南開大學
Nankai University

网络空间安全学院

信息隐藏技术实验报告

DCT 域信息隐藏法

姓名：魏伯繁

学号：2011395

专业：信息安全

2023 年 5 月 2 日

目录

1 实验要求

DCT 域的信息隐藏包括：1. 修改系数方法；2. 系数比较方法。以上两种方法任选一种，实现变换域中的信息隐藏与提取。

2 实验原理

DCT（离散余弦变换）是一种常用的信号处理技术，广泛应用于图像和音频信号压缩、处理和特征提取等领域。基于 DCT 的信息隐藏方法是在图像的 DCT 域（也称为频域）中进行的。具体包括修改 DCT 系数方法和系数比较方法两种。

2.1 修改 DCT 系数方法

修改 DCT 系数的方法是利用 DCT 系数的特性进行信息隐藏，即对于一个块的 DCT 变换系数，其本质是对块内像素做了一次变换，且变换后的系数按重要程度从高到低排列。因此，在块内选取一些重要的 DCT 系数，稍稍改变它们的比例，就可以嵌入一定量的信息，而不太引起人眼的感知变化。

以修改左上角系数为例，修改系数的方法可分为挖掘空洞和加扰两种：

(1) 挖掘空洞：该方法的核心思想是把块内最重要的 DCT 系数缩小或者增大，从而挖掘若干个空洞来嵌入信息。具体来说，在这个方法中，通常情况下，选取最重要的一或两个 DCT 系数作为信息嵌入点，若对应二值水印为 0，则乘以一个小于 1 的系数，否则乘以一个稍大于 1 的系数。

(2) 加扰：该方法的核心思想是利用 DCT 系数对块内像素灰度的影响来实现信息隐藏。具体来说，这个方法中每个块的系数值按顺序顺次溢出到后面的系数中，然后把要嵌入的信息放在其中一些熵值较低的 DCT 系数中（如左上角的系数），再将溢出的系数重新带回到块内，从而实现信息的嵌入。

(3) 针对修改 DCT 系数方法，还有一种常见的方法是基于积分图的嵌入法。该方法主要思想是先对每一个块的 DCT 系数进行积分操作得到积分图，然后通过修改积分图中的值来实现信息的嵌入。具体来说，首先将块内 DCT 系数按照从大到小的方式排序，然后对所有排序过的 DCT 系数分别进行积分，得到一个与原始图像大小相同的积分图。接着，根据要嵌入的信息，将积分图中相应的像素值进行修改，最后利用离散余弦反变换将经过修改的积分图还原为一幅与原始图像形状一致的加密图像。该方法在隐藏信息方面的效果比较好，且容易被其他人感知到。

2.2 系数比较方法

系数比较方法是指对 DCT 系数进行比较，然后对比结果进行信息嵌入，不直接改变原始系数的值。常见的系数比较方法主要有两种：LSB （Least Significant Bit）嵌入法和基于阈值的积限法。

(1) LSB 嵌入法：该方法的核心思想是利用某些比较弱的 DCT 系数来嵌入信息，如在左下角或右下角、或者从中间部位开始选取若干系数，然后将要嵌入的信息位添加到系数的低位上，再将修改后的系数信息反推回原始大小的块中。

(2) 基于阈值的积限法：该方法的核心思想是将 DCT 系数比较结果量化成二值水印后，通过设定阈值来确定信息嵌入点，即对块内所有 DCT 系数都设置一个阈值，若 DCT 系数大于阈值，把对应位置的二值水印设为 1，否则设为 0。

(3) 针对系数比较法，还有一种常用的方法是基于扩频序列的嵌入法。该方法的核心思想是通过将信息序列加入到嵌入序列中，然后再利用扩频技术将电子噪声散播到系统信号中，从而实现信息隐藏。具体来说，在嵌入过程中，需要先将需要隐藏的信息用扩频技术转换成扩频序列，然后将扩频序列和待

嵌入 DCT 系数做异或操作，得到新的 DCT 系数。这样，在反嵌入时，只需要将加密图像的 DCT 系数提取出来，并使用扩频技术进行解密，即可得到隐藏在其中的信息。该方法的优点是抗干扰性强，不容易被其他人感知到，但是嵌入容量较小

总体来讲，DCT 域信息隐藏法的优点是难以被突破和撤销，缺点是嵌入的信息容量较有限。此外，嵌入效果会受到许多因素的影响，如块的大小和选择，DCT 系数选取和修改策略，以及反嵌入时用的解密密钥等。因此，在实际应用中需要根据具体情况进行权衡和选择。

2.3 综合分析

另外，需要注意的是，在实际应用中，基于 DCT 的信息隐藏方法可能会受到各种攻击的干扰，例如旋转、缩放、噪声、压缩和剪切等。因此，信息隐藏的容错性、鲁棒性和安全性也是需要考虑的重要因素。

此外，为了保证消息的完整性和加密性，通常还需要对信息进行加密，以防止对手对信息的篡改和破解。基于对称密钥的加密方法通常比较适合信息隐藏应用，例如，使用 AES、DES 或者 Blowfish 等加密算法进行加密。在加密时，需要确保密钥的安全性和保密性，特别是在网络数据传输中需要采用 SSL 或者加密通道等技术来保证通信的隐私和安全性。。

综上，基于 DCT 的信息隐藏方法可以为图像和音频等数字媒体提供一定程度的隐私保护和版权保护。然而，它也存在着一定的局限性和风险，应该在具体应用时进行权衡和选择，以达到最优的隐私保护和信息传输效果。

3 编程实现

3.0.1 修改 DCT 系数

这段代码是实现了基于修改 DCT 系数的信息隐藏方法，其步骤主要包括：

1. 首先，对原始图像进行分块处理，每个块的大小为 w x w。
2. 然后，对每个块进行离散余弦变换 DCT2。
3. 根据要隐藏的信息在秘密信息载体中建立指定的二元序列，并以此控制上述步骤中离散余弦变换的系数变换，从而实现将秘密信息隐藏进载体图像中。
4. 对于每个块中的 DCT 系数的直流分量 DCT(1,1) 进行量化的隐藏，即如果嵌入信息的像素值为 0，那么修改系数的方法为 cb(1,1) = cb(1,1)*(1-a*0.001)，其中 a=-1；如果嵌入信息的像素值为 1，那么修改系数的方法为 cb(1,1) = cb(1,1)*(1+a*0.001)，其中 a=1。
5. 最后，对修改后的 DCT 系数使用反离散余弦变换 IDCT2 进行逆变换，得到隐藏了秘密信息的加密图像。新的加密图像存储在 new_image 中。

```
1       for i = 1:blocks
2           for j = 1:blocks
3               x=(i-1)*w+1;
4               y=(j-1)*w+1;
5               cb=image(x:x+w-1,y:y+w-1);
```

```
            cb=dct2(cb);
            if wm(i,j)==0
                a=-1;
            else
                a=1;
            end
            cb(1,1)=cb(1,1)*(1+a*0.001);
            cb=idct2(cb);
            new_image(x:x+w-1,y:y+w-1)=cb;
        end
    end
```

3.1 提取隐藏信息

这段代码是基于修改 DCT 系数的信息隐藏方法中的信息提取部分。其主要功能是提取隐藏在载体图像中的秘密信息，包括以下步骤：

1. 首先对加密图像进行分块处理，每个块的大小为 w x w，与嵌入时一样。
2. 对每个块中的 DCT 系数的直流分量 DCT(1,1) 进行量化的隐藏，得到加密图像。
3. 然后比较加密图像与原始图像相同位置的像素值，如果加密图像的像素值比原始图像大，则提取的二元信息值为 1，否则为 0。
4. 最后，将提取的信息存储在提取出的二元信息序列 extract 中，该序列的大小与加密图像相同，并与嵌入时隐藏的序列一一对应。

3.2 实验结果

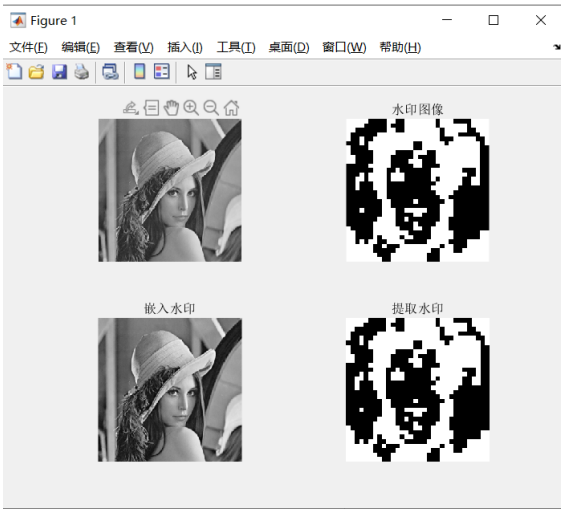

图 3.1: 实验结果图

4 心得体会

在信息隐藏技术的实验中，我对常用的基于修改 DCT 系数的信息隐藏方法进行了深入的学习和掌握。通过实际操作，我更深刻地理解了数字图像处理的基本概念、秘密信息的嵌入规则及提取过程。同时，我也认识到了利用信息隐藏实现隐私保护的重要性和必要性。

在本次实验中，我不仅了解了 DCT 变换和量化等数学方法及其在图像处理中的应用，更重要的是，我掌握了一种具有一定保密性的信息传递方法，并学习了如何保护敏感信息不被恶意窃取和篡改等隐私风险。这种数字隐写术可以应用于电子商务、医疗保健以及私人通讯等领域，保障了传输的数据隐私和传输的安全性，极大地提高了信息传输的可靠性。而这种隐写术的数字水印还可以应用于版权保护、信息真实性鉴别等领域。

总的来说，信息隐藏技术是一个较为新颖的理论体系，具有广阔的应用前景。通过本次实验，我不仅学会了使用 Matlab 进行实际操作，同时也对信息隐藏技术的优点、缺陷和应用前景有了更加深入的认识，相信这种数字隐写术未来可以应用于更广泛领域，并且得以更好地发展和完善。

参考文献