+ez)²=c₂

中中毛

(2.10)



由于矩阵H 的特殊形式，根据矩阵原理Hy⁷=c, 只有向量的前w 比特能影响 消息c的第一比特(第1子块),同样c的第二比特仅受y 的前2w比特的影响，c 的 第三比特仅受y的第w+1位至第3w位的比特影响，以此类推。

2.1.2隐写术的基本特征

隐写术的基本特征包括：隐写容量、不可见性、鲁棒性、安全性。

(1)容量

容量指在保证载体质量的前提下，可以嵌入秘密信息的量。通常随着容量的增

10

中国知网 https://www.cnki.net



硕士学位论文

MASTER'STHESIS



大，含密图像的不可感性和不可检测性均会降低。

(2)不可见性

不可见性又称不可感知性，指秘密消息嵌入前后所引起载体图像的失真，视觉 上不可见。不可见性较低的图像在传输过程中比较容易引起人的怀疑。

(3)鲁棒性

鲁棒性在信息隐写技术中常用来评判隐写算法的健壮程度，指含密图像在传输 过程中遭遇一些异常时仍能够恢复出秘密信息的能力。通常情况下，异常指含密图 像遭受压缩、剪切、滤波、噪声等攻击。

(4)安全性

安全性即保证隐藏信息的内容是安全的， 一般通过使用密钥加密来实现。除此 之外，秘密信息隐藏在载体中的具体位置应该也是安全的，保证在传输过程中尽量 规避非合作者的怀疑，不易被第三方检测出。

安全性

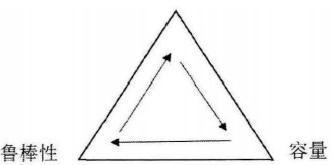


图2.5信息隐藏三大指标关系

以上是常用来评价隐写算法好坏的指标，如图2.5所示，这三个评价指标遵循 着三角关系互相约束。如果信息隐藏容量比较大的情况下，其安全性将会降低。所 以采用何种方式达到三者平衡，实现秘密信息的最优嵌入一直是个值得研究的问题。

**2.1.3隐写算法的性能评估**

隐写算法性能评估一般从三个角度出发，即不可见性、鲁棒性以及隐藏消息容 量大小。不可见性评估通常是测试使用该隐写算法嵌入秘密信息后生成的含密图像 质量如何，即图像失真程度大小；鲁棒性是衡量含密图像在传输过程可以抵抗攻击 的能力如何，在经加噪、滤波等图像处理之后，计算其可以恢复出的秘密信息量。

(1)不可见性评价

对图像的评价包括主观评价和客观评价。主观评价是嵌入秘密消息后的图像所 给我们带来的主观感受，图像修改是否人眼可见，此种评价方式通常主观意念比较 强，缺少一定的数据支撑。客观评价常通过计算失真图像的峰值信噪比(Peak Signal to Noise Ratio,PSNR)⁴5]以及结构相似性(Structural Similarity,SSIM)46 来 评

11

**中国知网** **https://www.cnki.net**