信息安全实验——密码学实验

实验四：基于图像的部分加密

北京邮电大学信息安全中心　　刘建毅
liujy@bupt.edu.cn

- \\10.105.40.218\\ 实验四
- 实验类别
- 设计型实验：用 MATLAB 设计并实现对图像的部分加密。
- 实验目的
- 了解图像数据系数特点，掌握离散小波变换基本操作。了解选择加密技术，使用 MATLAB 实现基于小波分解的对图像的部分加密算法，掌握利用加密技术实现访问权限控制的版权保护的方法。
- 实验条件
- (1) Windows2000 或 WindowsXp 以上操作系统；
- (2) MATLAB6.5 以上版本软件；
- (3) 图像文件

- 实验原理
- 一级小波变换可将图像分解为 4 个子图： LL—— 逼近子图，代表输入图像水平和垂直两个方向的低频成分； HL—— 水平方向细节子图，它代表输入图像水平方向的高频成分和垂直方向的低频成分； LH—— 垂直方向细节子图，它代表输入图像水平方向的低频成分和垂直方向的高频成分； HH—— 对角线方向细节子图，它代表输入图像水平和垂直方向的高频成分。小波图像的各个子带分别对应了原图在不同尺度和分辨率下对原始图像的逼近，表现图像的能量集中于低频区域。高频区域表现的是图像边缘，轮廓和纹理在不同方向、不同尺度和不同频率下由细到粗的描述。有些数字水印方法可以嵌入在高频区域，达到视觉的不可察觉性。针对每个子带，还可以继续分解。

- 部分加密方法是：将原始图像进行二级小波分解，利用不同的子密钥对各个分量分别进行加密，将密文重构，通过逆变换得到加密图像。利用密钥控制用户权限，不同权限用户所能浏览图像的分辨率不同。
- 加密过程：利用密钥对图像的二维数据矩阵中的每个数进行异或（加密解密算法可选），基本公式是： **m Xor y = z** 。式中 **m** 为原始数据， **y** 为密钥， **z** 为加密后的数据。

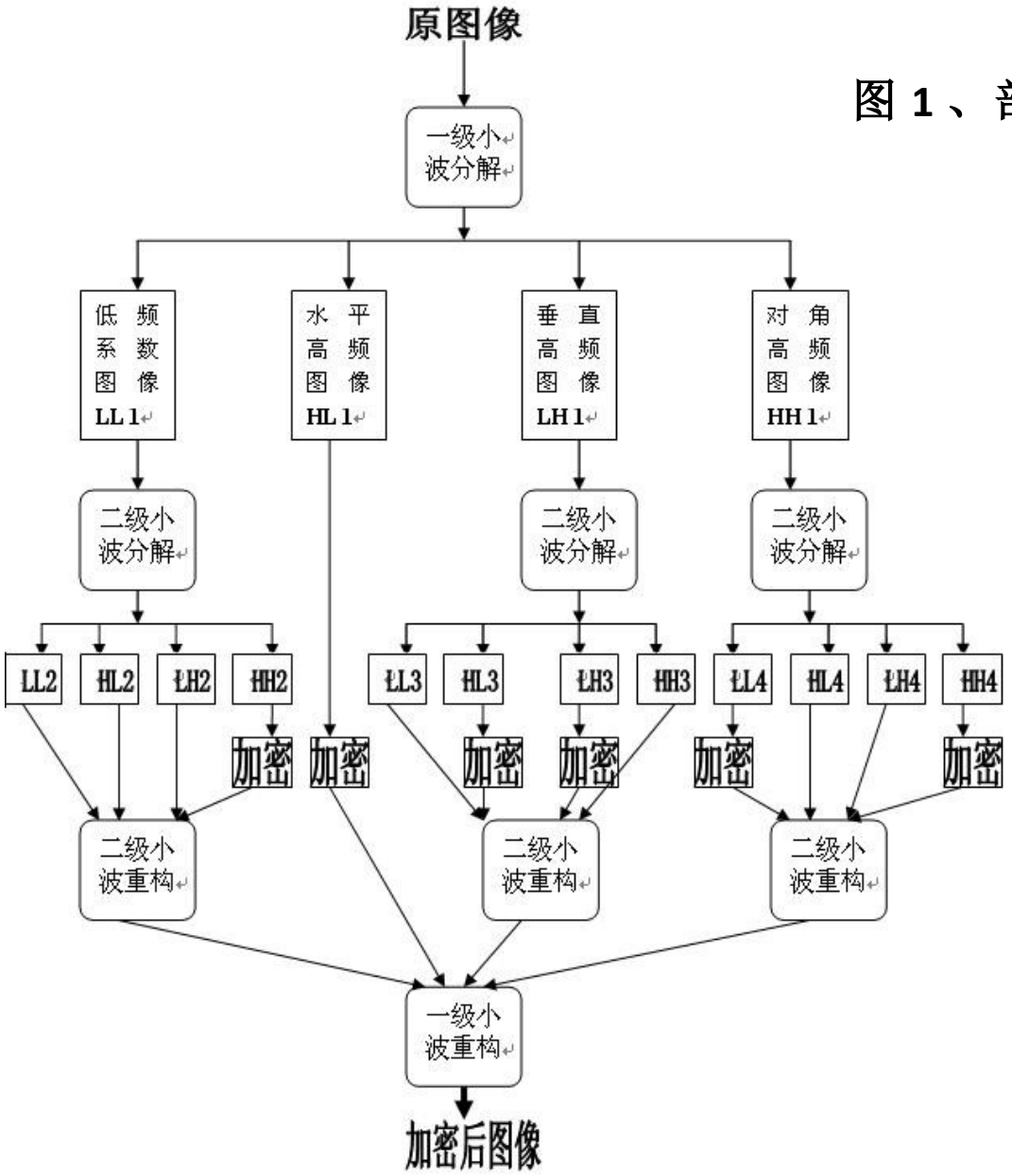

原图像
一级小波分解
低频系数图像 LL1
水平高频图像 HL1
垂直高频图像 LH1
对角高频图像 HH1
二级小波分解
二级小波分解
二级小波分解
LL2
HL2
LH2
HH2
LL3
HL3
LH3
HH3
LL4
HL4
LH4
HH4
加密
加密
加密
加密
加密
加密
二级小波重构
二级小波重构
二级小波重构
一级小波重构
加密后图像

图 1、部分加密流程图

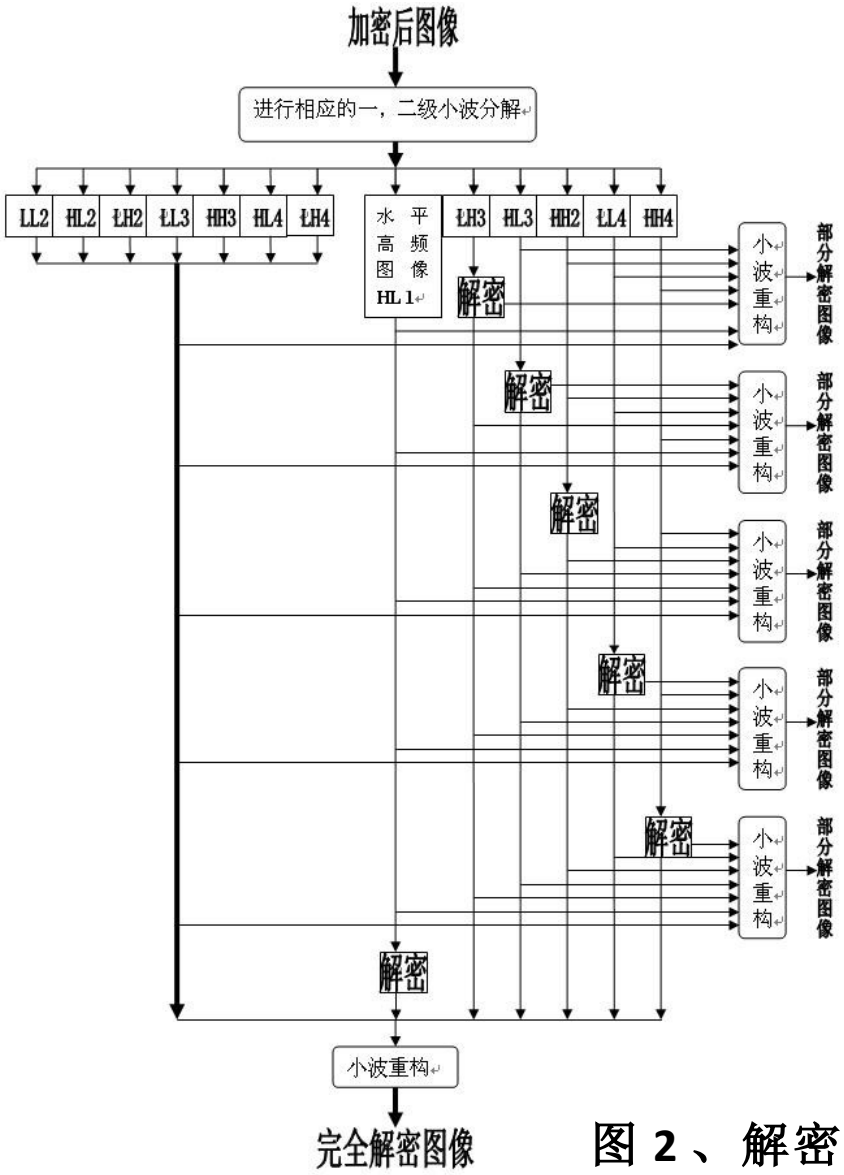


图 2、解密流程图

解密过程实际是提供了密码后对被加密的二维数据矩阵中的每个数进行再次异或，基本公式是： m Xor y Xor y = m 。式中 m 为原始数据， y 为密钥。

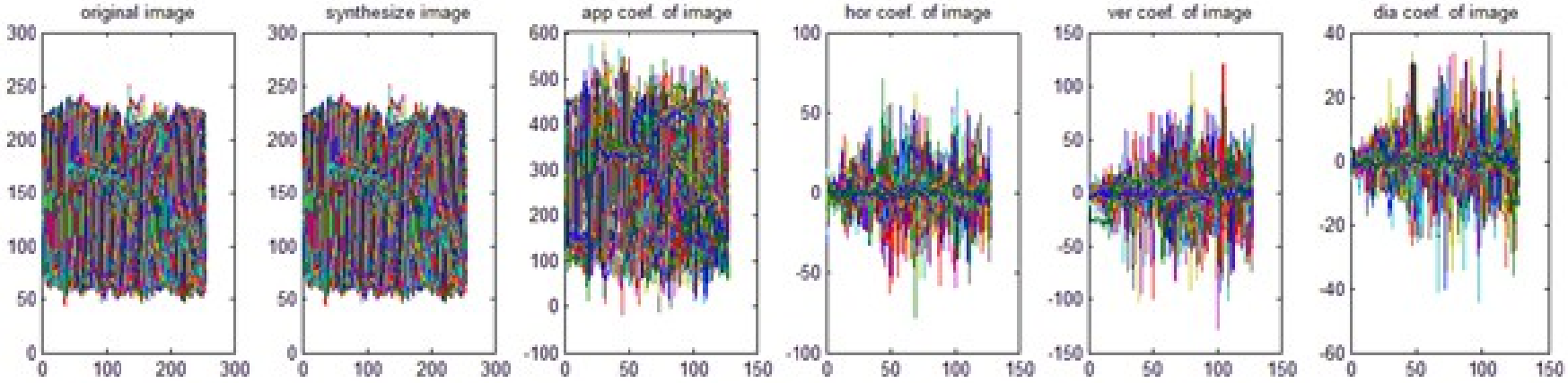
- 实验步骤
- 1. 用离散小波变换分析合成图像
- 分析合成图像文件包括以下步骤：
- 读取图像文件数据
- 二维离散小波变换
- 二维离散小波逆变换
- 观察结果
- 详细操作步骤为：

- 第一步：读取图像文件数据
- 在命令行中输入下述命令：
- **[fn, pn] = uigetfile('*.bmp', ' 请选择图像文件 ');**
- **[x, map] = imread(strcat(pn, fn), 'bmp');**
- **I = rgb2gray(x);**
- 说明：
- 读取图像文件
- 函数原型： **A = imread(filename,fmt)**
- 功能：读取 **fmt** 指定格式的图像文件内容
- 输入参数：
- **filename** ：图像文件名，字符串
- **fmt** ：图像文件格式名，字符串，函数支持的图像格式包括：**JPEG** ， **TIFF** ， **GIF** ， **BMP** 等等。
- 返回参数： **A** ：图像数据内容，整型
- 说明， **imread** 的其它参数和用法，可使用 **help imread** 命令查找。
- 例： **A=imread('src.bmp')** ，读取名为 ‘ **src.bmp**’ 的 **bmp** 图像。当参数中不包括文件格式名时，函数尝试推断出文件格式。
- **A=imread('src.bmp', 'bmp')** 读取名为 ‘ **src.bmp**’ 的 **bmp** 图像。效果与上述用法相同。
- **rgb2gray** 将 **RGB** 图像转换为灰度图。

- 第二步：二维离散小波变换
- 在命令行中输入下述命令：
- **sx = size(I);**
- **[cA1, cH1, cV1, cD1] = dwt2(I, 'bior3.7');**
- 说明：
- **dwt2** 函数对输入参数进行二维一级离散小波变换并返回近似分量，水平细节分量，垂直细节分量和对角线细节分量。如果要对图像进行多级小波分解，使用 **wavedec2** 函数。

- 第三步：二维离散小波逆变换
- 在命令行中输入下述命令：
- **xsync = uint8(idwt2(cA1, cH1, cV1, cD1, 'bior3.7', sx));**
- **A1 = uint8(idwt2(cA1, [], [], [], 'bior3.7', sx));**
- **H1 = uint8(idwt2([], cH1, [], [], 'bior3.7', sx));**
- **V1 = uint8(idwt2([], [], cV1, [], 'bior3.7', sx));**
- **D1 = uint8(idwt2([], [], [], cD1, 'bior3.7', sx));**
- 说明：
- **idwt2** 函数对输入参数进行二维离散小波逆变换并返回其系数。可以尝试仅使用近似分量，水平细节分量，垂直细节分量或对角线细节分量重构图像。

- 第四步：观察结果
- 请输入命令显示十个子图，分别是原始图像，使用全部系数恢复的图像，小波系数近似分量，水平细节分量，垂直细节分量和对角线细节分量以及仅使用近似分量，水平细节分量，垂直细节分量或对角线细节分量重构的图像。
- **figure;**
- **subplot(2, 6, 1); plot (I);title('original image');**
- **subplot(2, 6, 2); plot (xsync);title('synthesize image');**
- **subplot(2, 6, 3); plot(cA1);title('app coef. of image ');**
- **subplot(2, 6, 4); plot (cH1);title('hor coef. of image ');**
- **subplot(2, 6, 5); plot (cV1);title('ver coef. of image ');**
- **subplot(2, 6, 6); plot (cD1);title('dia coef. of image ');**
- **subplot(2, 6, 7); imshow(I);title('original image');**
- **subplot(2, 6, 8); imshow(xsync);title('synthesize image');**
- **subplot(2, 6, 9);imshow(A1);title('app coef. of image ');**
- **subplot(2, 6, 10);imshow(H1);title('hor coef. of image ');**
- **subplot(2, 6, 11); imshow(V1);title('ver coef. of image ');**
- **subplot(2, 6,12); imshow(D1);title('dia coef. of image ');**


original image
synthesize image
app coef. of image
hor coef. of image
ver coef. of image
dia coef. of image


original image
synthesize image
app coef. of image
hor coef. of image
ver coef. of image
dia coef. of image

- **2.** 加解密
- **function Y = endecrypt(a, x);**
- 异或方法： **bitxor**
- **3.** 对图像基于分辨率部分加密
- **sI = size(I);**
- **[cA1,cH1,cV1,cD1] = dwt2(I,'db1'); %** 二维小波变换
- **[cA2,cH2,cV2,cD2] = dwt2(cA1,'db1');%** 对近似分量做二级小波变换
- **[cA3,cH3,cV3,cD3] = dwt2(cH1,'db1'); %** 对水平分量做二级小波变换
- **[cA4,cH4,cV4,cD4] = dwt2(cV1,'db1'); %** 对垂直分量做二级小波变换
- **b = input('message', 's');**
- **c = input('message', 's');**
- **d = input('message', 's');**
- **e = input('message', 's');**
- **f = input('message', 's');**
- **g = input('message', 's');**
- **cD2 = endecrypt(b, cD2); %** 对近似分量二级小波变换的对角线分量加密
- **cA3 = endecrypt(c, cA3); %** 对水平分量二级小波变换的近似分量加密
- **cD3 = endecrypt(d, cD3); %** 对水平分量二级小波变换的对角线分量加密
- **cV4 = endecrypt(e, cV4); %** 对垂直分量二级小波变换的垂直分量加密
- **cD4 = endecrypt(f, cD4); %** 对垂直分量二级小波变换的对角线分量加密
- **cD1 = endecrypt(g, cD1); %** 对对角线分量加密
- **cA1 = idwt2(cA2,cH2,cV2,cD2,'db1'); %** 二级小波重构为近似分量
- **cH1 = idwt2(cA3,cH3,cV3,cD3,'db1'); %** 二级小波重构为水平分量
- **cV1 = idwt2(cA4,cH4,cV4,cD4,'db1'); %** 二级小波重构为垂直分量
- **X = idwt2(cA1,cH1,cV1,cD1,'db1'); %** 一级小波重构
- **subplot(1,2,1); imshow(I, []); %** 原图
- **subplot(1,2,2); imshow(X, []); %** 部分加密后的图

- 5. 对图像部分解密实现访问控制
- sI = size(I);
- [cA1,cH1,cV1,cD1] = dwt2(X,'db1'); % 二维小波变换
- [cA2,cH2,cV2,cD2] = dwt2(cA1,'db1'); % 对近似分量做二级小波变换
- [cA3,cH3,cV3,cD3] = dwt2(cH1,'db1');% 对水平分量做二级小波变换
- [cA4,cH4,cV4,cD4] = dwt2(cV1,'db1'); % 对垂直分量做二级小波变换
- b = input('message', 's'); % 输入解密密钥
- cD2 = endecrypt(b, cD2); % 对近似分量二级小波变换的对角线分量解密
- cA1 = idwt2(cA2,cH2,cV2,cD2,'db1'); % 重构近似分量
- cH1 = idwt2(cA3,cH3,cV3,cD3,'db1'); % 重构水平分量
- cV1 = idwt2(cA4,cH4,cV4,cD4,'db1'); % 重构垂直分量
- X1 = idwt2(cA1,cH1,cV1,cD1,'db1'); % 一级小波变换重构
- subplot(1,2,1); imshow(I, []);
- subplot(1,2,2); imshow(X1, []); % 部分解密后的图
-
- c = input('message', 's');
- cA3 = endecrypt(c, cA3); % 对水平分量二级小波变换的近似分量解密
- cA1 = idwt2(cA2,cH2,cV2,cD2,'db1');
- cH1 = idwt2(cA3,cH3,cV3,cD3,'db1');
- cV1 = idwt2(cA4,cH4,cV4,cD4,'db1');
- X2 = idwt2(cA1,cH1,cV1,cD1,'db1');
- subplot(1,2,1); imshow(I, []);
- subplot(1,2,2); imshow(X2, []); % 部分解密的图
-
- d = input('message', 's');
- cD3 = endecrypt(d, cD3); % 对水平分量二级小波变换的对角线分量解密
- cA1 = idwt2(cA2,cH2,cV2,cD2,'db1');
- cH1 = idwt2(cA3,cH3,cV3,cD3,'db1');
- cV1 = idwt2(cA4,cH4,cV4,cD4,'db1');
- X3 = idwt2(cA1,cH1,cV1,cD1,'db1');
- subplot(1,2,1); imshow(I, []);
- subplot(1,2,2); imshow(X3, []); % 部分解密的图

- 实验报告
- 1. 编程实现加密算法，并输入一幅图像对加密过程进行验证，记录显示结果，并与原始图像进行比较。
-
- 2. 编程实现解密算法，并对一副图像进行分层访问控制，记录显示结果，并与原始图像进行比较。
-
- 3、理解整个加密和解密过程，试写出实验的关键步骤。简单概述你在编程过程中遇到了哪些问题，如何解决的？