第三章 信息隐藏

马晓静
lindahust@mail.hust.edu.cn

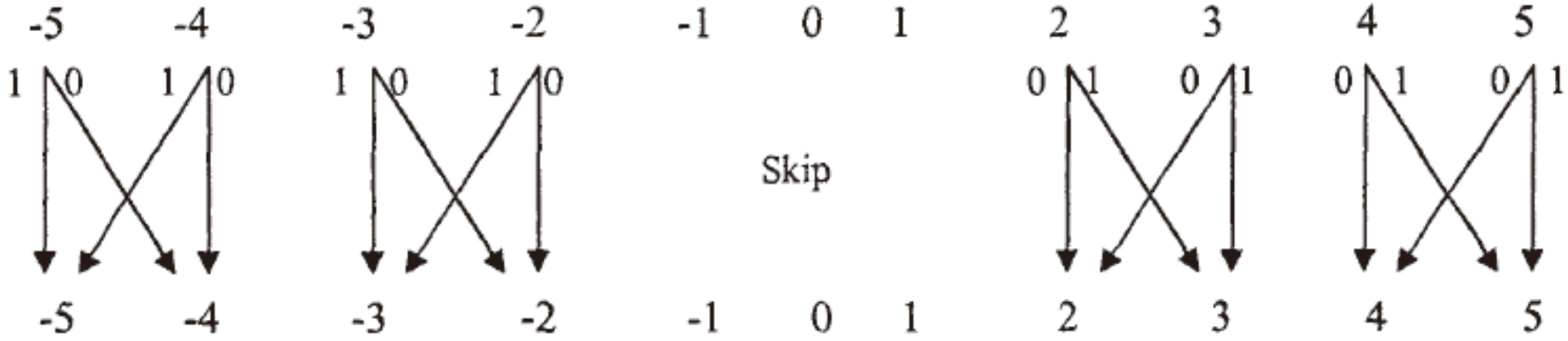
变换域隐写

- 在变换域进行隐写可以将对图像修改的能量分散，一方面可以结合人类视觉特性增强载体的不可察觉性，另一方面也可以提高一定的鲁棒性。
- 变换域隐藏的总体思想，就是将秘密信息隐藏在载体的最重要部位
- DCT变换等，都是能量守恒变换，在变换域中将能量集中，隐藏时将秘密信息与载体的视觉重要部分紧密联系在一起

- **JSTEG**
- **F5**

JSTEG

此处负数的时候反了，实际可以理解成使用补码表示的数字的最低位表示隐藏信息。



- JSteg是最早以JPEG图像为载体的隐密算法，主要是利用了LSB替换思想在DCT域实现。
- 其主要思路是：将一个二进制位的隐密信息嵌入到量化后的DCT系数的LSB上，但对原始值为-1、0、1的DCT系数例外。
- 提取隐密信息时，只需将载密图像中不等于-1、0、1的量化DCT系数的LSB逐一取出即可。
- 顺序或随机选择元素。

嵌入实例

- 嵌入信息：0010100110111010...
- 63个AC系数：57, 45, 0, 0, 0, 0, 23, 0, -30, -16, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,..., 0
- JSTEG
  - 56 , 44 , 0, 0, 0, 0, 23, 0, -31, -16, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,..., 0.
    提取信息：00101

category表格里：

-30 00001 -15:0000 -16:01111 -17:01110

9. Huffman Coding

Category	Values	Bits for the value
1	-1,1	0,1
2	-3,-2,2,3	00,01,10,11
3	-7,-6,-5,-4,4,5,6,7	000,001,010,011,100,101,110,111
4	-15,...,-8,8,...,15	0000,...,0111,1000,...,1111
5	-31,...,-16,16,...31	00000,...,01111,10000,...,11111
6	-63,...,-32,32,...63	000000,...,011111,100000,...,111111
7	-127,...,-64,64,...,127	0000000,...,0111111,1000000,...,1111111
8	-255,..,-128,128,..,255	...
9	-511,..,-256,256,..,511	...
10	-1023,..,-512,512,..,1023	...
11	-2047,..,-1024,1024,..,2047	...

Figure 6. Table of values and bits for the value

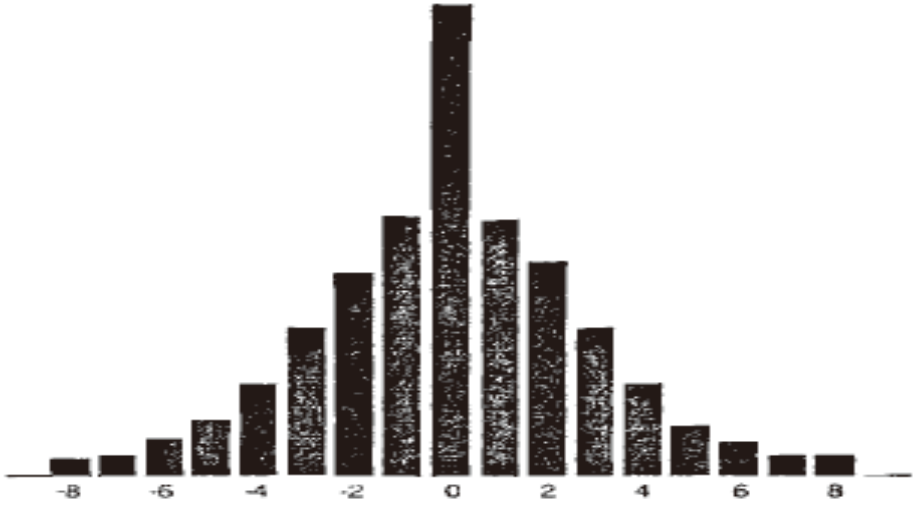
JSTEG

- JPEG图像的DCT系数通常满足以下三个特性

  (1) DCT系数的绝对值越大，其对应直方图中的值出现频率就越小。

  (2) 随着DCT系数绝对值的增大，其出现频率下降的幅度减小。

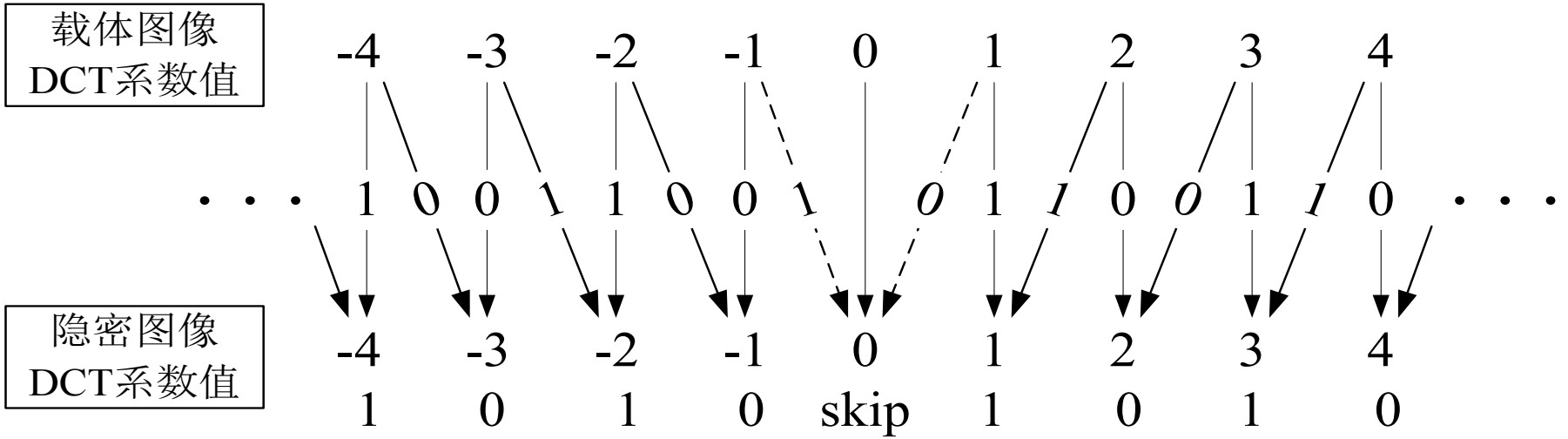
  (3) 各系数出现的频率关于0对称。



JSTEG：DCT系数“成对效应”

F4

- F4算法中，用正奇数和负偶数代表秘密消息1、负奇数和正偶数代表秘密消息0。
- **F4嵌入机制**



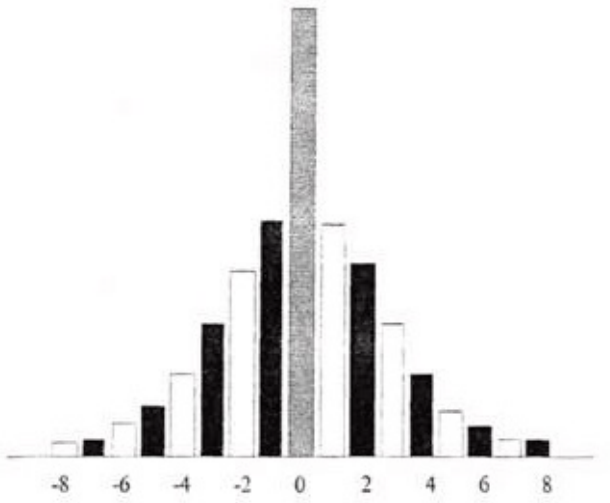
嵌入实例

- 嵌入信息：0010100110111010...
- 63个AC系数：57, 45, 0, 0, 0, 0, 23, 0, -30, -16, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,..., 0
- JSTEG
  - 56 , 44 , 0, 0, 0, 0, 23, 0, -31, -16, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,..., 0.
    提取信息：00101
- F4
  - 56 , 44 , 0, 0, 0, 0, 23, 0, -29, -16, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,..., 0.
    提取信息：00101

category表格里：-30 00001 -15:0000 -16:01111 -17:01110

F4

- F4隐密算法作用后图像的DCT系数直方图矩阵



F5

- F4缺陷：顺序嵌入；
- F5原理：
  - 在F4基础上改为随机嵌入方式
  - 并应用了矩阵编码来减小数据修改量。

F5

- 矩阵编码：

  （1,n,k）：将k比特秘密信息嵌入到$n=2^k-1$个符合要求的DCT系数上，最多只修改1个位置；

- 例：k=2，b1,b2是2个秘密信息比特，a1,a2,a3是3个位置的LSB，⊕表示异或；

  b1=a1⊕a2，b2=a2⊕a3，则不修改数据；

  b1≠a1⊕a2，b2=a2⊕a3，则修改a1；

  b1=a1⊕a2，b2≠a2⊕a3，则修改a3；

  b1≠a1⊕a2，b2≠a2⊕a3，则修改a2。

  提取隐密信息时，只需进行逆操作，即b1=a1⊕a2，b2=a2⊕a3。

  K=3?

F5

矩阵编码：

- 例：k=2，b1,b2是2个秘密信息比特，a1,a2,a3是3个位置的LSB，⊕表示异或；

  b1=a1⊕a2，b2=a2⊕a3，则不修改数据；

  b1≠a1⊕a2，b2=a2⊕a3，则修改a1；

  b1=a1⊕a2，b2≠a2⊕a3，则修改a3；

  b1≠a1⊕a2，b2≠a2⊕a3，则修改a2。

  提取隐密信息时，只需进行逆操作，即b1=a1⊕a2，b2=a2⊕a3。

  - 嵌入两比特的隐密信息平均只需修改3/4个LSB，而普通的LSB隐密需要修改一个LSB，嵌入效率提高了，而F5算法应用矩阵编码，目的就是为了提高LSB隐密算法的嵌入效率
  - 但有一个缺陷就是载体利用率降低了。

F5

1. 获得量化DCT系数；
2. 根据密钥种子产生伪随机数重排列量化DCT系数；
3. 利用矩阵编码嵌入秘密信息密文。不考虑DC系数和值为0的AC系数。
    1. 根据矩阵编码计算是否需要修改DCT系数，若不需要则继续嵌入下一组数据；若需要则将DCT系数绝对值减1，符号不变。
    2. 判断修改后的DCT系数是否变为0，若没有则继续嵌入下一组数据；若系数变为0，则本次隐藏无效，返回继续嵌入本组数据。
4. 嵌入完成后，逆置乱DCT系数，编码获得隐密JPEG图像

- 基本保留了载体图像原DCT系数的直方图特征，所以能够抵抗视觉攻击和统计攻击

嵌入实例

- 嵌入信息：0010100110111010...
- 63个AC系数：57, 45, 0, 0, 0, 0, 23, 0, -30, -16, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,..., 0
- JSTEG
  - 56 , 44 , 0, 0, 0, 0, 23, 0, -31, -16, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,..., 0.
    提取信息：00101
- F4
  - 56 , 44 , 0, 0, 0, 0, 23, 0, -29, -16, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,..., 0.
    提取信息：00101
- F5
  - 57 , 45 , 0, 0, 0, 0, 23, 0, -29, -16, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,..., 0.
    提取信息：0010

category表格里：-30 00001 -15:0000 -16:01111 -17:01110

Lossless Data Hiding