

信息隐藏技术实验报告

变换域隐藏法

2113662 张丛

实验内容
变换域隐藏法
原理
实现
实验结果
小结

实验内容

使用修改系数方法，实现变换域中的信息隐藏与提取。

变换域隐藏法

原理

在载体的显著区域隐藏信息，比 LSB 方法能够更好地抵抗攻击，而且保持了对人类感观的不可察觉性。



信息隐藏法：



基本隐藏算法

以一定的方式挑选一些中频系数，在这些中频系数中叠加秘密信息：

所有中频系数

固定位置的中频系数

随机挑选中频系数

选择最大的几个中频系数

修改系数方法：

实例1. 修改系数方法

原理：在选出的中频系数中叠加秘密信息

$$x'(i,j) = x(i,j)(1 + \alpha m_i)$$

$x(i,j)$

DCT系数

$x'(i,j)$

隐藏后的DCT系数

m_i

第 i 个秘密信息比特

α

可调参数，控制嵌入强度

DCT 域修改的系数一般都是中频系数，我们可以在这些中频系数中叠加所需的秘密信息。具体为在选中的中频系数中叠加秘密信息，成比例修改 DCT 系数：

$$x'(i, j) = x(i, j)(1 + \alpha m_i)$$

其中， α 是可调参数，控制嵌入强度， $x'(i, j)$ 和 $x(i, j)$ 分别为 DCT 系数和隐藏后的系数， m_i 就是第 i 个信息比特。

实验将通过修改图片的方式嵌入秘密信息，然后将新的图片与原图进行比较来提取秘密信息。所有的图片都应该是位图。

实现

```
% 预处理图像
img = (imread('gray_image.jpg')); % 读取原始图像
watermark = imbinarize(imread('222.bmp')); % 读取水印图像，并转为二值图像
img = imresize(img, [256, 256]); % 调整原始图像大小为256x256
watermark = imresize(~watermark, [64, 64]); % 调整水印图像大小为64x64，并取反

img = double(img) / 256; % 将原始图像转为double类型，并归一化
watermark = im2double(watermark); % 将水印图像转为double类型

size = 256; width = 4; % 设置参数

blocks = size / width; % 计算图像分块数
new_image = zeros(size); % 初始化新图像
vec = ones(64); % 初始化提取水印信息的向量

% 嵌入水印
for i = 1 : blocks
    for j = 1 : blocks
        x = (i - 1) * width + 1;
        y = (j - 1) * width + 1;
        cur = img(x:x+width-1, y:y+width-1);
        cur = dct2(cur);

        if watermark(i, j) == 0
            a = -1;
        else
            a = 1;
        end

        cur(1, 1) = cur(1, 1) * (1 + .01 * a) + .01 * a;
        cur = idct2(cur);
        new_image(x: x + width - 1, y : y + width - 1) = cur;
    end
end

% 提取水印
for i = 1 : blocks
    for j = 1 : blocks
        x = (i - 1) * width + 1;
        y = (j - 1) * width + 1;

        if new_image(x, y) > img(x, y)
```

```

        vec(i, j) = 1;
    else
        vec(i, j) = 0;
    end
end
end

% 显示结果
subplot(231); imshow(img); title("原始图像");
subplot(232); imshow(watermark); title("水印图像");
subplot(233); imshow(imcomplement(watermark)); title("反色之前的水印图像");
subplot(234); imshow(new_image, []); title("嵌入水印");
subplot(235); imshow(vec, []); title("提取图像");
subplot(236); imshow(imcomplement(vec), []); title("提取图像后反色与原图对比");

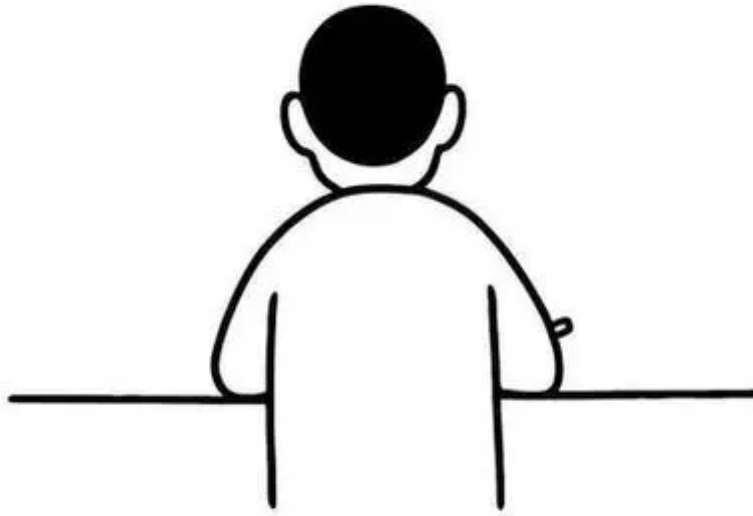
```

图像水印的嵌入和提取的流程：

1. 读取原始图像和水印图像，并对它们进行预处理（调整大小、转换为double类型）。
2. 将原始图像分成大小为4x4的块，对每个块进行DCT变换。
3. 根据水印图像的像素值，对DCT系数进行微调。
4. 对调整后的DCT系数进行IDCT变换，得到嵌入水印后的图像。
5. 根据嵌入水印后的图像和原始图像的像素值大小关系，提取出水印信息。
6. 显示原始图像、水印图像、嵌入水印后的图像以及提取水印后的图像，以及水印图像的反色和提取水印后反色的对比图像。

实验结果

水印图：



实验结果：



可见，原始图像和嵌入水印的图像几乎完全相同，除了色调有所变化，这实现了对人类感观的不可察觉性。

同时提取的水印图像和嵌入的水印图像也是一致的。故而，只要能制作合适的水印图像，可以秘密隐藏传输信息。

小结

这次实验让我学习了变换域隐藏法，这是图像水印技术的一种重要方法。通过实验，我更深刻地认识到了图像水印技术在信息安全和数字媒体保护中的重要性，以及其广泛的应用价值。在数字媒体领域，图像水印技术已经被广泛应用于数字版权保护、数字证据保全、数字图像处理等方面，具有非常广泛的应用前景和市场潜力。

实验不仅让我学习了图像水印技术的基本原理和实现方法，还提高了我使用MATLAB进行图像处理和编程的能力。我相信这些知识和技能对于我的未来发展和职业规划都将产生积极的影响。我将继续深入研究图像水印技术，为保护数字媒体的安全和可信度做出更多贡献。